CISCO Engage | Tech Day

Secure Networking With Catalyst Center and SDA

Nathan Lee, Solutions Engineer

March 18, 2026

Agenda

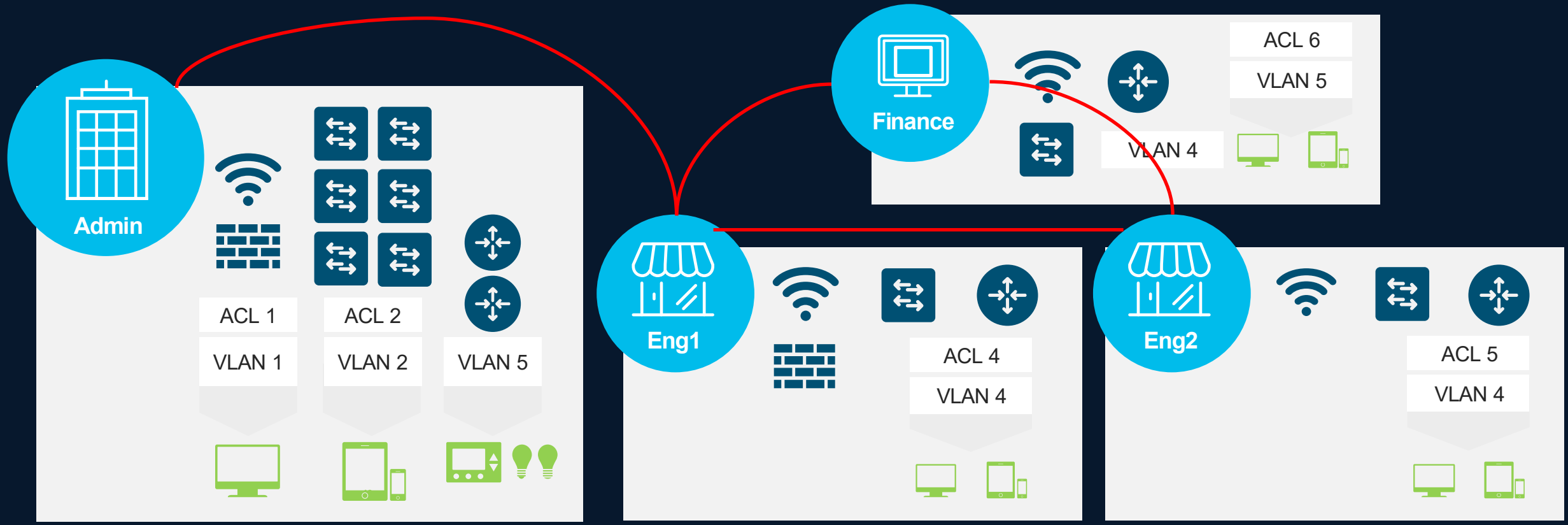
1. Introduction
2. Why SDA?
3. SDA Components
4. SDA Mechanics
5. Demo

Introduction

Why SDA?

Traditional Approaches to Campus Segmentation

Any issues here?



Setting Up End-End **Security** | Enabling Seamless **Mobility** | Users, Device and **IoT** Segmentation | Stability of Enterprise Network

What's the Business Intent Here?

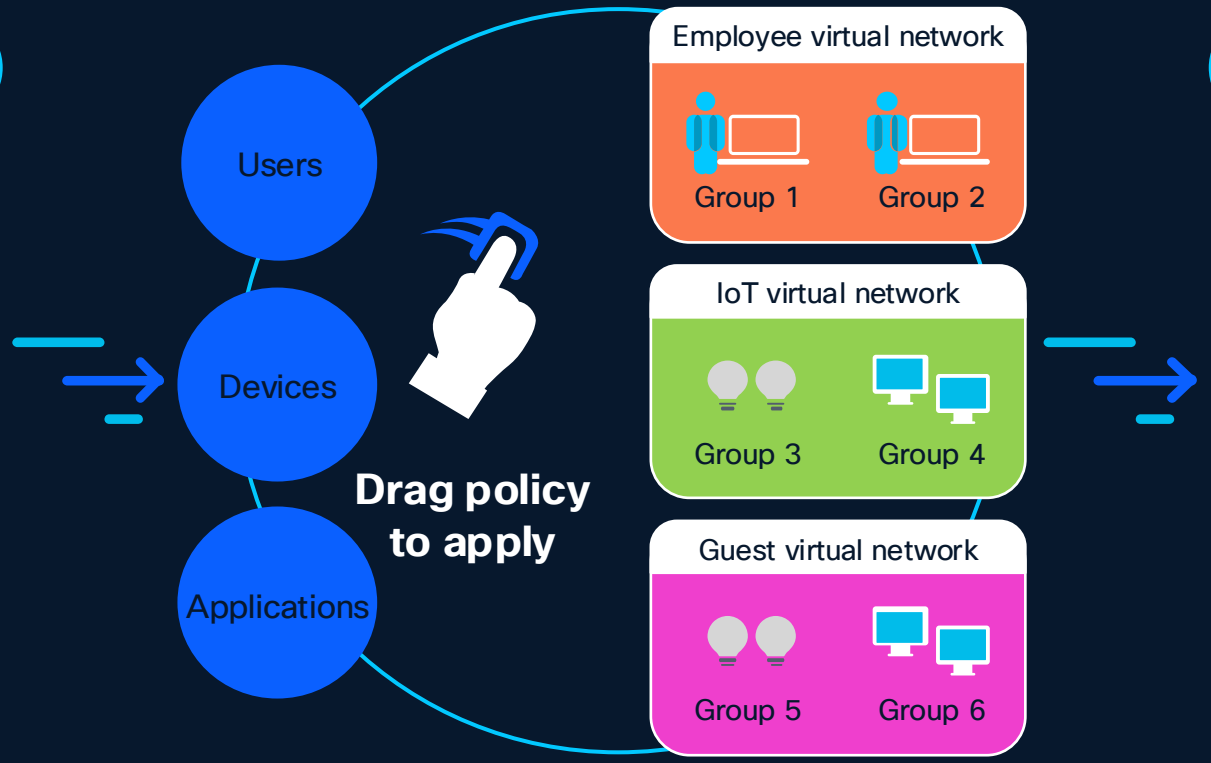
Traditional Security Policy

```
access-list 102 permit ip 178.97.113.59 255.255.255.255 gt 178 111.184.163.103 255.255.255.255 gt 959
access-list 102 deny ip 164.149.136.73 0.0.0.127 gt 1624 163.41.181.145 0.0.0.255 eq 810
access-list 102 permit icmp 207.221.157.104 0.0.0.255 eq 1979 99.78.135.112 0.255.255.255 gt 3231
access-list 102 permit tcp 100.126.4.49 0.255.255.255 lt 1449 28.237.88.171 0.0.0.127 lt 3679
access-list 102 deny icmp 157.219.157.249 255.255.255.255 gt 1354 60.126.167.112 0.0.31.255 gt 1025
access-list 102 deny icmp 76.176.66.41 0.255.255.255 lt 278 169.48.105.37 0.0.1.255 gt 968
access-list 102 permit ip 8.88.141.113 0.0.0.127 lt 2437 105.145.196.67 0.0.1.255 lt 4167
access-list 102 permit udp 60.242.95.62 0.0.31.255 eq 3181 33.191.71.166 255.255.255.255 lt 2422
access-list 102 permit icmp 186.246.40.245 0.255.255.255 eq 3508 191.139.67.54 0.0.1.255 eq 1479
access-list 102 permit ip 209.111.254.187 0.0.1.255 gt 4640 93.99.173.34 255.255.255.255 gt 28
access-list 102 permit ip 184.232.88.41 0.0.31.255 lt 2247 186.33.104.31 255.255.255.255 lt 4481
access-list 102 deny ip 106.79.247.50 0.0.31.255 gt 1441 96.62.207.209 0.0.0.255 gt 631
access-list 102 permit ip 39.136.60.170 0.0.1.255 eq 4647 96.129.185.116 255.255.255.255 lt 3663
access-list 102 permit tcp 30.175.189.93 0.0.31.255 gt 228 48.33.30.91 0.0.0.255 gt 1388
access-list 102 permit ip 167.100.52.185 0.0.1.255 lt 4379 254.202.200.26 255.255.255.255 gt 4652
access-list 102 permit udp 172.16.184.148 0.255.255.255 gt 4163 124.38.159.247 0.0.0.127 lt 3851
access-list 102 deny icmp 206.107.73.252 0.255.255.255 lt 2465 171.213.183.230 0.0.31.255 gt 1392
access-list 102 permit ip 96.174.38.79 0.255.255.255 eq 1917 1.156.181.180 0.0.31.255 eq 1861
access-list 102 deny icmp 236.123.67.53 0.0.31.255 gt 1181 31.115.75.19 0.0.1.255 gt 2794
access-list 102 deny udp 14.45.208.20 0.0.0.255 lt 419 161.24.159.166 0.0.0.255 lt 2748
access-list 102 permit udp 252.40.175.155 0.0.31.255 lt 4548 87.112.10.20 0.0.1.255 gt 356
access-list 102 deny tcp 124.102.192.59 0.0.0.255 eq 2169 153.233.253.100 0.255.255.255 gt 327
access-list 102 permit icmp 68.14.62.179 255.255.255.255 lt 2985 235.228.242.243 255.255.255.255 lt 2286
access-list 102 deny tcp 91.198.213.34 0.0.0.255 eq 1274 206.136.32.135 0.255.255.255 eq 4191
access-list 102 deny udp 76.150.135.234 255.255.255.255 lt 3573 15.233.106.211 255.255.255.255 eq 3721
```

SD-Access *segments* the network and *securely onboards* client devices

Before SD-Access

- VLAN and IP address-based
- Create IP-based ACLs for access policy
- Deal with policy violations and errors manually



