Your Time Is Now

Cisco Connect

5 - 7 April, 2017

Pula, Croatia

Cisco Campus Fabric Introduction

Vedran Hafner
Systems engineer
Cisco

Campus Fabric
Abstract

Cisco Connect

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

- **Host Mobility** (w/o stretching VLANs)
- **Network Segmentation** (w/o implementing MPLS)
- **Role-based Access Control** (w/o end-to-end TrustSec)

Using Cisco technologies *available today*, you can overcome these challenges and build an “Evolved” Campus Network to better meet your business objectives.

Cisco
Connect

Agenda

1. **Key Benefits**
   Why do I care?
2. **Key Concepts**
   What is a Fabric?
3. **Solution Overview**
   What are the components?
4. **Putting It Together**
   How do I build it?
5. **Use Case**

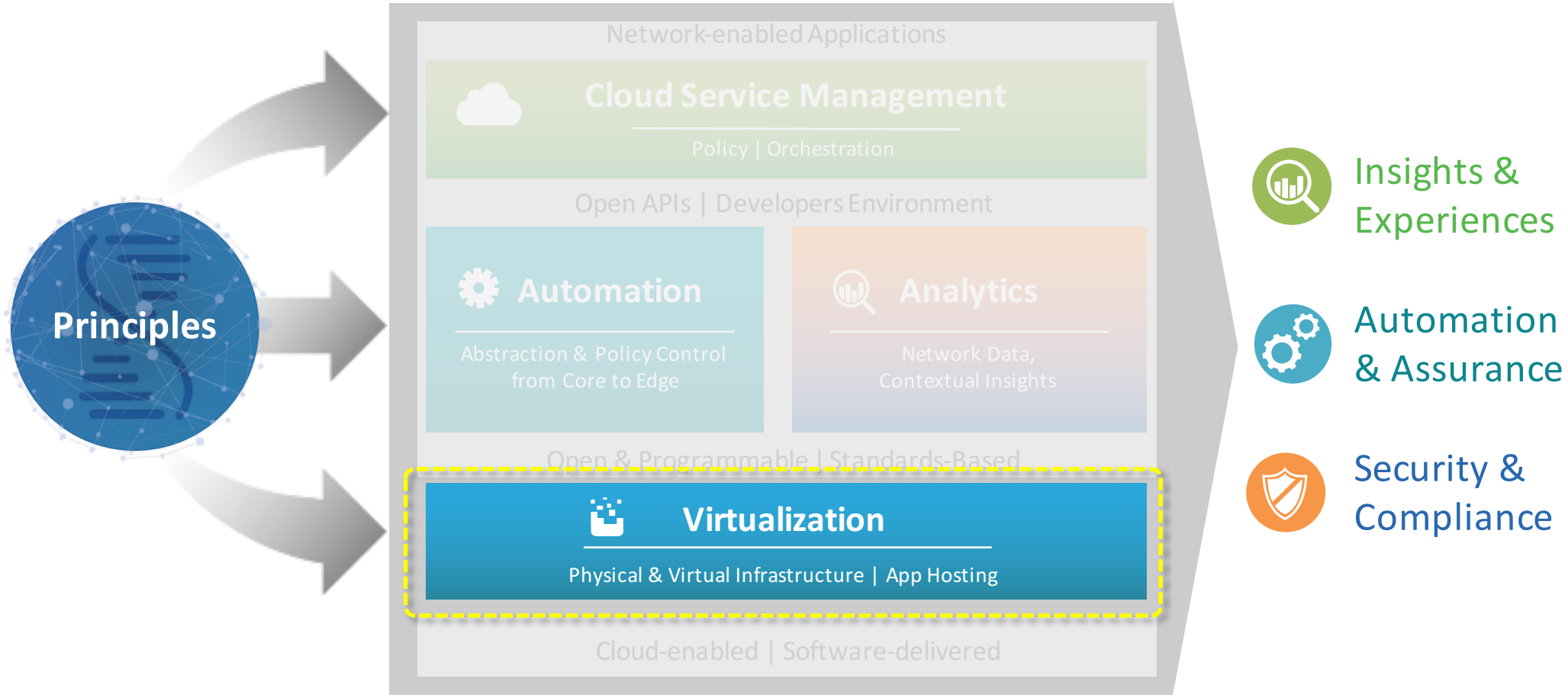
Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Key Benefits
Why do I care ?

