

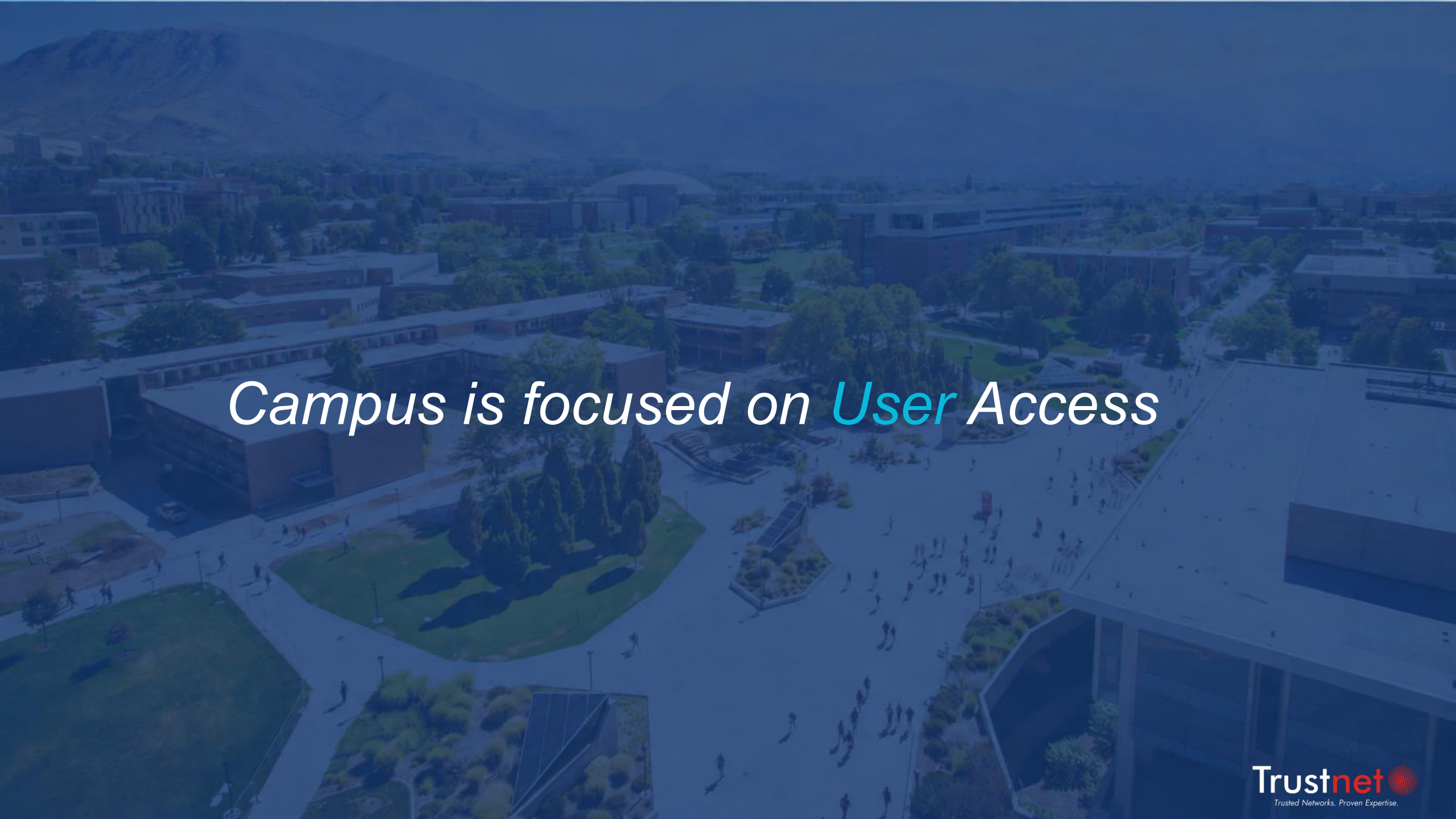
Overlay Design Options for Campus Networks