After SD-Access

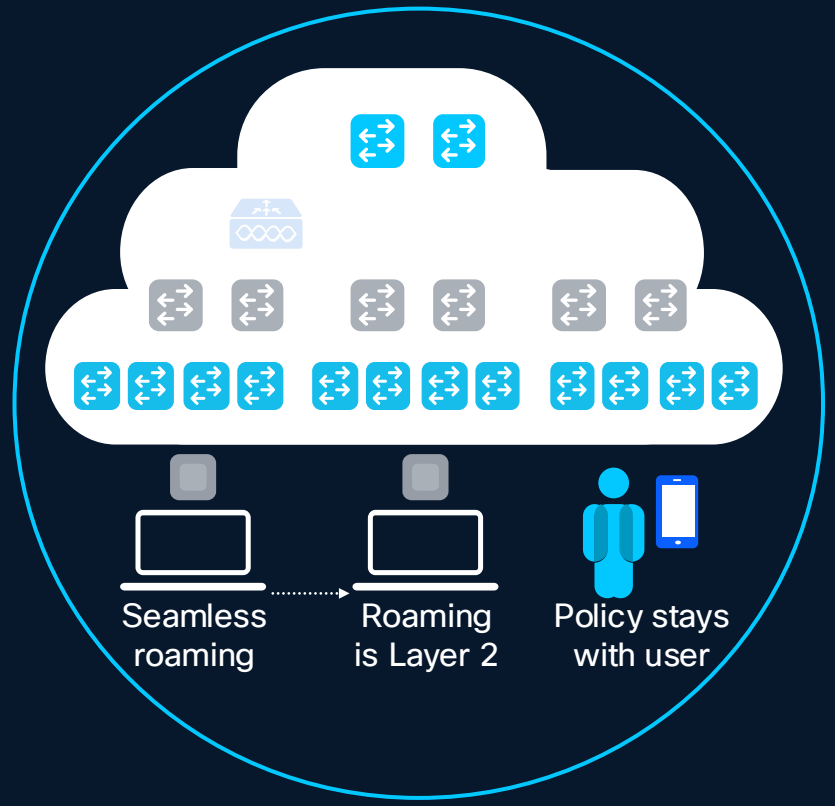
- No VLAN or subnet dependency for segmentation and access control
- Define one consistent policy
- Policy follows identity
- Visibility into traffic flows through AI/ML

Completely automated | Group-based policy | Policy follows identity

SD-Access enforces *policy consistently* over wired and wireless networks

Before SD-Access

- Repeated policy work for wired and wireless
- Roaming issues across Layer-3 domains
- Chase down IP addresses for troubleshooting



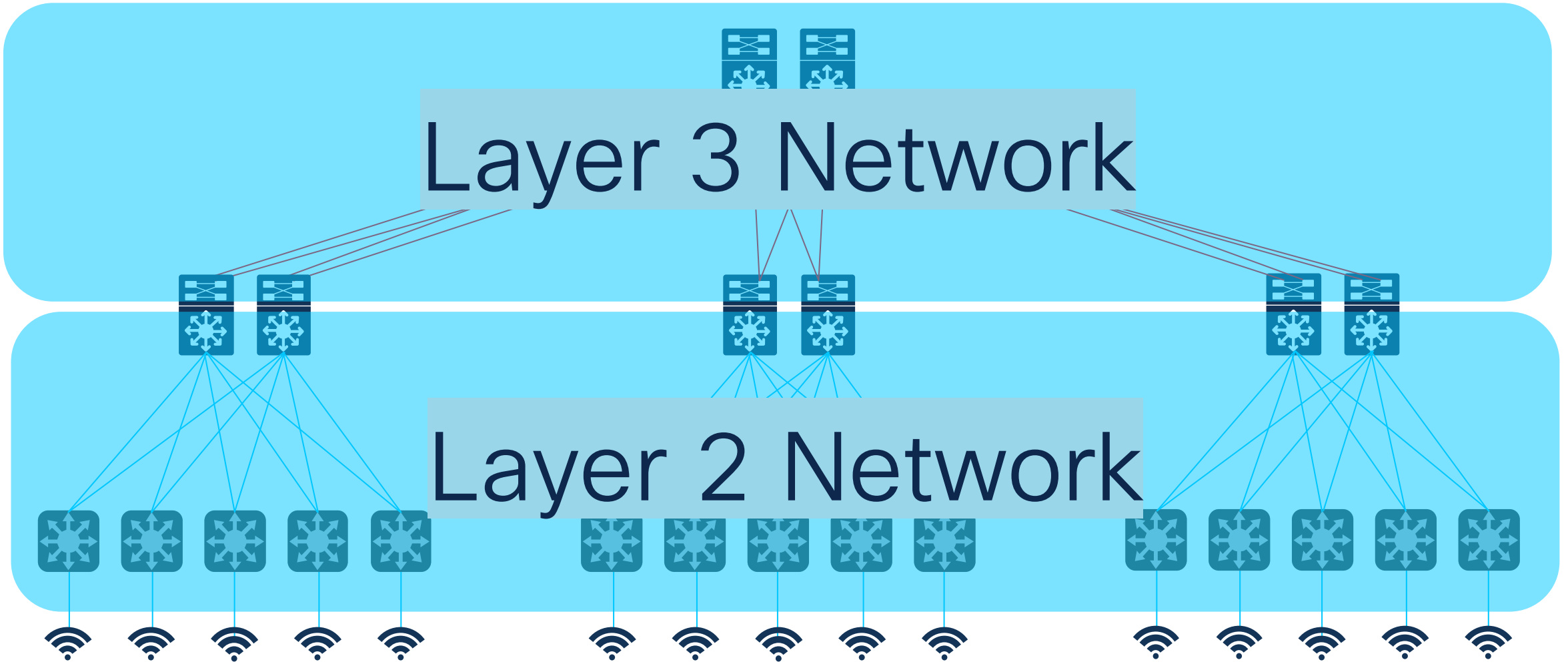
After SD-Access

- Consistent management across wired and wireless
- Optimal traffic flows with seamless roaming
- Policy uniformly enforced regardless of wired or wireless

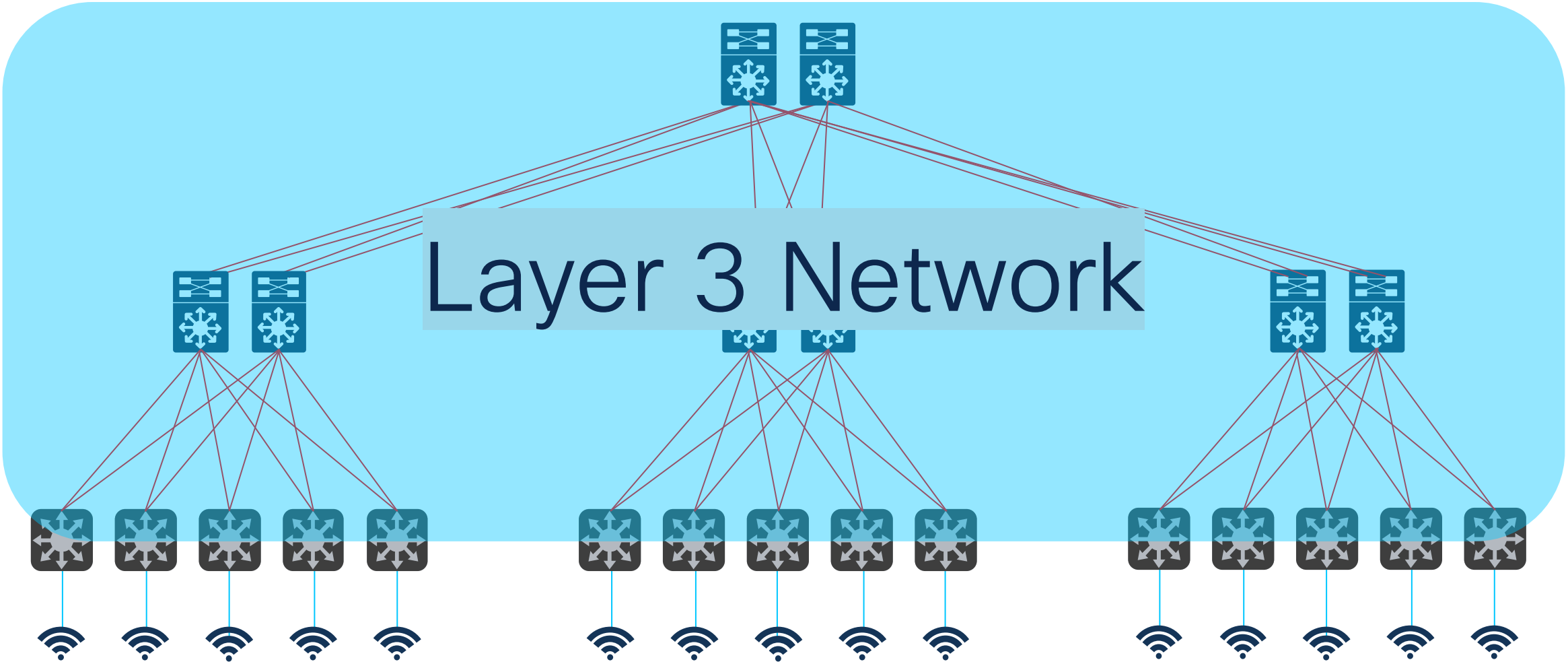
Simplified provisioning | Campus-wide roaming | Wired and wireless consistency