Cisco Digital Network Architecture
Overview

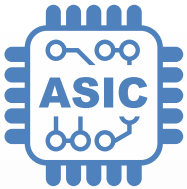
Cisco Connect



Campus Fabric Foundational Technologies

Cisco Connect

Programmable Custom ASICs



Industry Leading

Wired and Wireless | Stacking | TrustSec | SDN

Advanced Functionality

Programmable Pipeline | **Flexibility** | Recirculation

Optimized for Campus

Integrated Stacking | Visibility | **Security**

Future Proofed

Long Life Cycle | **Investment Protection**

+

Converged Software Services

Network Enabled Applications

Collaboration | Mobility | IoT | **Security**

Automation

Programmable | Open

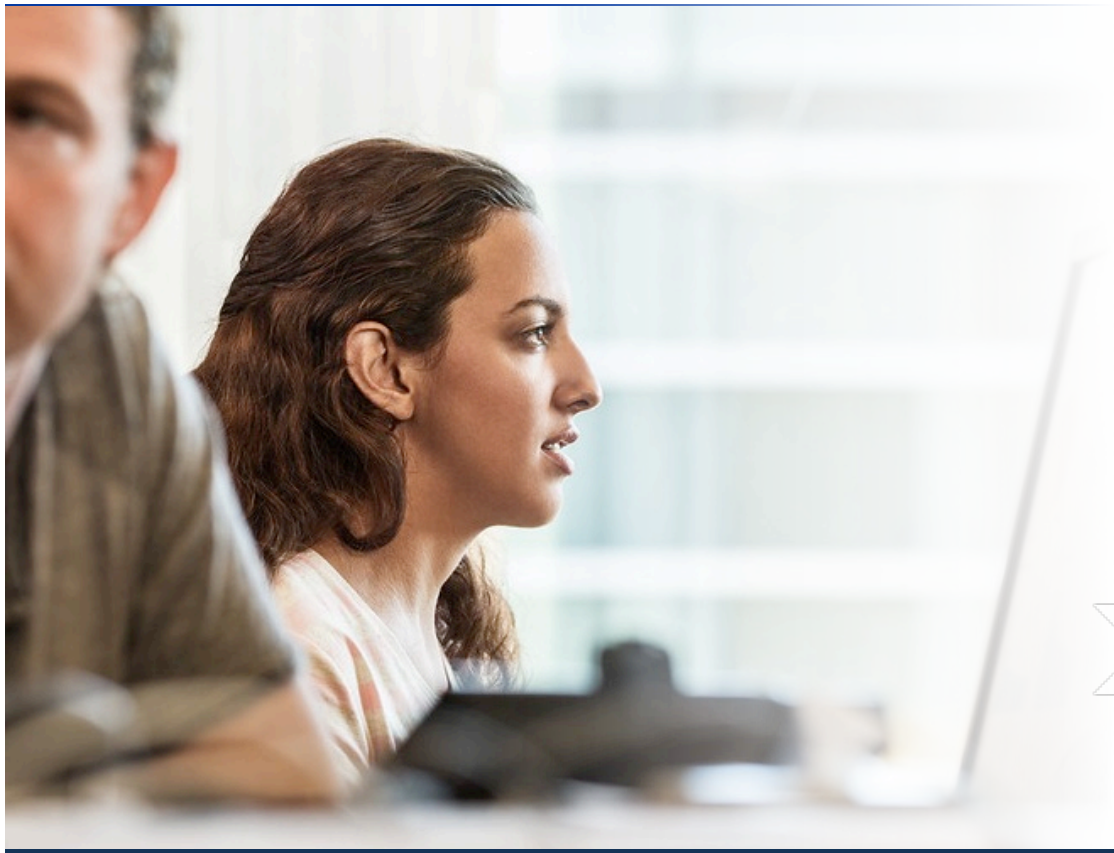
Virtualization

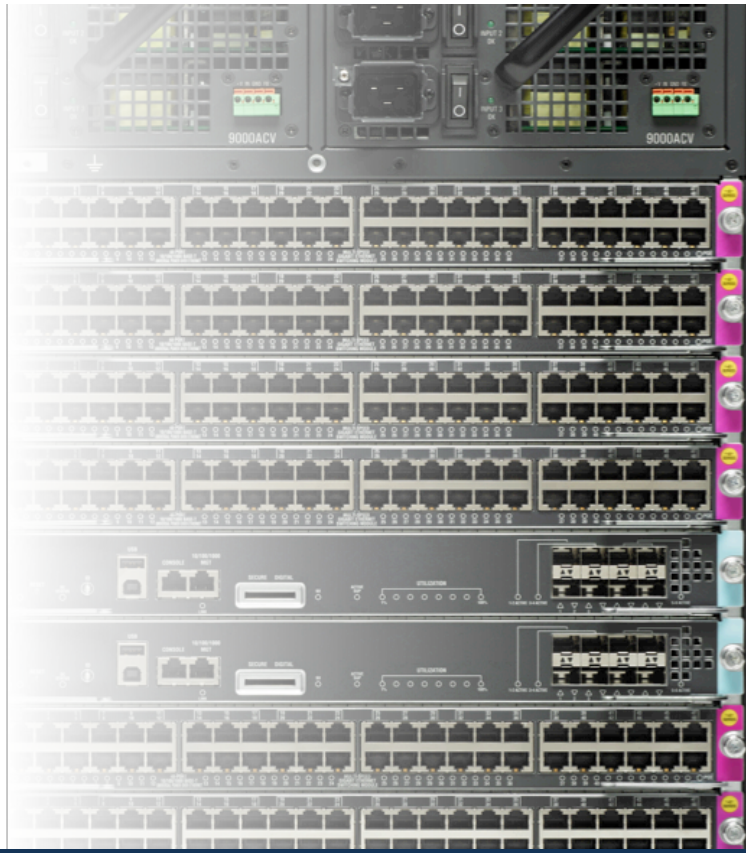
Campus Fabric | **Segmentation** | L2 Flexibility

Designed for Evolution

Strong Foundational Capabilities | **HA**

Driving Innovation Through Technology Investment





Provision

Simplified Provisioning

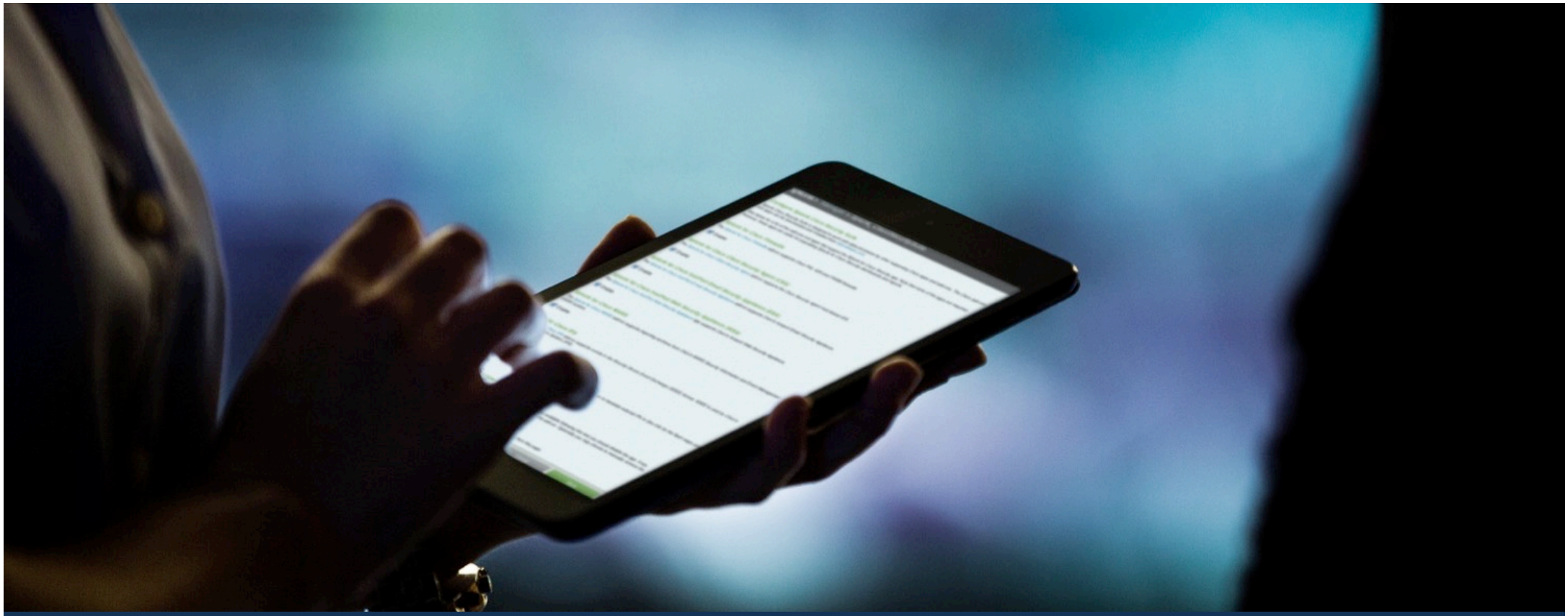
Deploy devices using “best practice” configurations using models and Smart CLI