Sinan YILMAZ
CCIE #28722
Trustnet Managing Partner

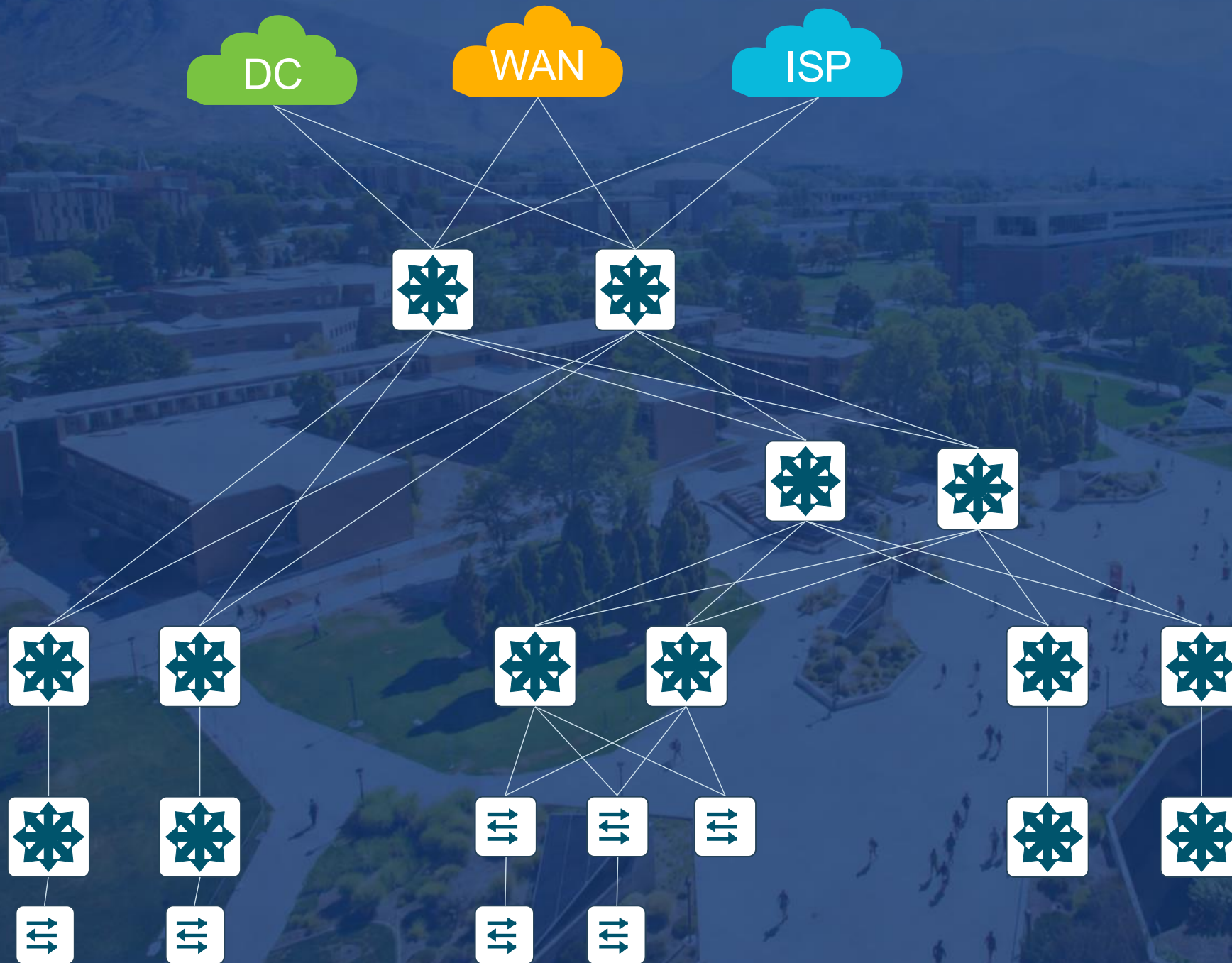


Agenda

- 01 **Campus Architecture**
- 02 **What is Underlay & Overlay**
- 03 **Fabric Benefits**
- 04 **SD-Access with LISP**
- 05 **Vxlan BGP EVPN**

An aerial photograph of a large university campus, featuring numerous brick buildings, green lawns, and walking paths. In the background, a range of mountains is visible under a clear sky. The entire image is overlaid with a semi-transparent blue filter.

*Campus is focused on **User** Access*



Core Interconnect
Core + Edge

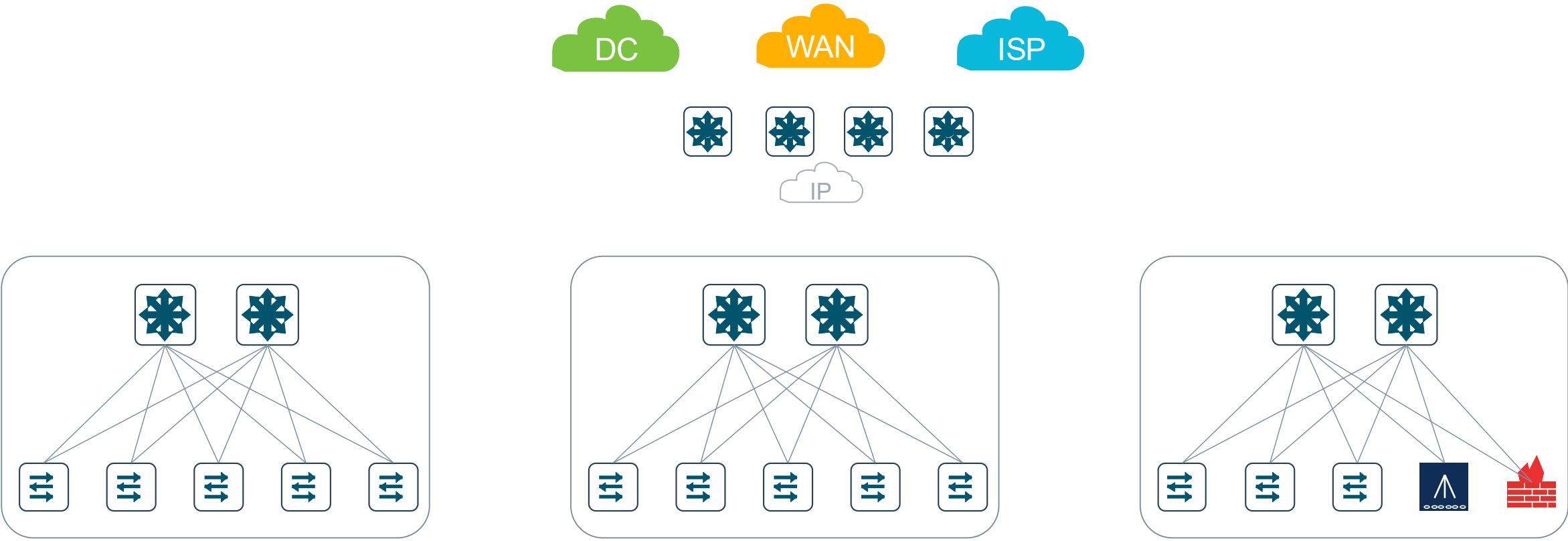
Core

Distribution

Access

Extended Access
IOT/FTTX

Traditional Multilayer Design

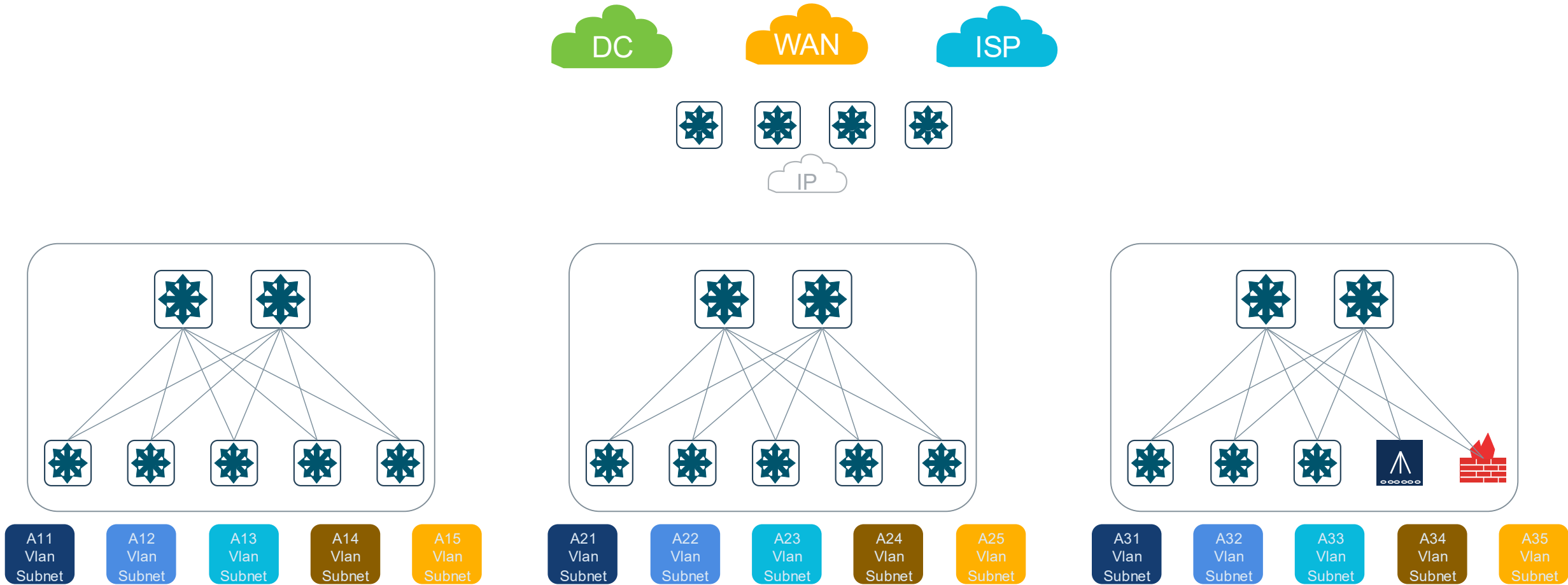


VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet – VLAN | Subnet –

Traditional Multilayer Design

- Structured physical networking supporting distributed bridging and central routing function
- Hierarchical system role and networking function at each layer
- Deterministic Layer 2 and Layer 3 forwarding paths provides network scalability, resiliency in best practice network environment
- Limited traditional protocols flexibility and complex operational overhead