SDA Components

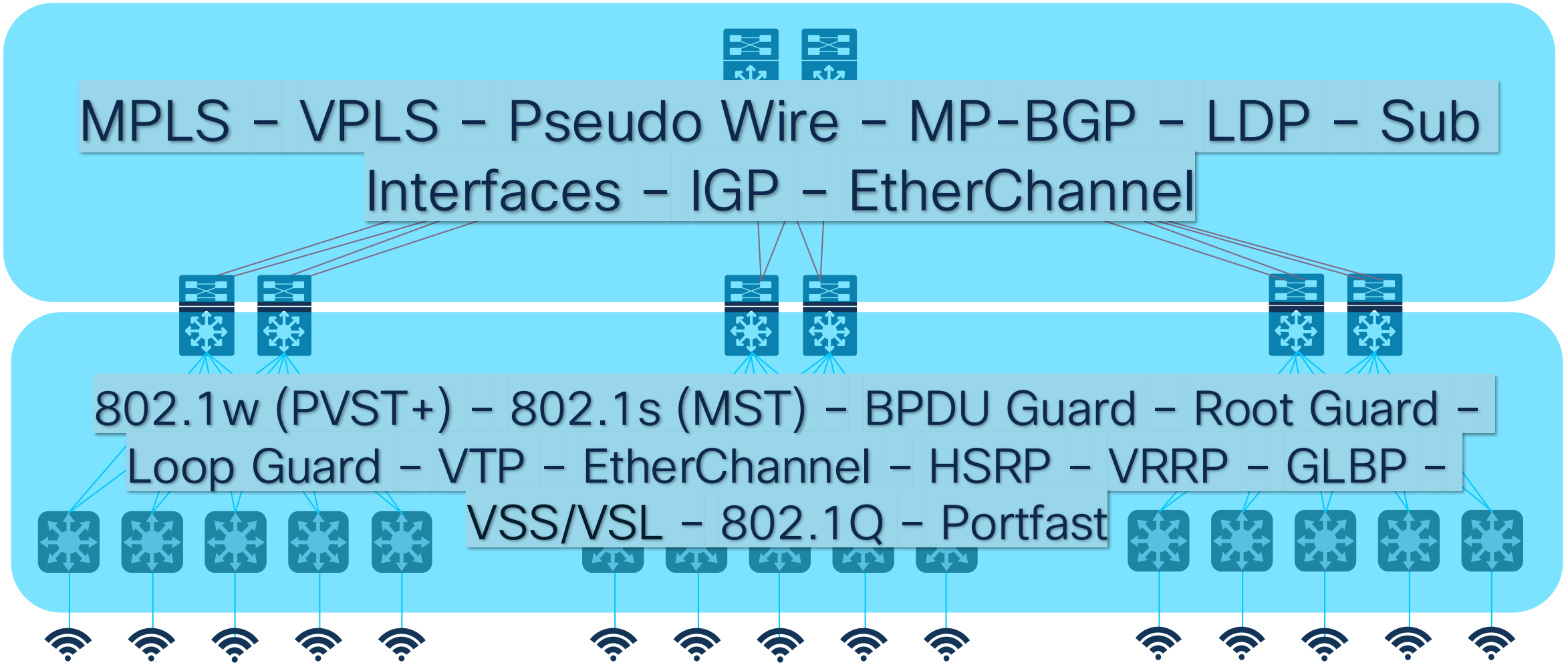
Old Networks



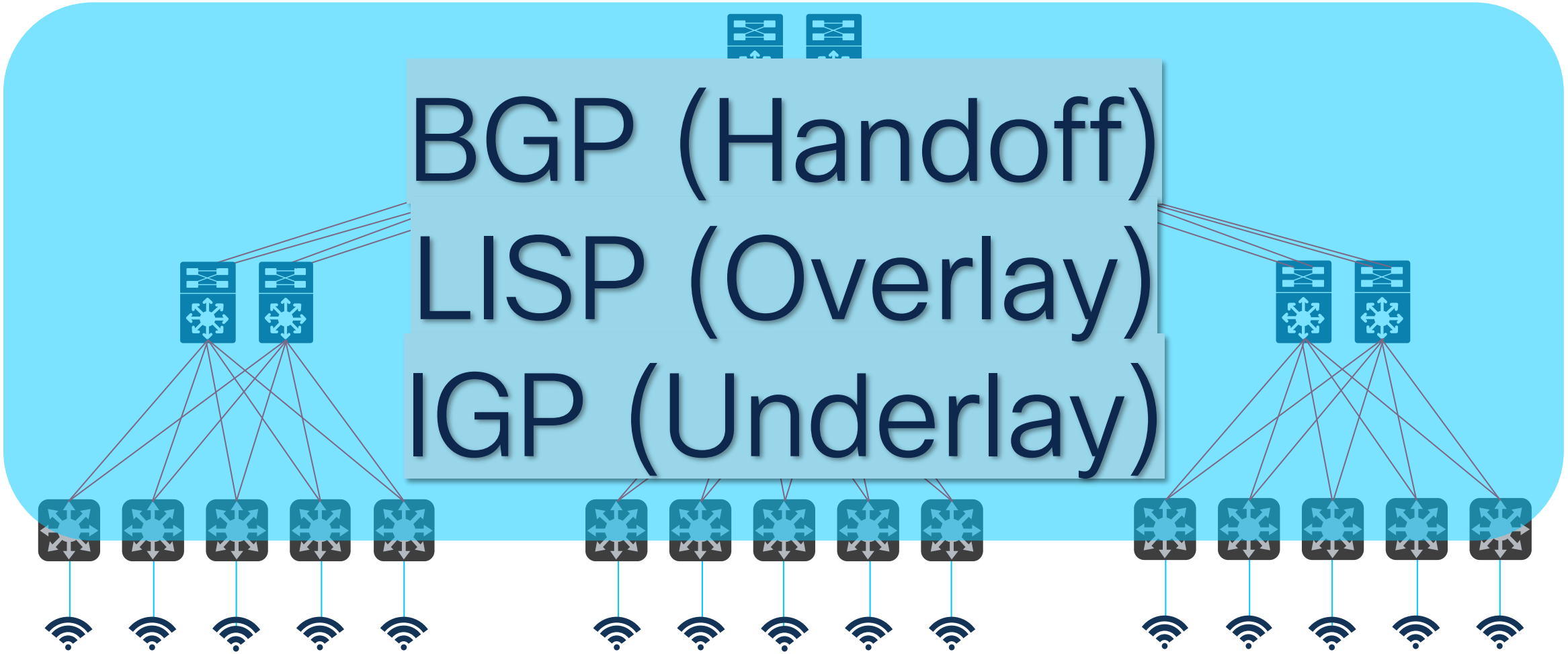
Resilient New Networks with Layer-3 Underlay