Segmentation

Security

Simple **Segmentation** constructs

to build **Secure** boundaries for “users and things”

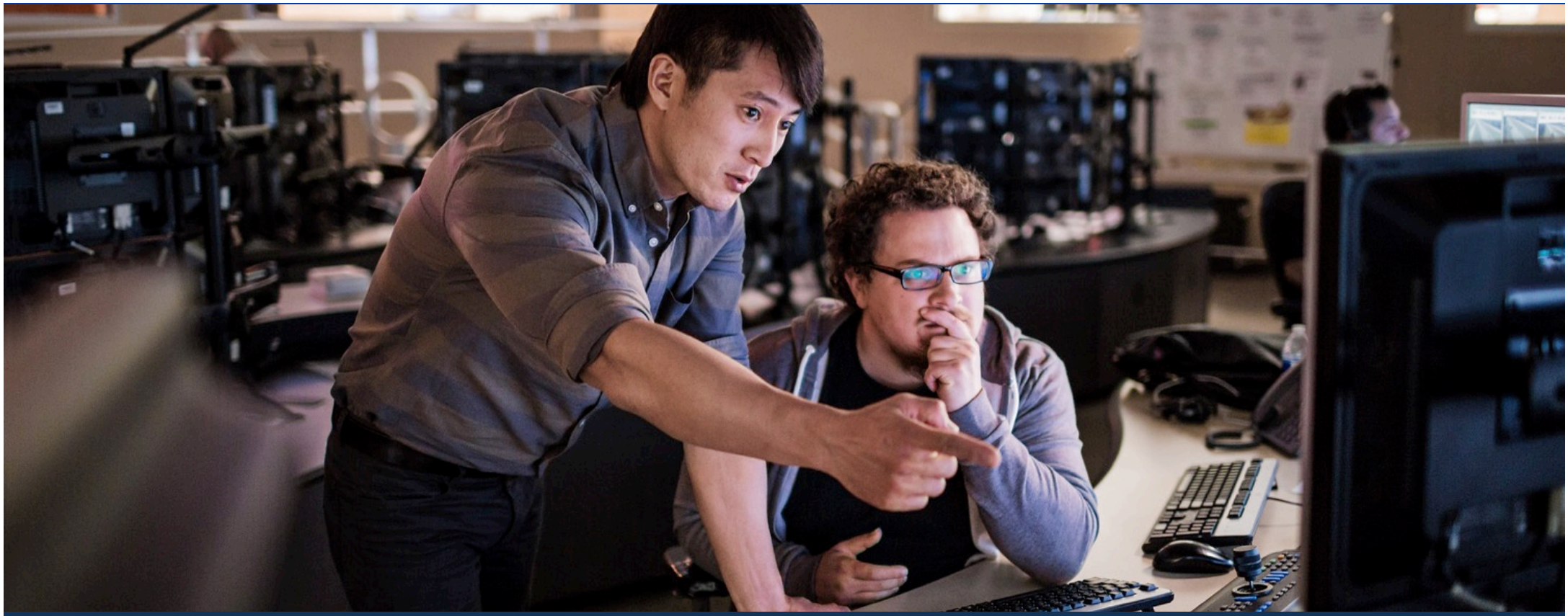


Mobility

Wired and Wireless

Host Mobility

because your address is no longer tied to your location



Intelligent Policy

Network Wide

Policy Enforcement

based on your identity, not on your address

Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Key Concepts