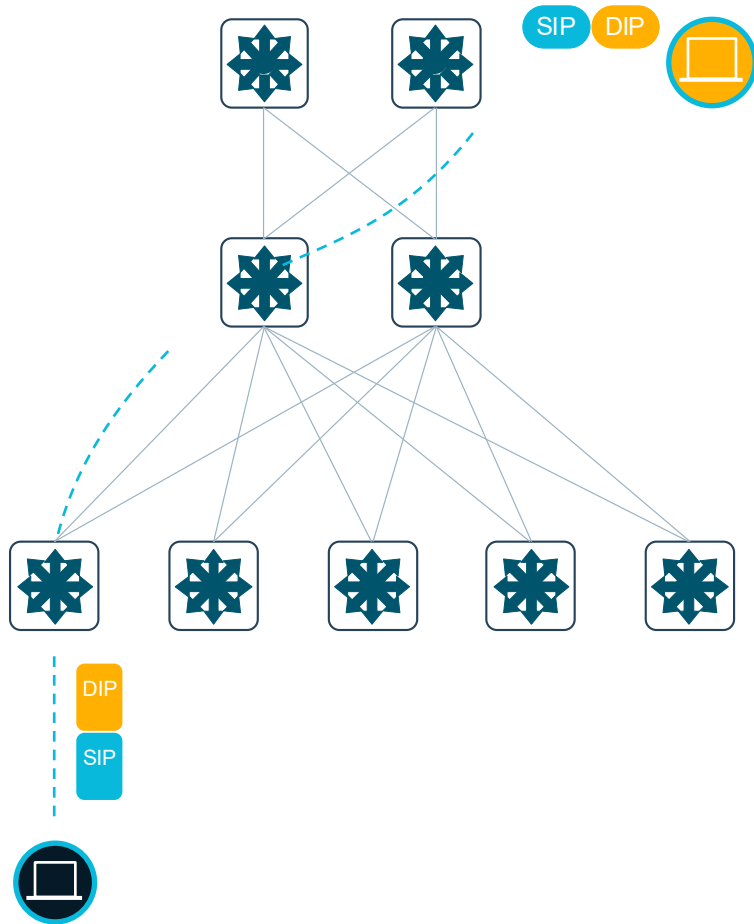
Traditional Routed Access Design



Traditional L3 Access Design

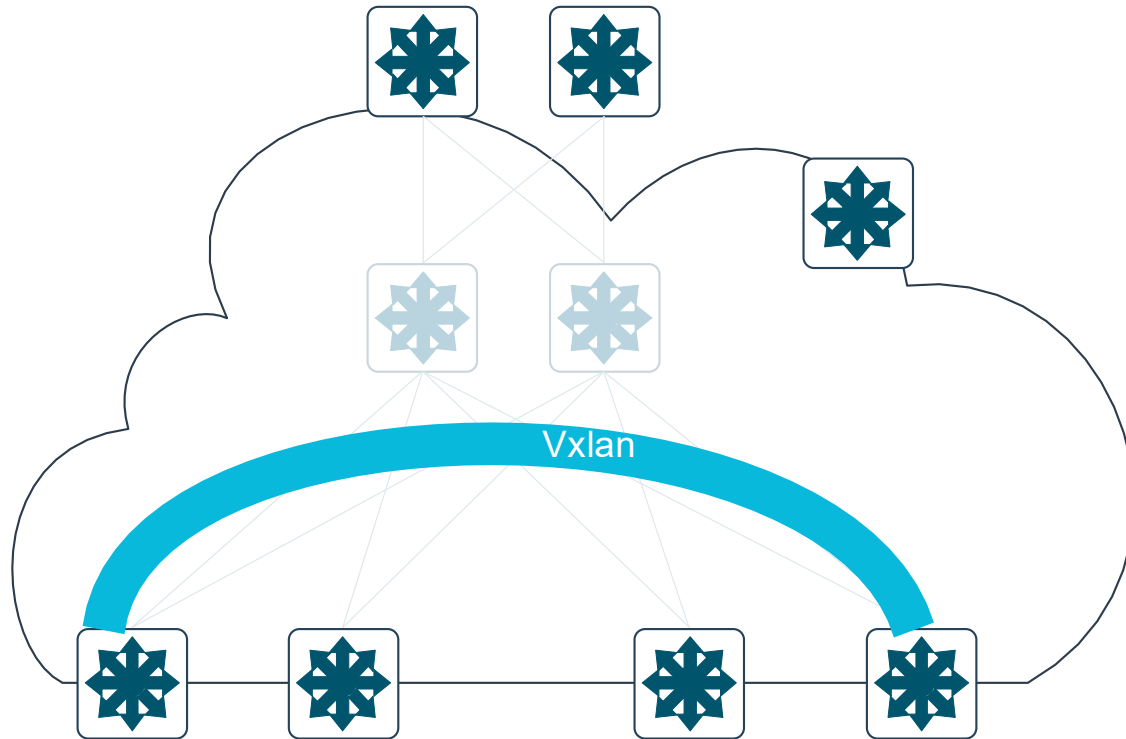
- Consistent structured physical networking supporting fully distributed bridging and routing function
- Common principal for hierarchical system role and networking function at each layer
- Simplified and deterministic non-blocking Layer 3 forwarding paths provides network scalability, resilient network environment
- Limited mobility and traditional Layer 2 protocols flexibility, complex routing operational overhead and increase cost

Underlay Networks



- Consists of the actual hardware (Routers/Switches), Routing, and physical Links (Fiber, copper, etc..)
- Traditional Layer 3 Routed Network and provides connectivity between network devices.
- End hosts communication relies on IGP or EGP Routing Protocols