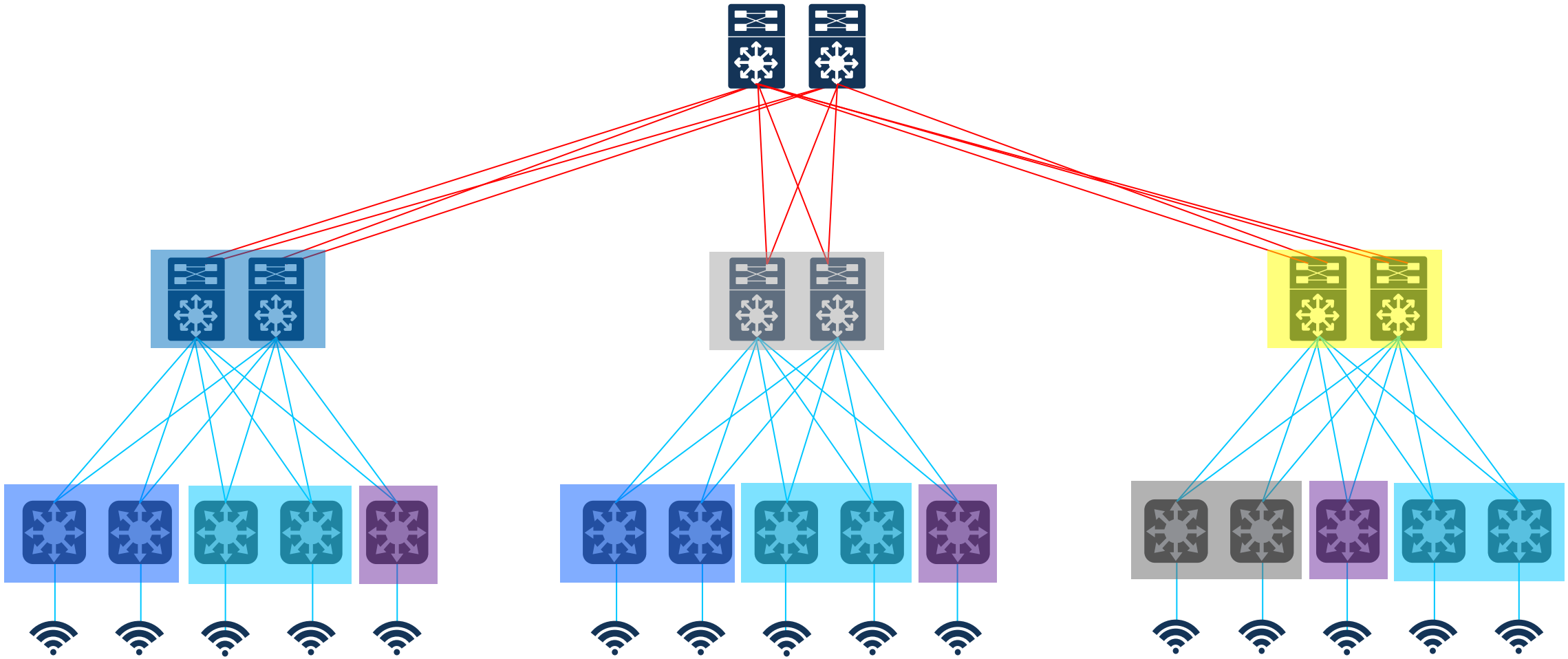
OLD Network Protocol Stacks



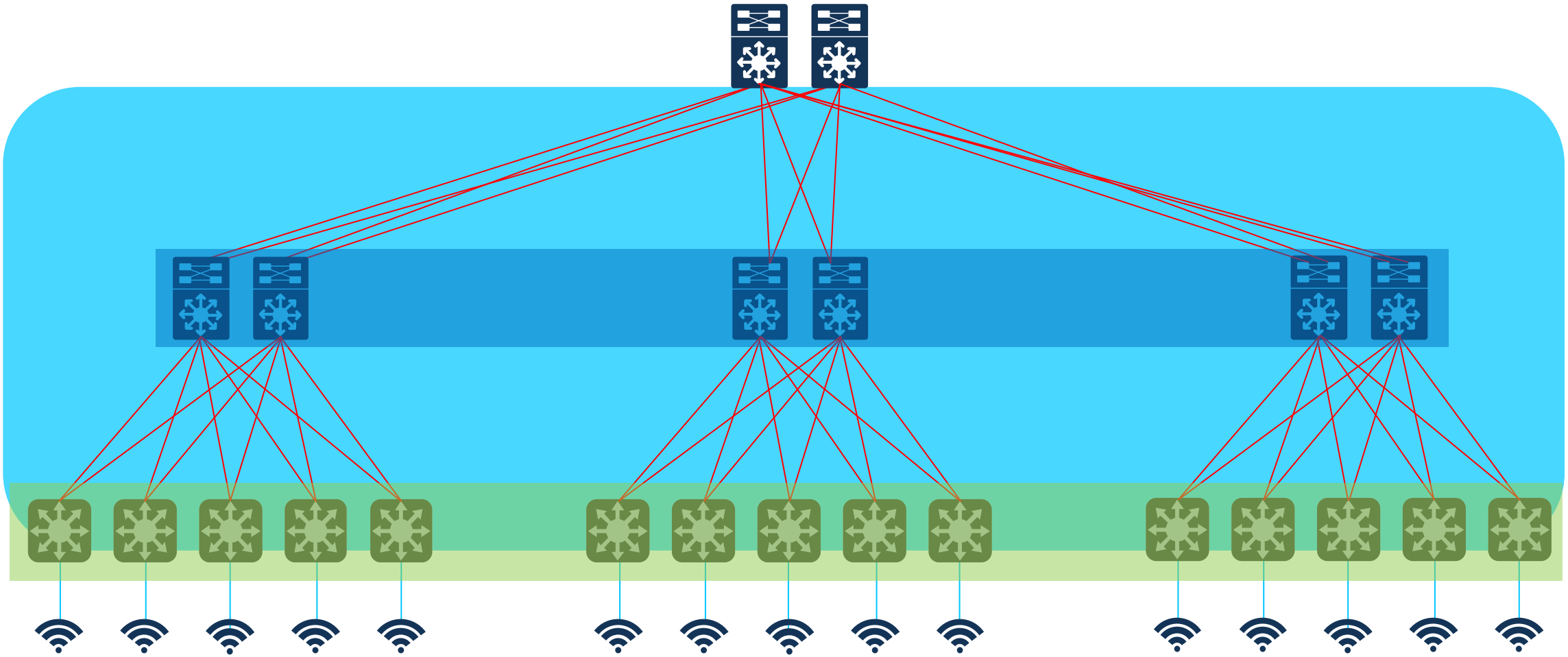
New Network Protocol Stack with Overlay



Unique Configurations in OLD network



Consistent Configurations in New network with Overlay



SD-Access

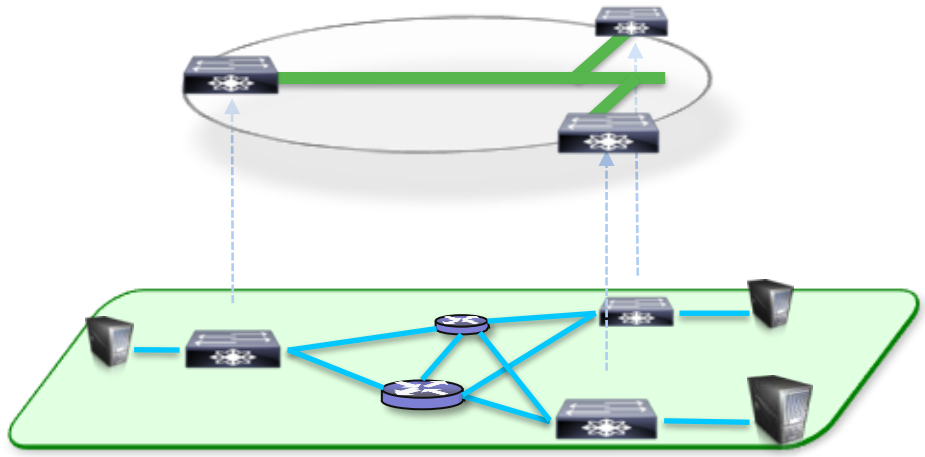
What exactly is a Fabric?

A Fabric is an Overlay

An *Overlay network* is a *logical topology* used to *virtually connect* devices, built *on top* of a simple, physical *Underlay network*.

An *Overlay network* often uses *alternate forwarding attributes* to provide *additional services,* not provided by the *Underlay*.

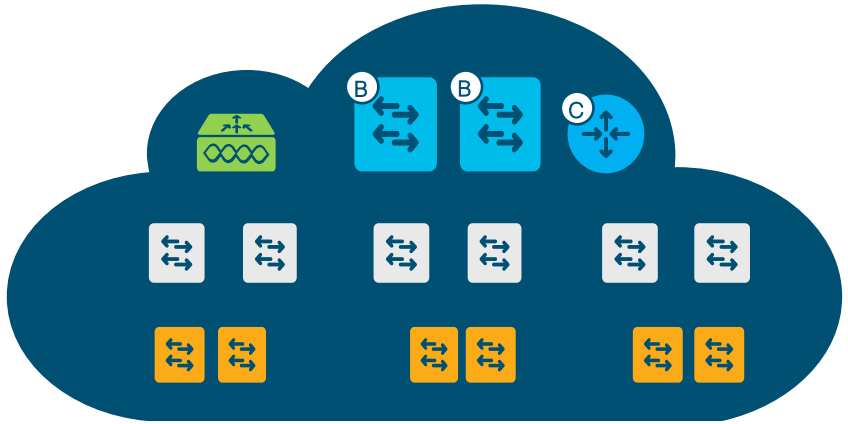
Examples of Network Overlays	
• GRE / mGRE	• LISP
• MPLS / VPLS	• OTV
• IPSec / DMVPN	• FP
• CAPWAP	• ACI



SD-Access

Key Components

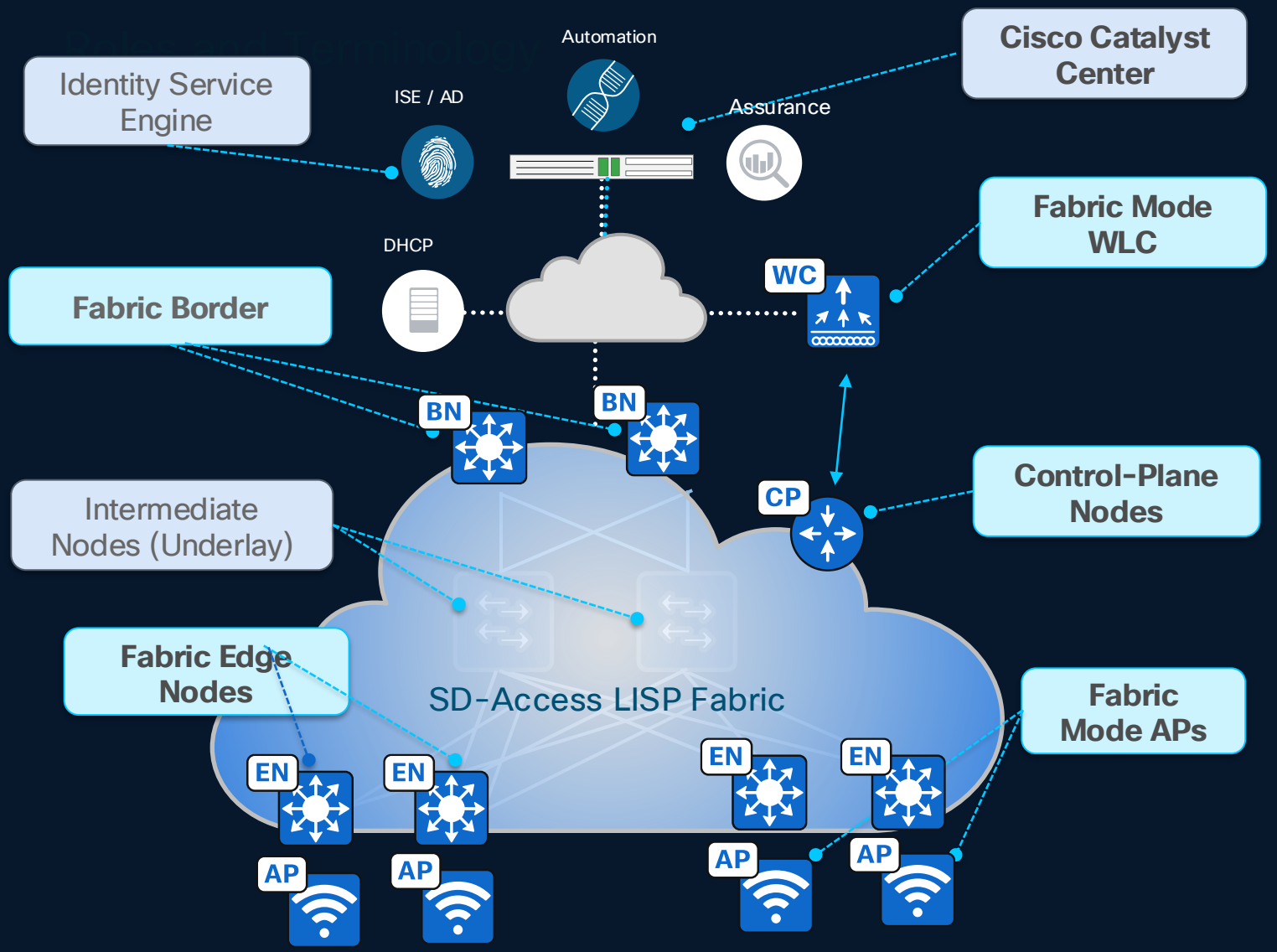
1. **Control-Plane** based on **LISP**
2. **Data-Plane** based on **VXLAN**
3. **Policy-Plane** based on **CTS**