What is a Fabric?

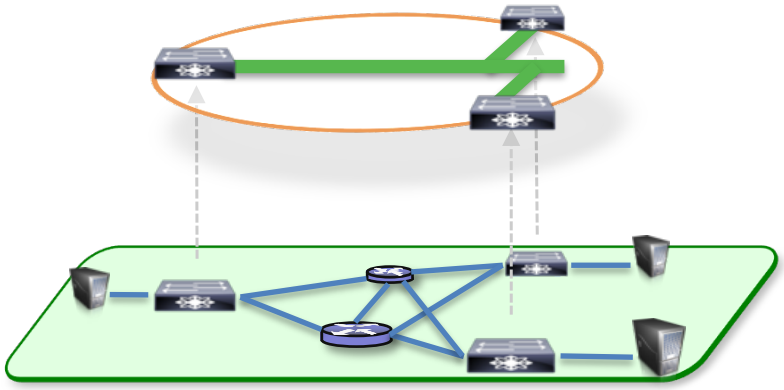
A **Fabric** is an **Overlay**

An “Overlay” is a *logical topology* used to *virtually connect* devices, built *on top* of an 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

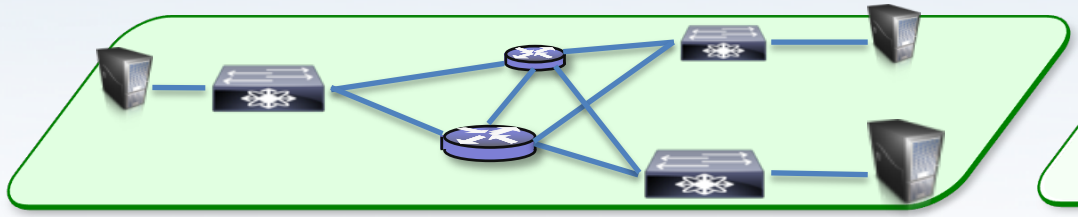


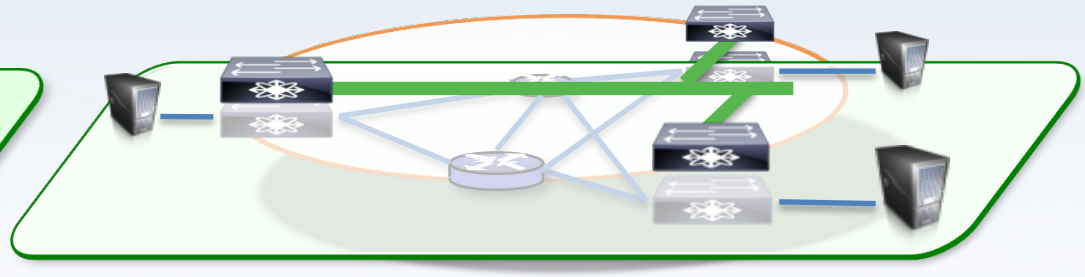
What exactly is a Fabric?

Why Overlays?