Vxlan Encapsulation



Standards based Encapsulation

- RFC 7348
- Uses UDP-Encapsulation

Transport Independent

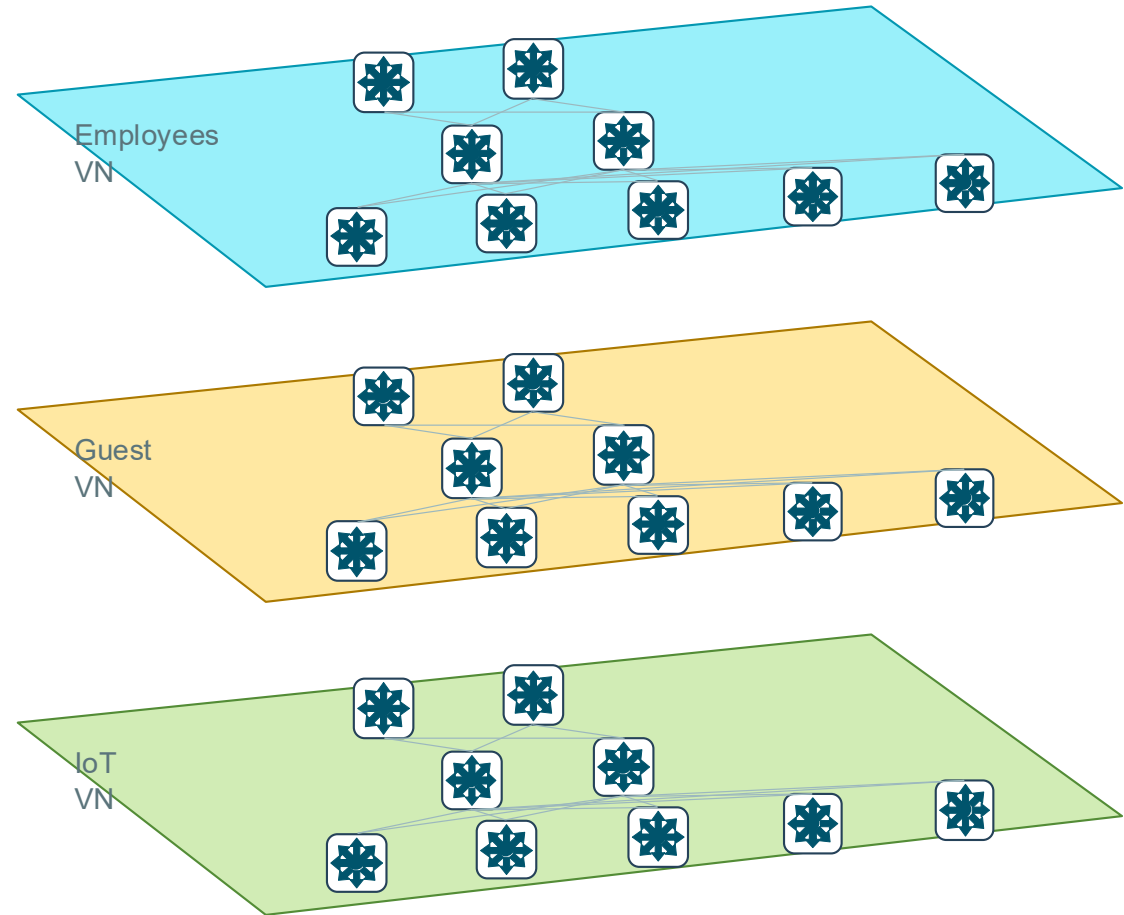
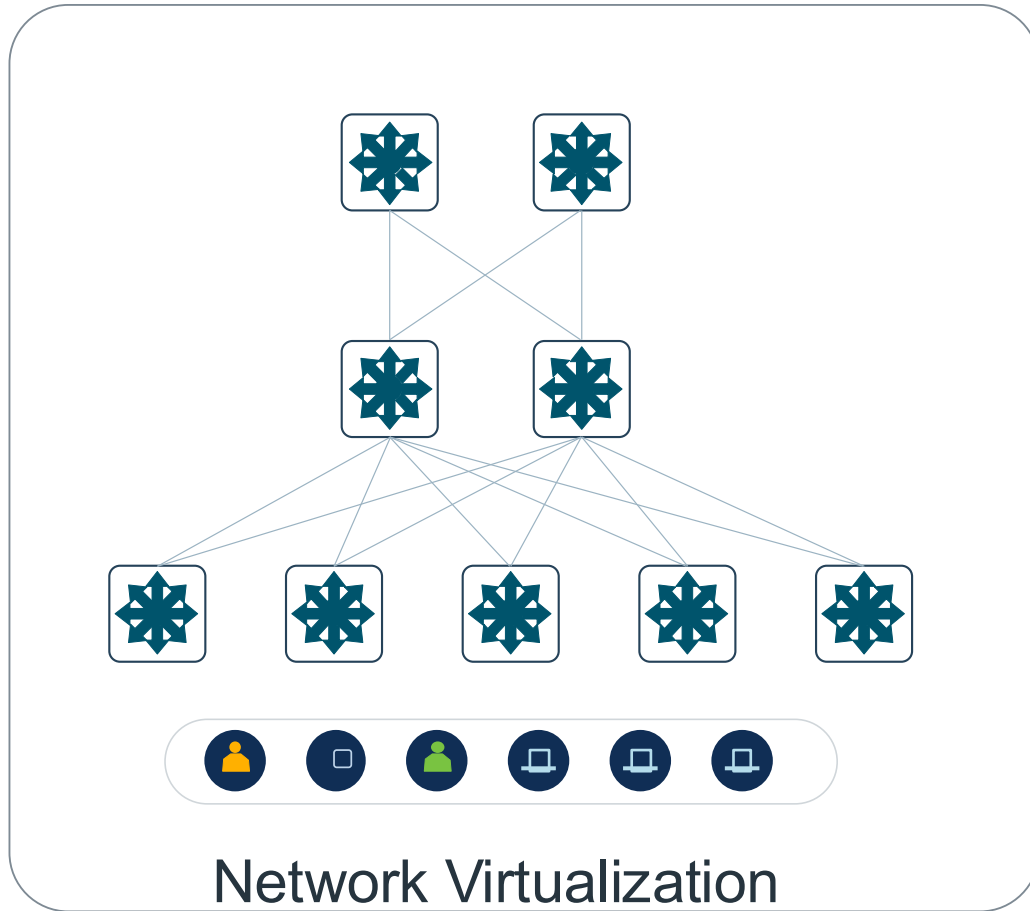
- Layer-3 Transport (Underlay)

Flexible Namespace

- 24-bit field (VNID) provides ~16M unique identifier
- Allows scalable Segmentations