Key Differences

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

SD-Access LISP Fabric Architecture



- **CISCO CATALYST CENTER CONTROLLER** – Enterprise orchestrator and data repository providing intuitive management and network assurance
- **IDENTITY SERVICE ENGINE** – External ID Services for dynamic user/device authorization and group policy management
- **CONTROL-PLANE (CP) NODE** – Mapping System that manages Endpoint ID to Location relationships via LISP 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 from AP to Edge Node
- **Underlay** – Non-fabric network components that serve as foundation for fabric

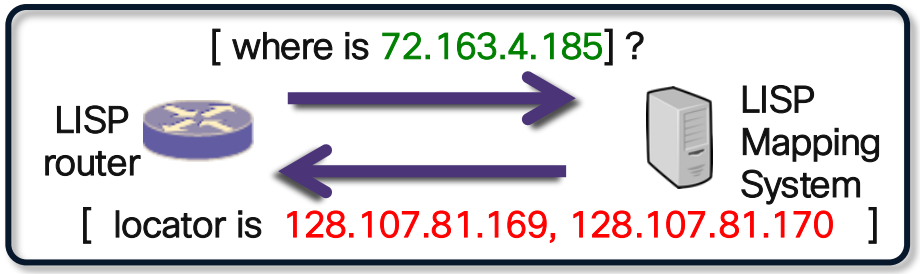
SDA Mechanics

LISP Operations

- LISP is analogous to a DNS lookup
  - DNS resolves IP addresses for URL Answering the "WHO IS" question

DNS
Name-to-IP
URL Resolution

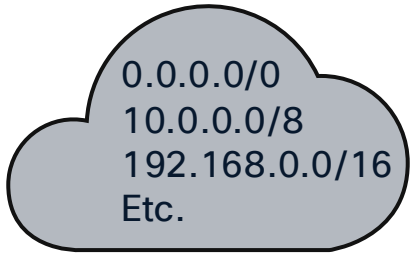
  - LISP resolves locators for queried identities Answering the "WHERE IS" question

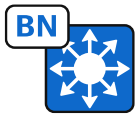


LISP
Identity-to-locator
Mapping Resolution

Fabric Operation

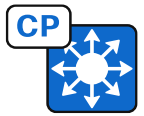
Default ETR Registration





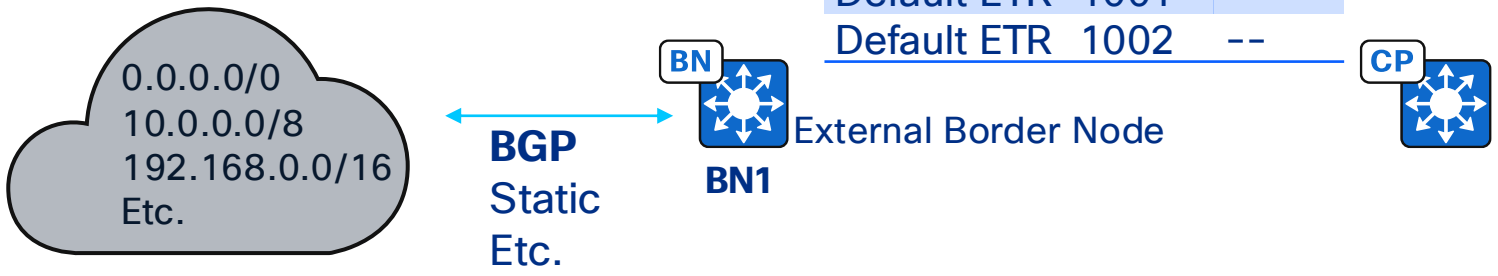
External Border Node

BN1



Fabric Operation

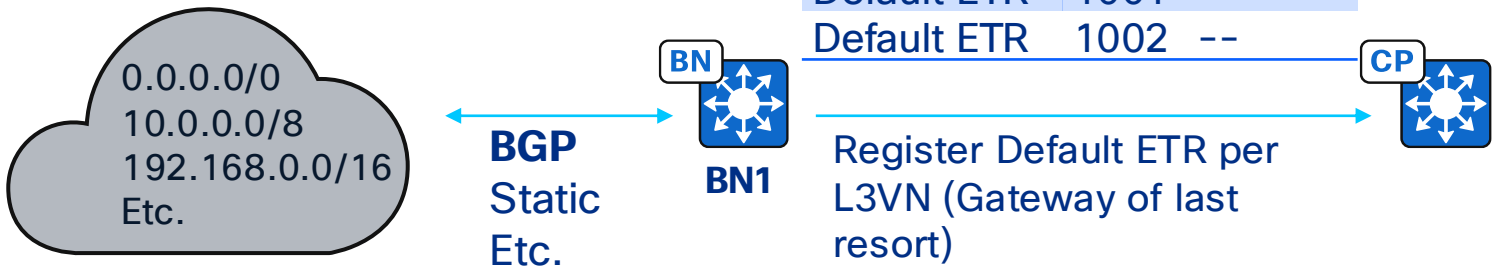
Default ETR Registration



Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

Fabric Operation

Default ETR Registration

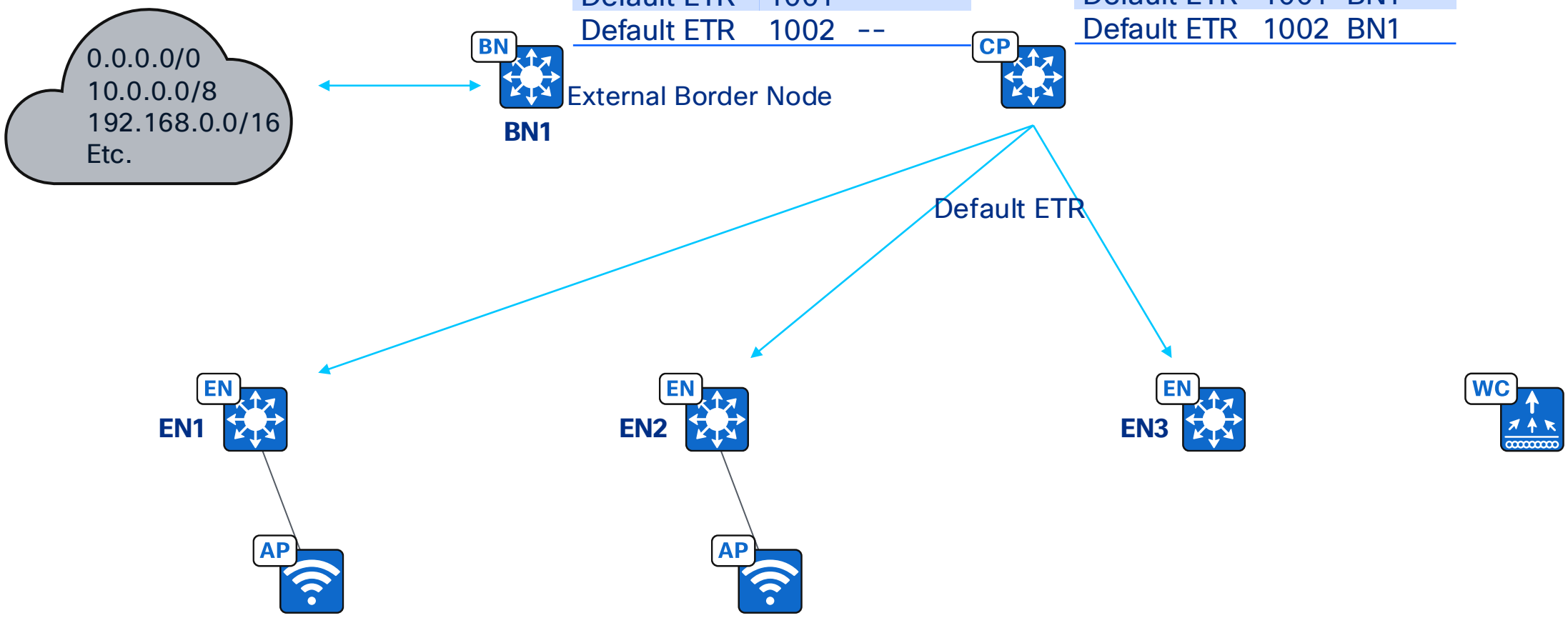


Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

Fabric Operation

Edge Node Bootstrap

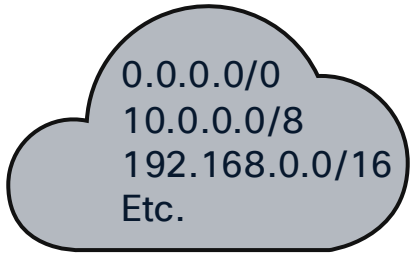


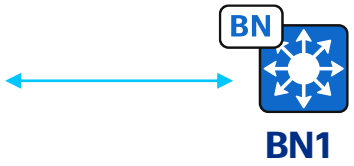
Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