Cisco Connect

Separate the Forwarding Plane from the Services Plane





Simple Transport Forwarding

- Physical Devices and Paths
- Intelligent Packet Handling
- Maximize Network Availability
- Simple and Manageable

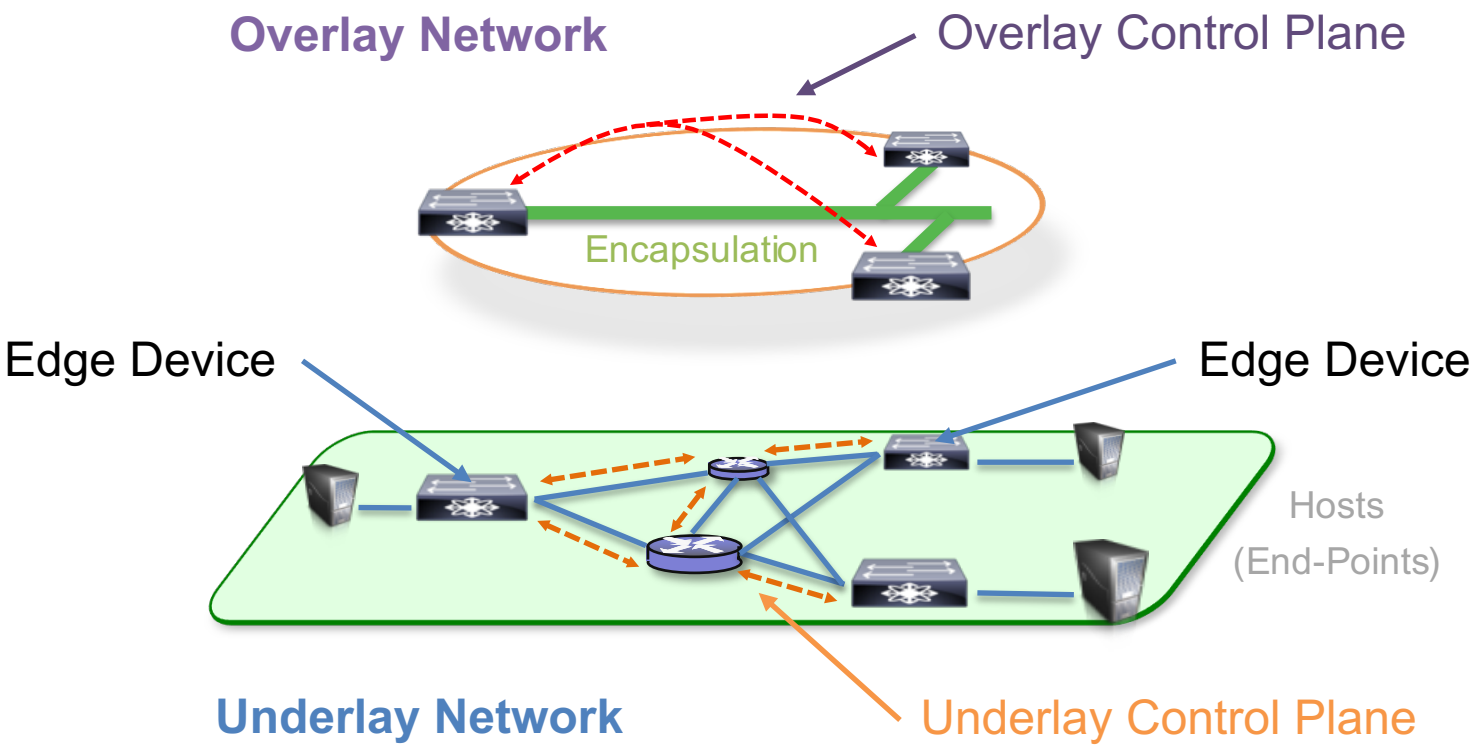
Flexible Virtual Services

- Mobility – Track End-points at Edges
- Scalability – Reduce core state
  - Distribute state to network edge
- Flexibility and Programmability
  - Reduced number of touch points

What exactly is a Fabric?