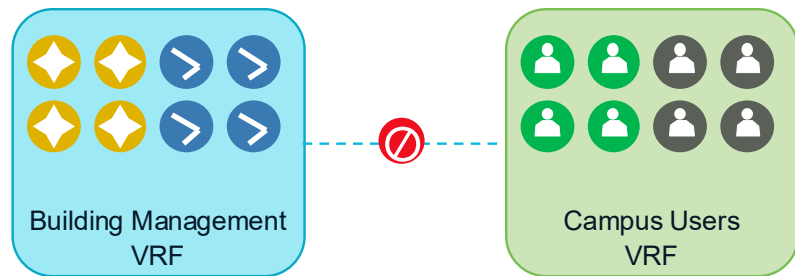
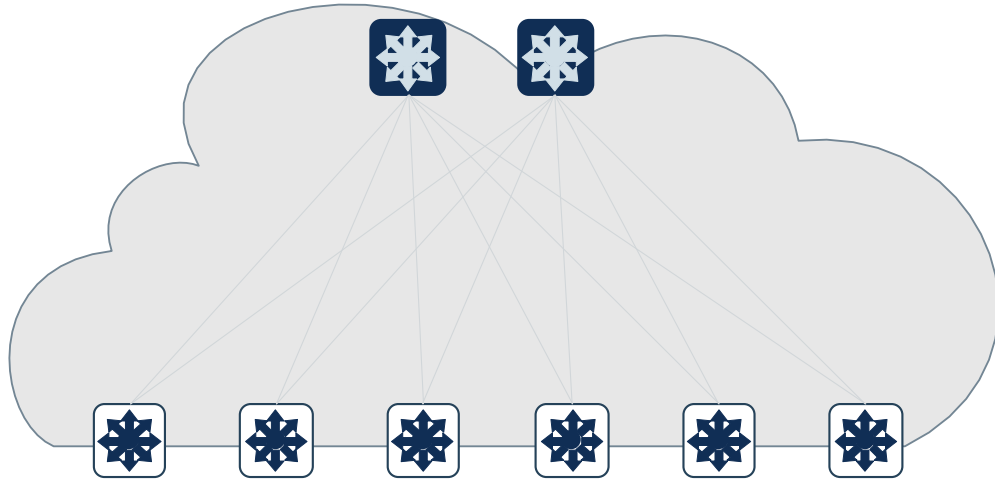
Why Fabrics ?

Overlay Networks

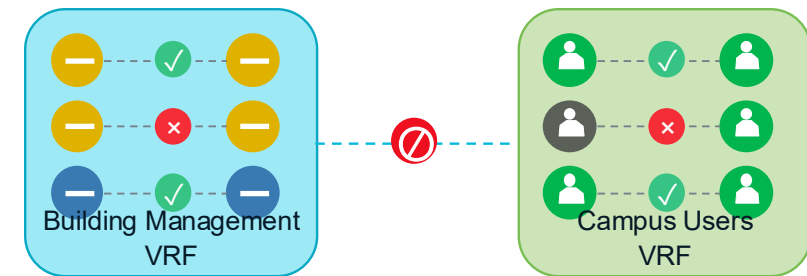
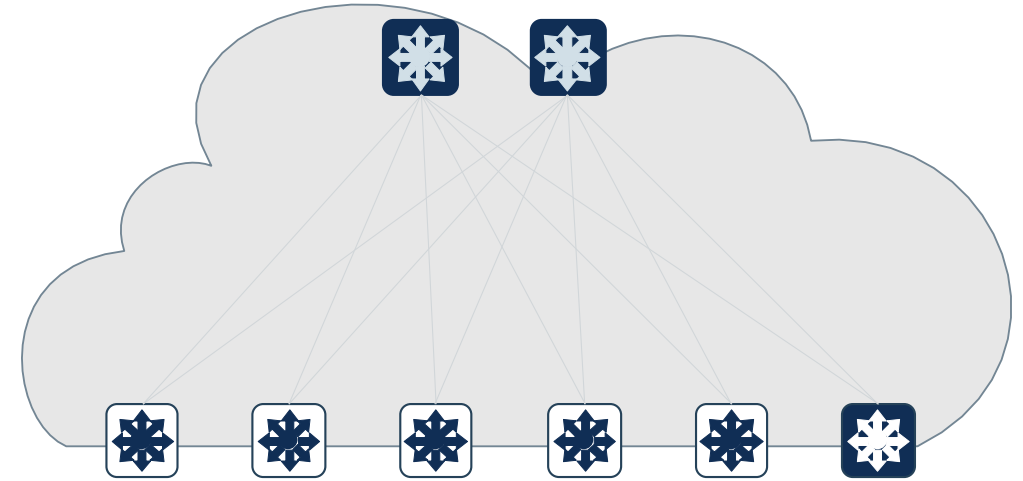


Virtualized network layer decoupled from physical underlay | Unique security policies per logical domain |
Traffic isolation per application, group, service etc...