Fabric Operation

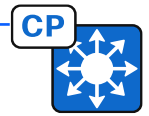
Edge Node Bootstrap





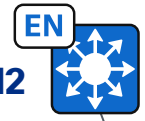
External Border Node

Destination	IID	Next Hop
Default ETR	1001	--
Default ETR	1002	--

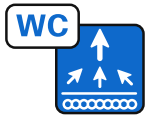


Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1

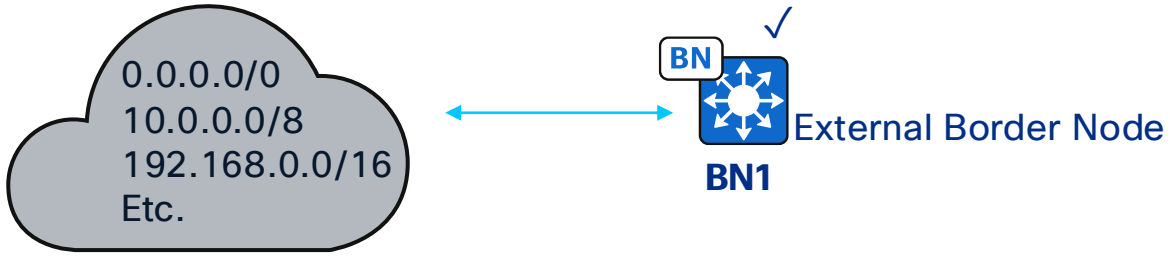


Destination	IID	Next Hop
Default ETR	1001	BN1
Default ETR	1002	BN1



Fabric Operation

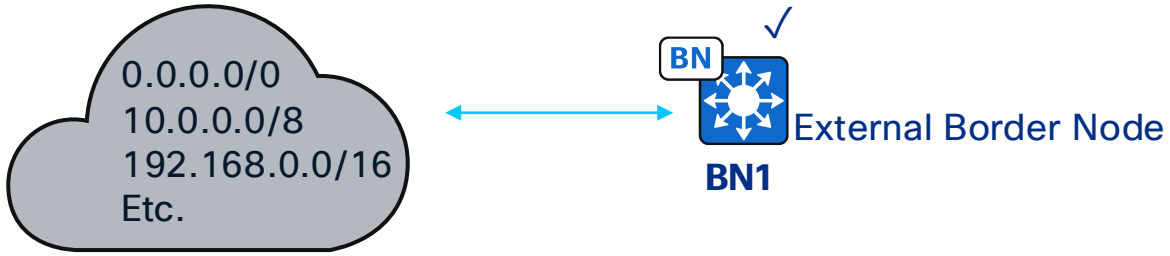
Edge Node Bootstrap

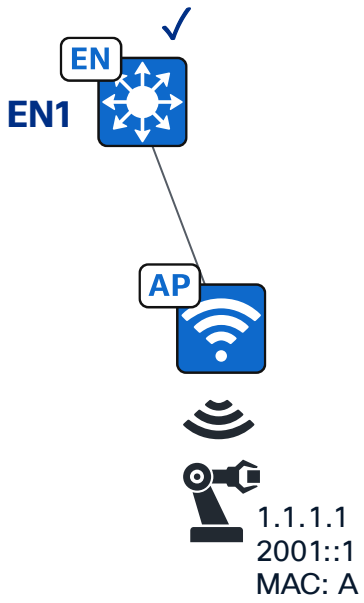


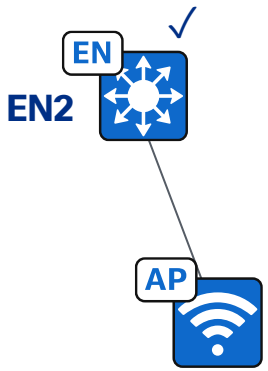
✓ Default ETR

Fabric Operation

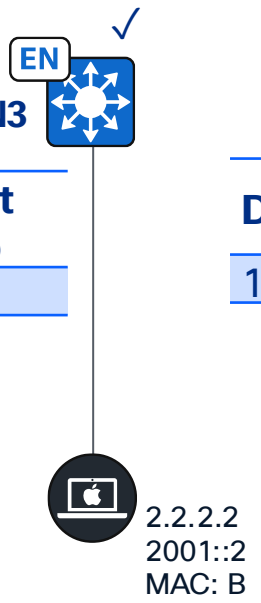
Endpoint Registration

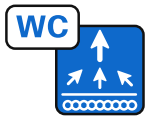






Destination	IID	Next Hop
2.2.2.2	1001	--





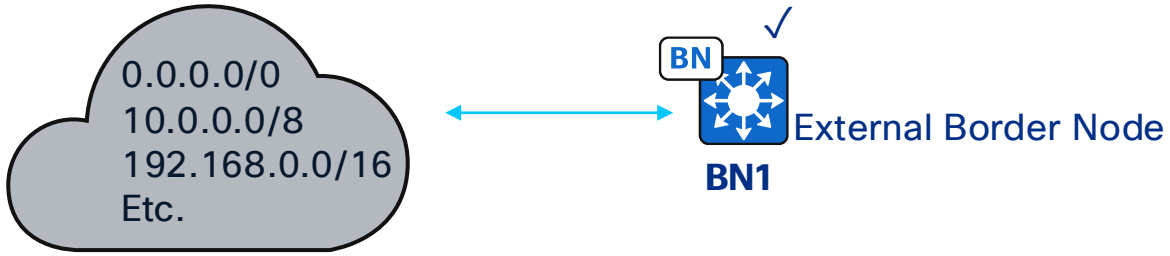
Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

✓ Default ETR

Fabric Operation

Endpoint Registration



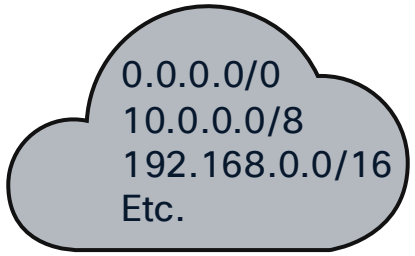
Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

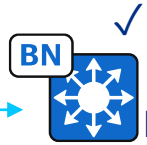
Destination	IID	Next Hop
2.2.2.2	1001	--

Destination	IID	Next Hop
1.1.1.1	1001	EN1

Fabric Operation

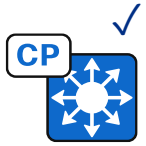
Endpoint Registration





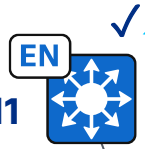
External Border Node

BN1



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

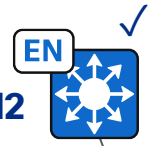
Notification



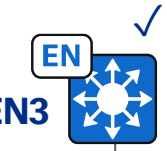
EN1

Destination	IID	Next Hop
1.1.1.1	1001	--

1.1.1.1
2001::1
MAC: A



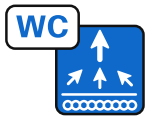
EN2



EN3

Destination	IID	Next Hop
2.2.2.2	1001	--

2.2.2.2
2001::2
MAC: B

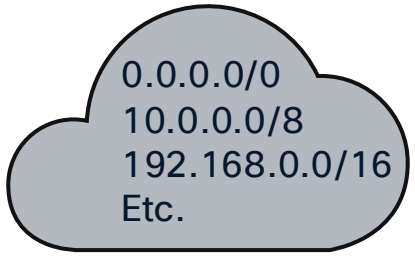


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

Publish



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

BN

BN1

External Border Node

Publish

CP

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

EN1

Destination	IID	Next Hop
1.1.1.1	1001	--

AP

1.1.1.1
2001::1
MAC: A

EN2

AP

EN3

Destination	IID	Next Hop
2.2.2.2	1001	--

2.2.2.2
2001::2
MAC: B

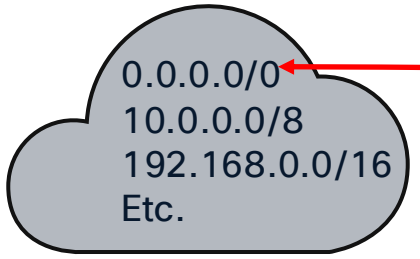
WC

Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

South to North Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

BN

BN1

External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

CP

EN

EN1

Destination	IID	Next Hop
1.1.1.1	1001	--

AP

1.1.1.1
2001::1
MAC: A

EN

EN2

AP

EN

EN3

Destination	IID	Next Hop
2.2.2.2	1001	--

WC

Destination	IID	Next Hop
1.1.1.1	1001	EN1

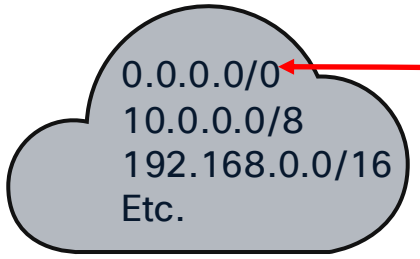
Dst: 8.8.8.8
Src: 2.2.2.2

2.2.2.2
2001::2
MAC: B

✓ Default ETR

Fabric Operation

South to North Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

BN

BN1

External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

CP

Where is 8.8.8.8?

EN

EN1

Destination	IID	Next Hop
1.1.1.1	1001	--

AP

1.1.1.1
2001::1
MAC: A

EN

EN2

AP

EN

EN3

Destination	IID	Next Hop
2.2.2.2	1001	--

WC

Destination	IID	Next Hop
1.1.1.1	1001	EN1

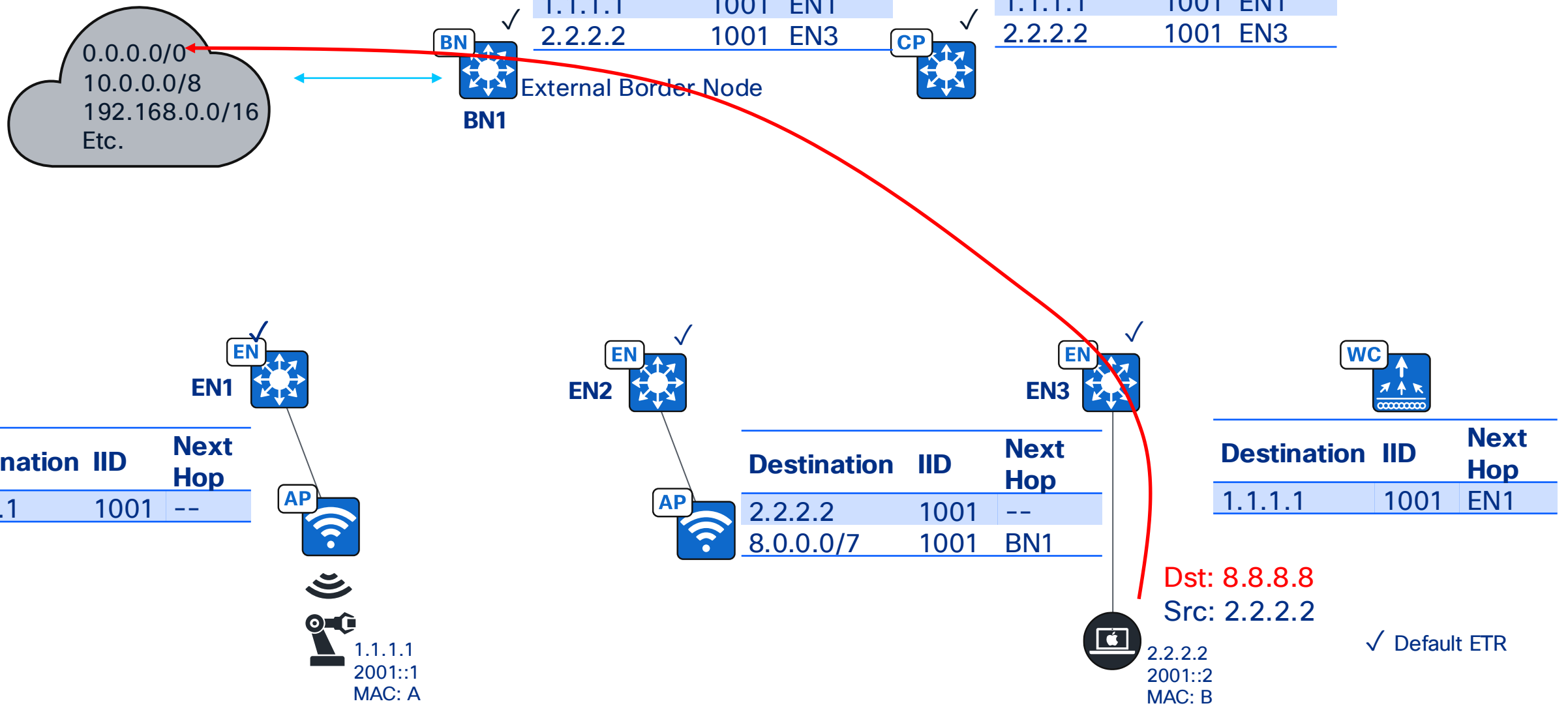
Dst: 8.8.8.8
Src: 2.2.2.2

2.2.2.2
2001::2
MAC: B

✓ Default ETR

Fabric Operation

South to North Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

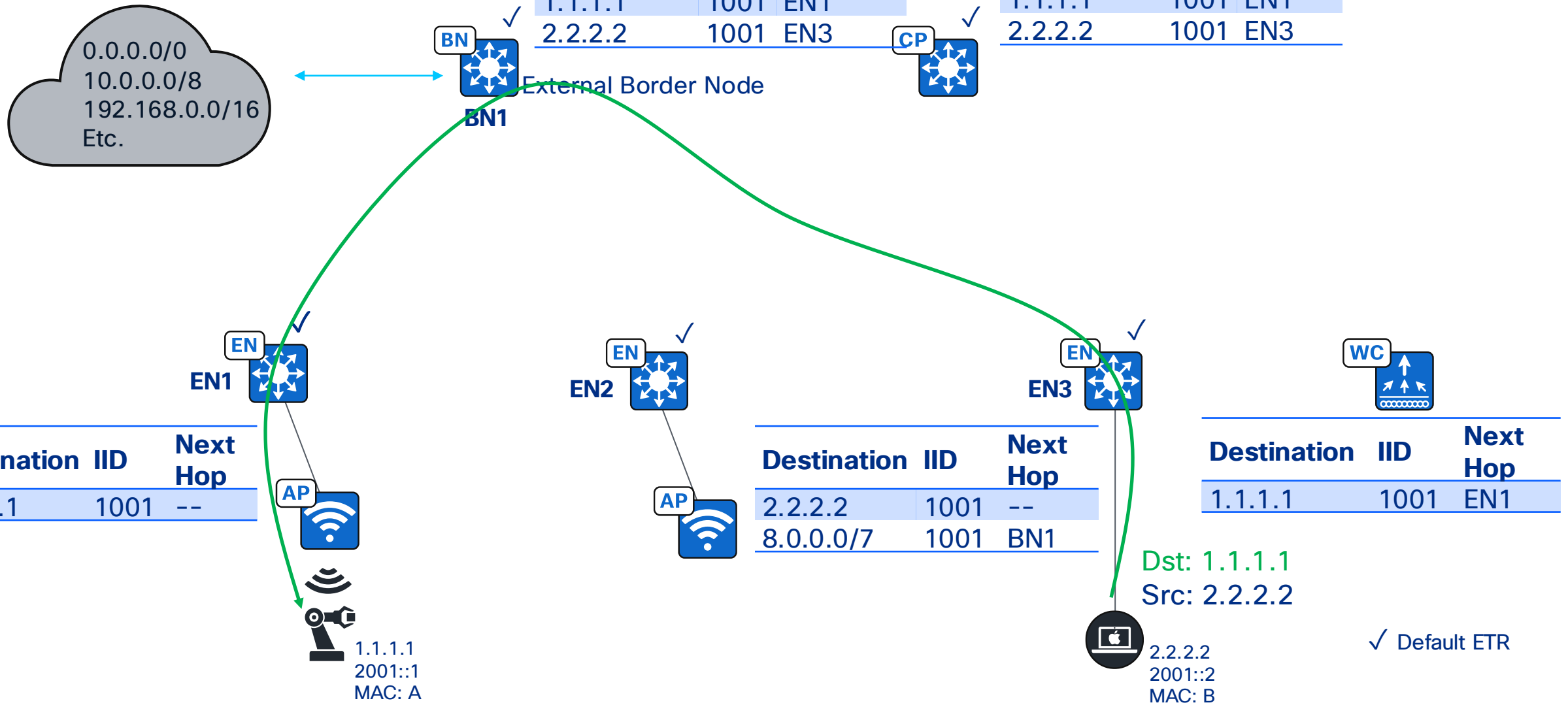
Destination	IID	Next Hop
1.1.1.1	1001	--

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1

Destination	IID	Next Hop
1.1.1.1	1001	EN1

Fabric Operation

East to West Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

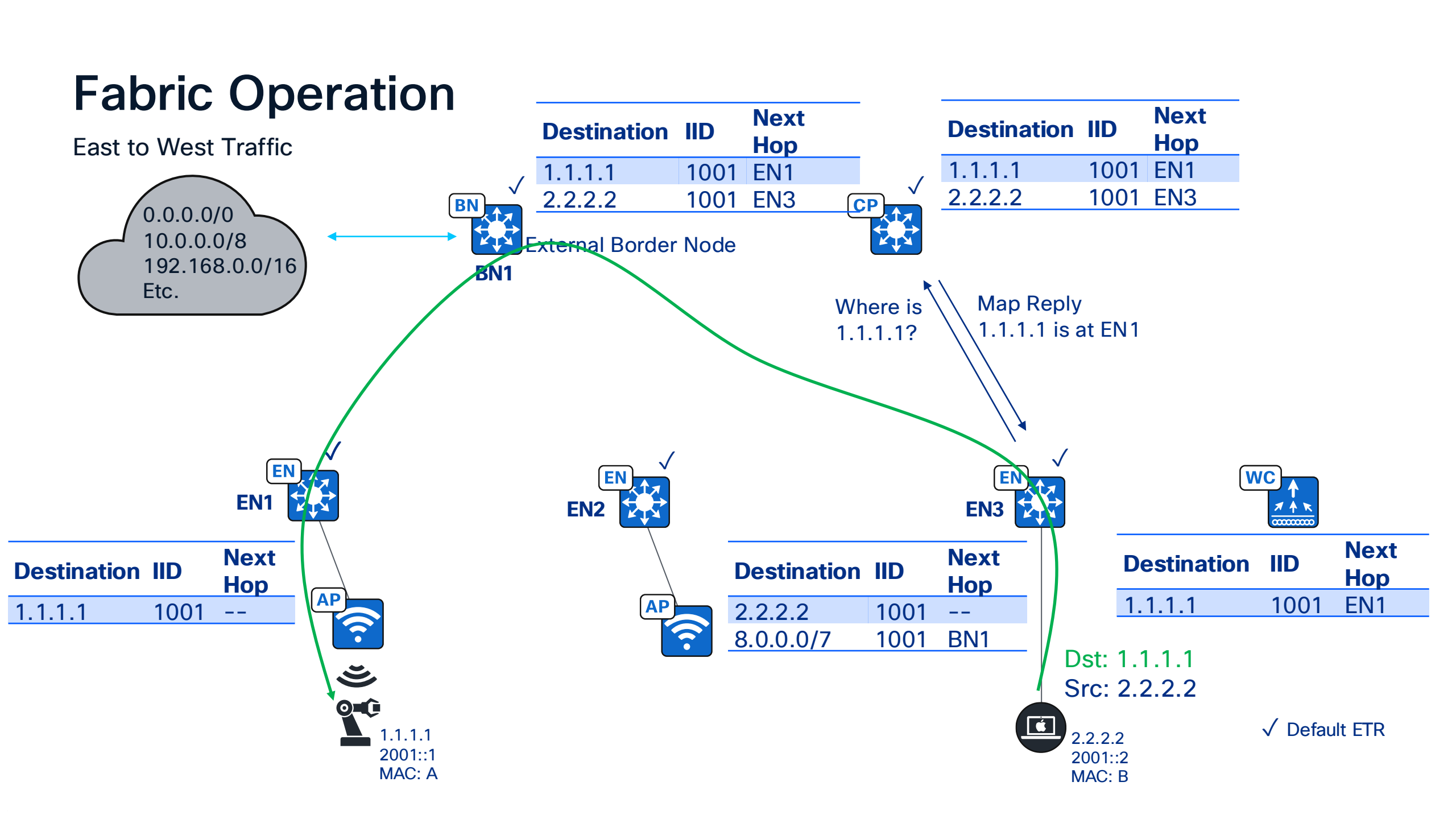
Destination	IID	Next Hop
1.1.1.1	1001	--