Segmentation at Scale

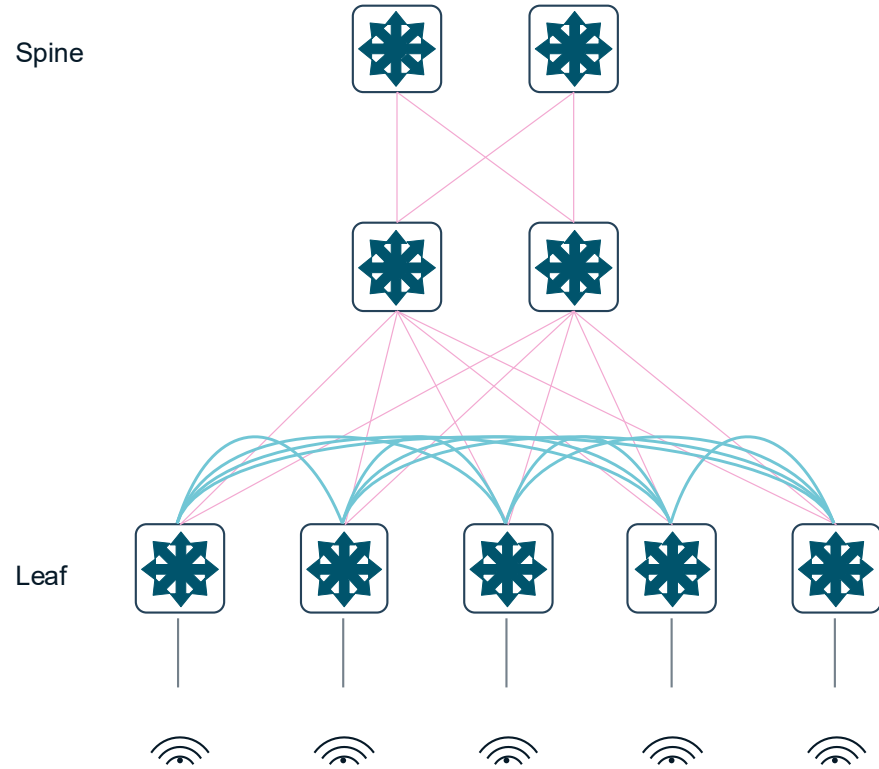


Macro Segmentation: No communication between VRF's



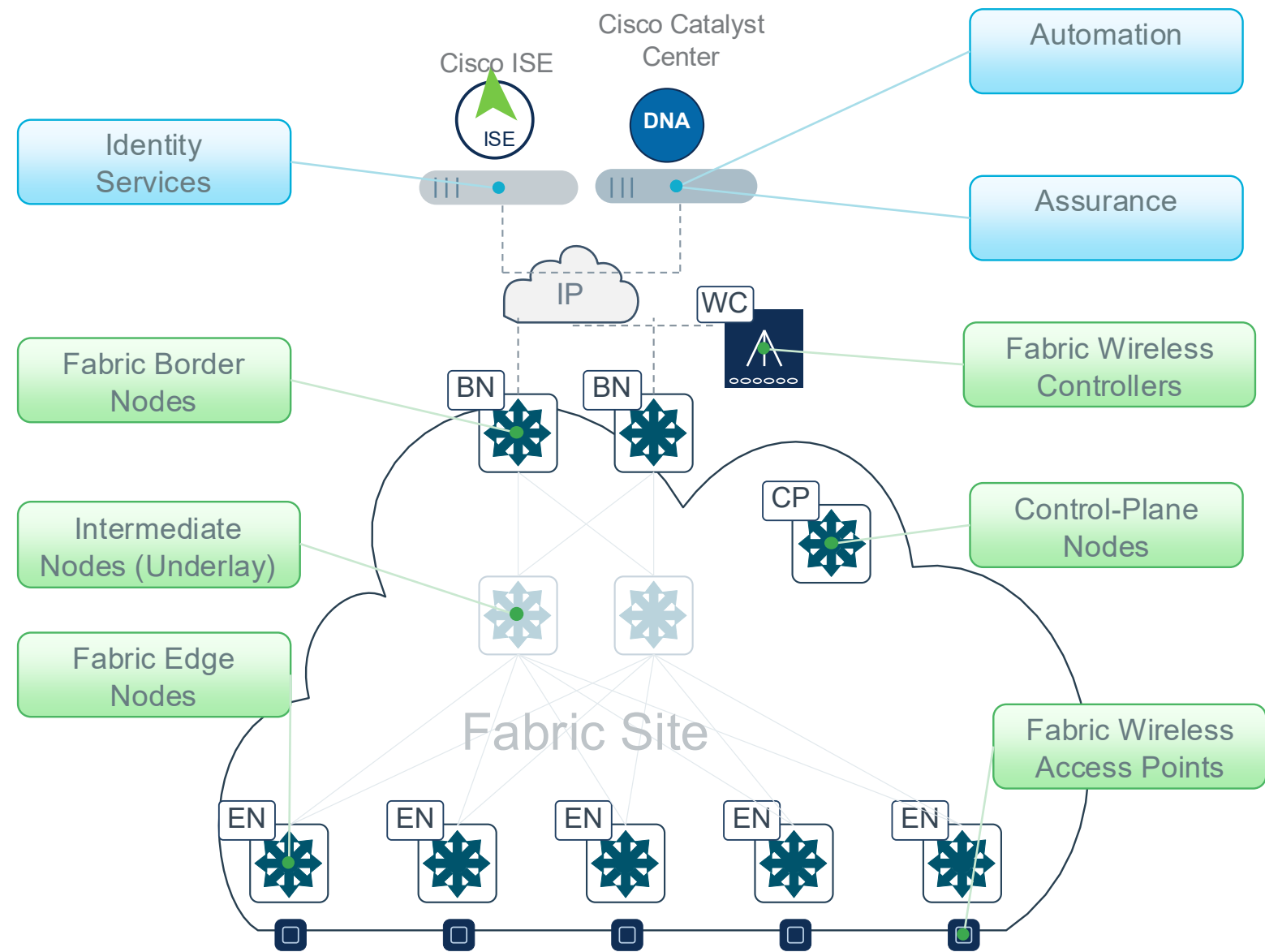
Micro Segmentation: Second level Segmentation between groups within a VRF

Scalable and Efficient Subnet Stretch



- Extend Layer 2 domains beyond traditional boundaries using VXLAN overlay, eliminating VLAN limitations
- Subnet stretch with or without extending Flood Domain
- Optimized Layer 2 domains over non-Blocking Layer 3 networks
- Allows flexible L2 extension with optimized L3 routing at the edge for better traffic flow
- Consistent Wired and Wireless Policy across the network

SD-Access with LISP

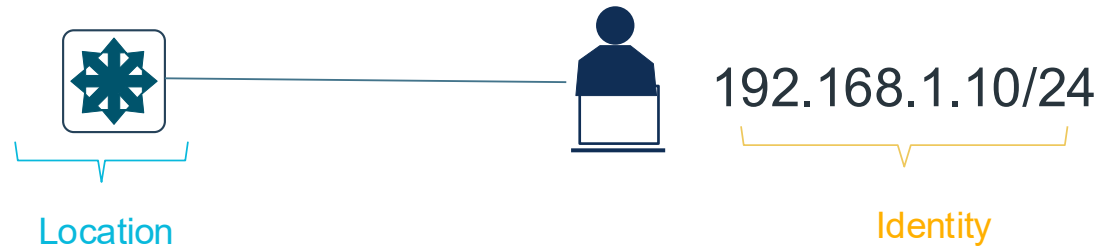


- **Network Automation** – Simple GUI and APIs for intent-based Automation of wired and wireless fabric devices
- **Network Assurance** – Data Collectors analyze Endpoint to Application flows and monitor fabric device status
- **Identity Services** – NAC & ID Services (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A fabric device (e.g. Core) that connects External L3 network(s) to the SD-Access fabric
- **Fabric Edge Nodes** – A fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SD-Access fabric
- **Intermediate Nodes** – A Layer 2 or Layer 3 Underlay network system providing basic transport and forwarding plane.
- **Fabric Wireless Controller** – A fabric device (WLC) that connects Fabric APs and Wireless Endpoints to the SD-Access fabric

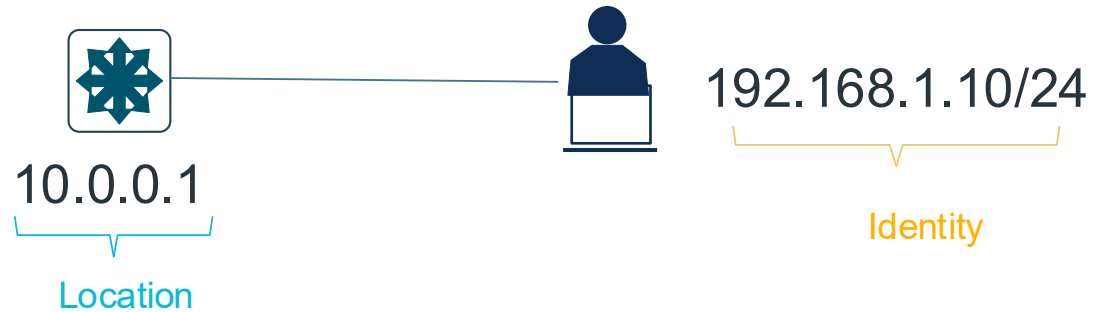
Compatibility Matrix:

https://www.cisco.com/c/dam/en/us/td/docs/Website/enterprise/catalyst_center_compatibility_matrix/index-sda.html

Locator/ID Separation Protocol (LISP)