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1

Destination	IID	Next Hop
1.1.1.1	1001	EN1

Fabric Operation

East to West Traffic



Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

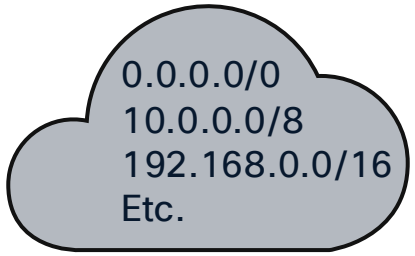
Destination	IID	Next Hop
1.1.1.1	1001	--

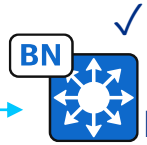
Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1

Destination	IID	Next Hop
1.1.1.1	1001	EN1

Fabric Operation

East to West Traffic

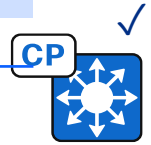




BN1

External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

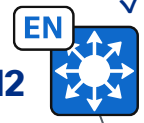


Destination	IID	Next Hop
1.1.1.1	1001	EN1
2.2.2.2	1001	EN3

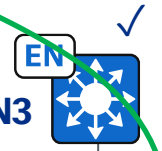
EN1

Destination	IID	Next Hop
1.1.1.1	1001	--

1.1.1.1
2001::1
MAC: A



EN2

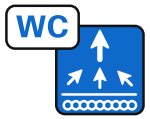


EN3

Destination	IID	Next Hop
2.2.2.2	1001	--
8.0.0.0/7	1001	BN1
1.1.1.1	1001	EN1

Dst: 1.1.1.1
Src: 2.2.2.2

2.2.2.2
2001::2
MAC: B

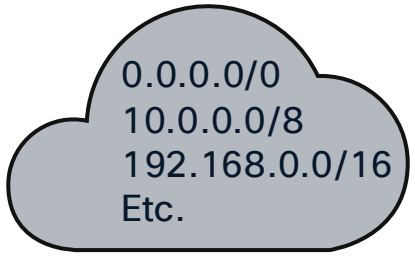


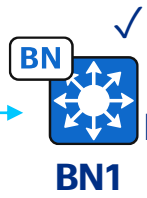
Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

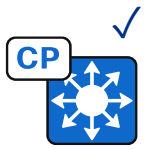
Host Mobility



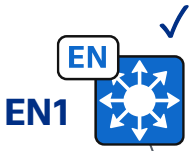


External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN1



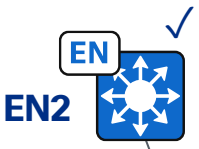
Destination	IID	Next Hop
1.1.1.1	1001	EN1



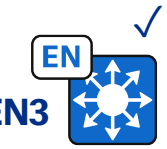
Destination	IID	Next Hop
1.1.1.1	1001	--

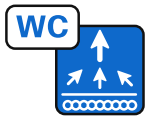
1.1.1.1
2001::1
MAC: A

Host moves to EN2



Destination	IID	Next Hop



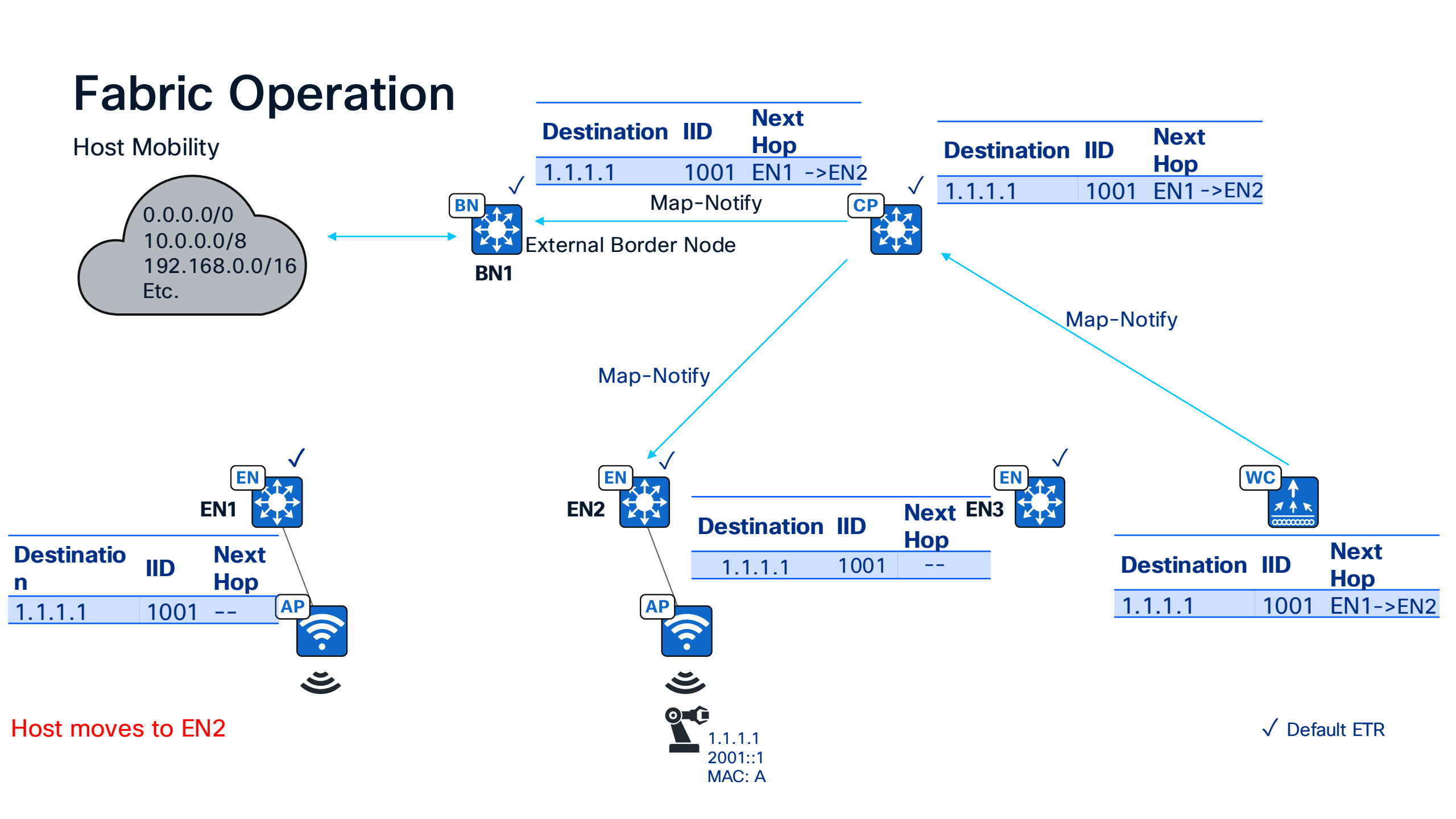


Destination	IID	Next Hop
1.1.1.1	1001	EN1

✓ Default ETR

Fabric Operation

Host Mobility



Destination	IID	Next Hop
1.1.1.1	1001	EN1 ->EN2

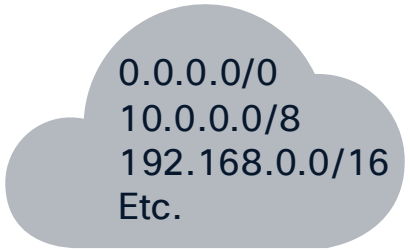
Destination	IID	Next Hop
1.1.1.1	1001	EN1 ->EN2

Destination	IID	Next Hop
1.1.1.1	1001	--

Destination	IID	Next Hop
1.1.1.1	1001	EN1->EN2

Fabric Operation

Host Mobility



BN

BN1

External Border Node

Destination	IID	Next Hop
1.1.1.1	1001	EN2

CP

Destination	IID	Next Hop
1.1.1.1	1001	EN2

Map-Notify
Put EID in Away Table
on EN1

EN

EN1

Destination	IID	Next Hop

AP

EN

EN2

Destination	IID	Next Hop
1.1.1.1	1001	--

AP

1.1.1.1
2001::1
MAC: A

EN

EN3

WC

Destination	IID	Next Hop
1.1.1.1	1001	EN2

Host moves to EN2

✓ Default ETR

Demo

Thank you


CISCO