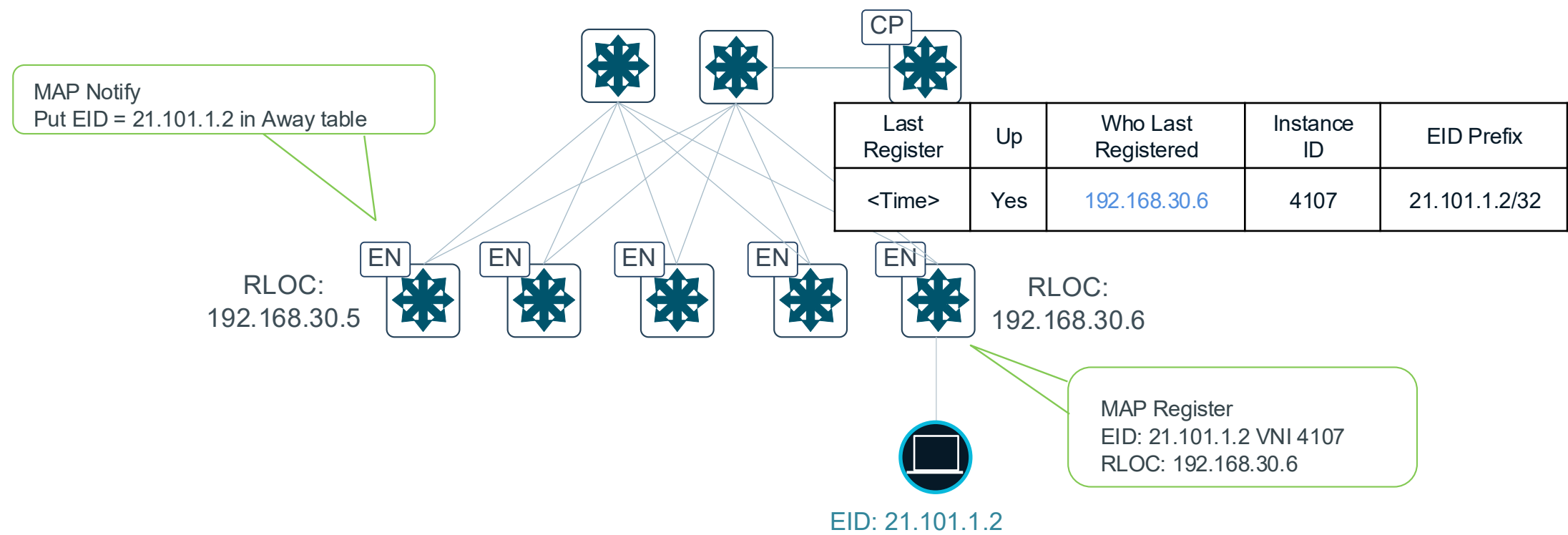


Resolving **Locators** for **Identities**



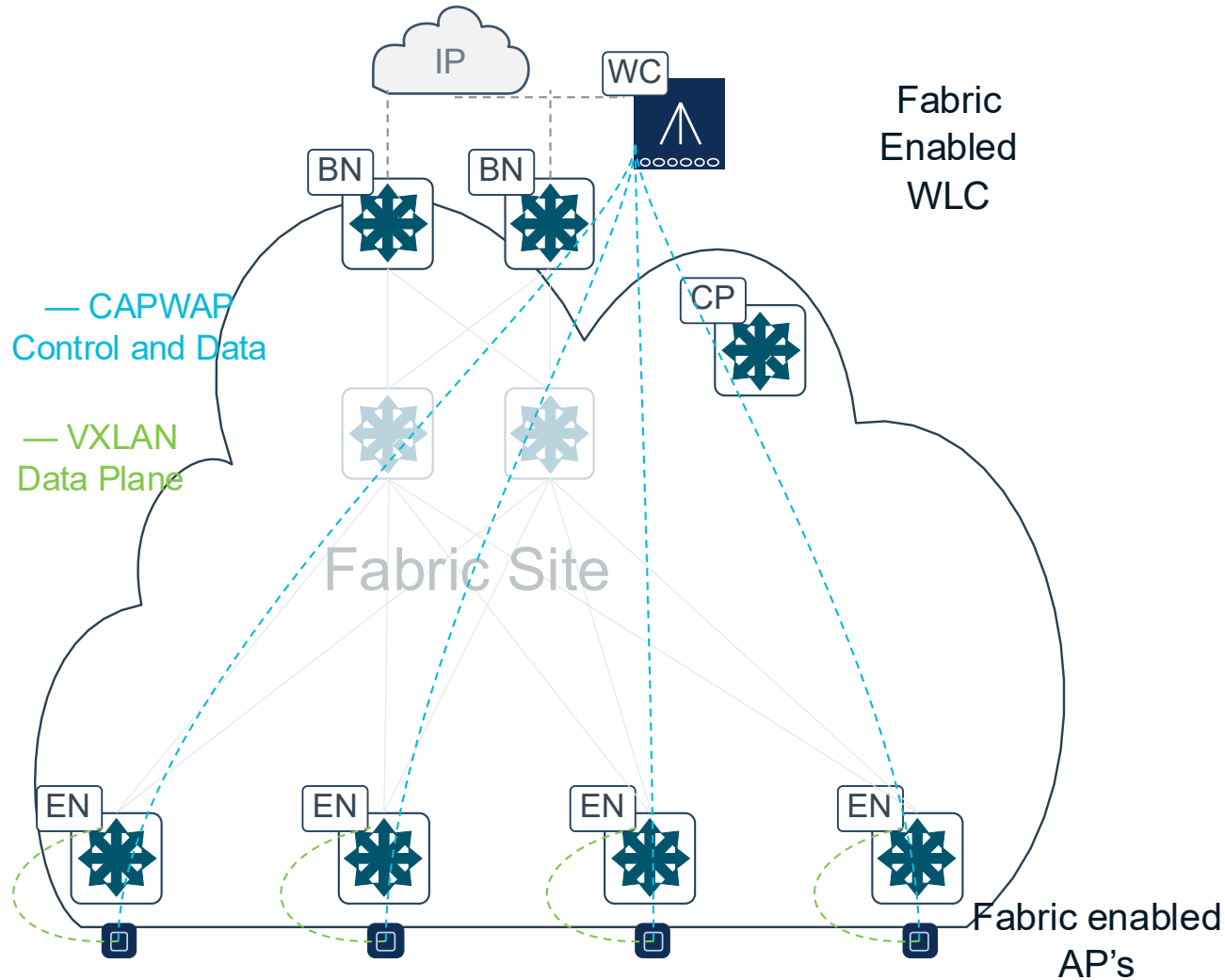
Locator/ID Separation Protocol (LISP)

Seamless Roaming



Cisco SD-Access Architecture

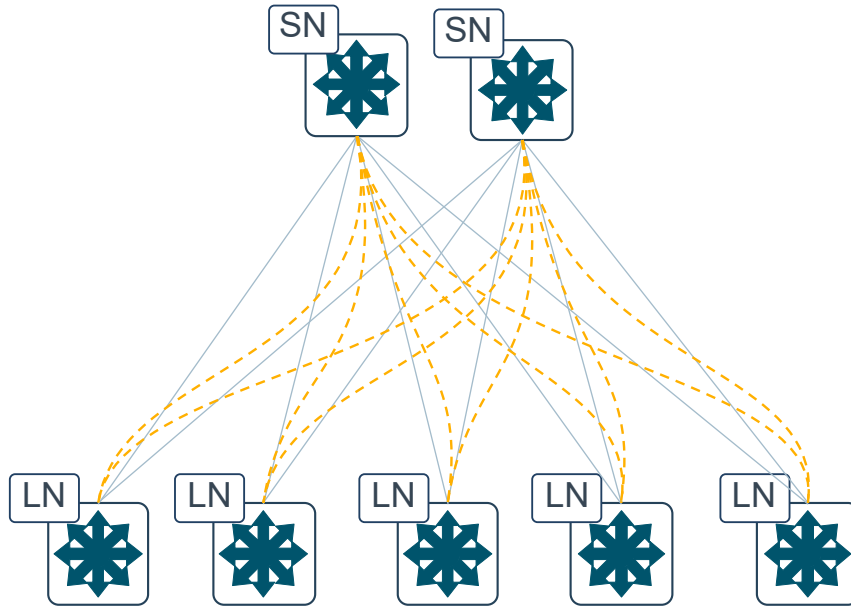
Fabric Enabled Wireless



- Unified Wired and Wireless Architecture
- Distributed Wireless – No hairpinning
- Simplified Management
- Consistent Wired and Wireless Policy
- End-to-End Automation for Wired and Wireless Deployment
- CAPWAP Control Plane, VXLAN Data Plane
- WLC/APs integrated in Fabric, LISP advantages

BGP EVPN VXLAN

BGP EVPN VXLAN



- Standards based Control-Plane
- RFC 8365 (and RFC 7432)
- Uses Multiprotocol BGP
- Uses Various Data-Planes
- VXLAN (EVPN-Overlay), MPLS, Provider Backbone (PBB)
- Many Use-Cases
- Integrated Routing and Bridging, MAC Mobility, Multi-Tenancy (VPN)

Cisco Enterprise Fabric Offerings

Cisco/Catalyst 9000 Fabric Network Automation

Catalyst Center



SDA LISP

Mobility, scale, cross-domain policy

Meraki Dashboard



Cloud Managed Fabric

Cloud simplicity, rapid rollout

Catalyst 9000 IOS-XE



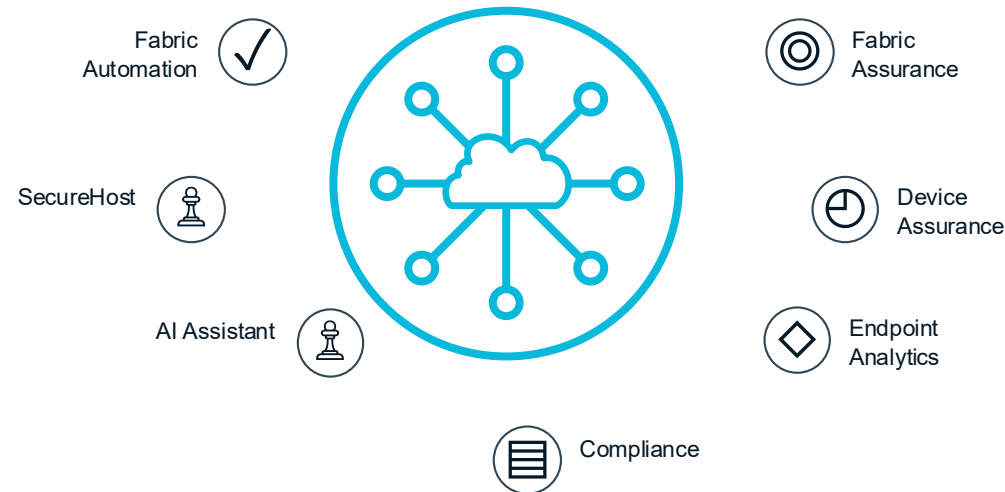
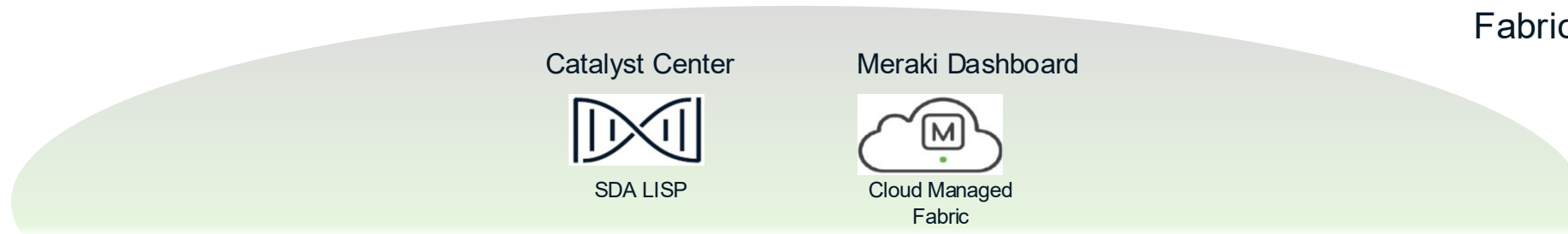
CLI | API

Standards, automation at scale

<https://github.com/Cat9kEVPN>

Simplified *On-Premises* or *Cloud Managed* Fabric Deployment

Fabric enabled wireless



 **IBN Fabric**
IT Transformation
Turnkey Automation
Rich Overlay Services

 **Secure Access**
Zero Trust NAC
L2/L3 Macro Segments
Micro segmentation

 **Flexible Design**
Brownfield Underlay
Variable Fabric Design
Tailored Overlay Zones

 **Deep Assurance**
Fabric VN Topology
Overlay Status
Device | Client | Apps

 **Network Compliance**
Endpoint Trust
Apps Pattern Visibility
Audit & Remediation

SD-Access vs. Traditional Campus Network

Criteria	Traditional Network	SD-Access
Configuration	Box-by-box, manual CLI	Centralized automation via Catalyst Center
Security	VLANs and ACLs scattered across devices	Identity-based macro and micro segmentation
Zero Trust	Added later, hard to enforce	Built-in access control with Cisco ISE
User mobility	New location means new IP and policy	IP address and policy follow the user
Wired and wireless	Separate management and policy	One architecture, one policy
Speed of change	Every change touches many devices	Defined once, applied fabric-wide
Visibility	Manual, reactive troubleshooting	End-to-end Assurance, proactive insight
Scale	4,094 VLANs, large L2 domains	~16M segments over a routed underlay

Why SD-Access

Stronger security, faster change and lower operational effort, delivered in one architecture.

Thank you