Overlay Terminology

Cisco Connect

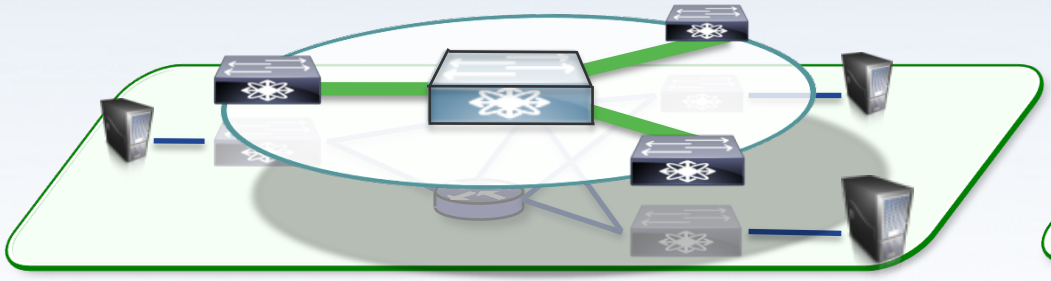


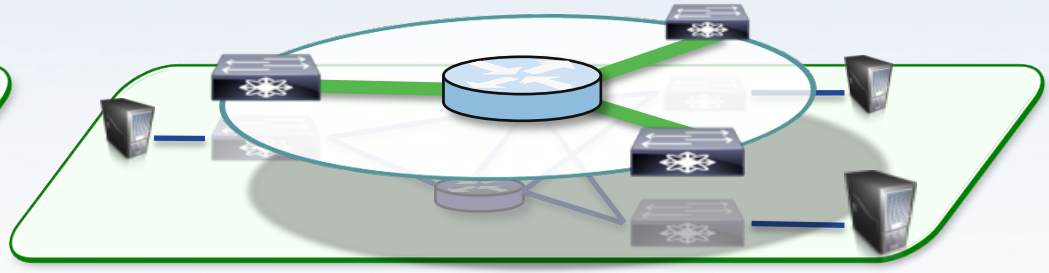
What exactly is a Fabric?

Types of Overlays

Cisco Connect

Hybrid L2 + L3 Overlays offer the Best of Both Worlds





Layer 2 Overlays

- Emulates a LAN segment
- Transport Ethernet Frames (IP & Non-IP)
- Single subnet mobility (L2 domain)
- Exposure to Layer 2 flooding
- Useful in emulating physical topologies

Layer 3 Overlays

- Abstract IP connectivity
- Transport IP Packets (IPv4 & IPv6)
- Full mobility regardless of Gateway
- Contain network related failures (floods)
- Useful to abstract connectivity and policy

What is unique about Campus Fabric?
Key Differences

Cisco Connect

1. **LISP based Control-Plane**
2. **VXLAN based Data-Plane**
3. **Integrated Cisco TrustSec**

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)

Campus Fabric
New Terminology

Cisco Connect

- "**Control-Plane Node**" ≈ "LISP Map-Server"
- "**Edge Node**" ≈ "LISP Tunnel Router" (xTR)
- "**Border Node**" ≈ "LISP Proxy Tunnel Router" (PxTR)
- "**Intermediate Node**" ≈ "Non-LISP IP Forwarder"

Campus Fabric Overview
New Terminology

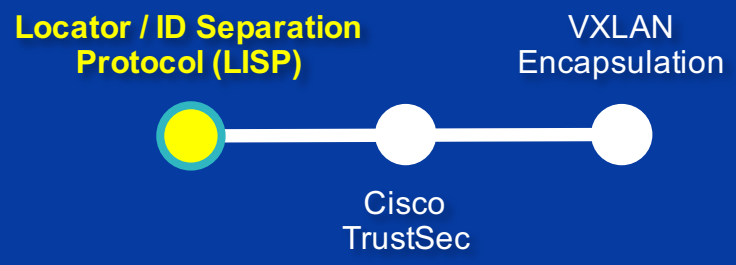
Cisco Connect

- "**Fabric Domain**" ≈ "FD" ≈ "LISP Process"
- "**Virtual Network**" ≈ "VN" ≈ "LISP Instance" ≈ "VRF"
- "**Endpoint ID Group**" ≈ "EIG" ≈ "Segment" ≈ "SGT"
- "**Host Pool**" ≈ "Dynamic EID" ≈ "VLAN + IP Subnet"

Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Solution Overview
What are the components ?



What is LISP?

Locator/ID Separation Protocol (LISP)

Cisco Connect

A routing Architecture

Separate address spaces for Identity and Location

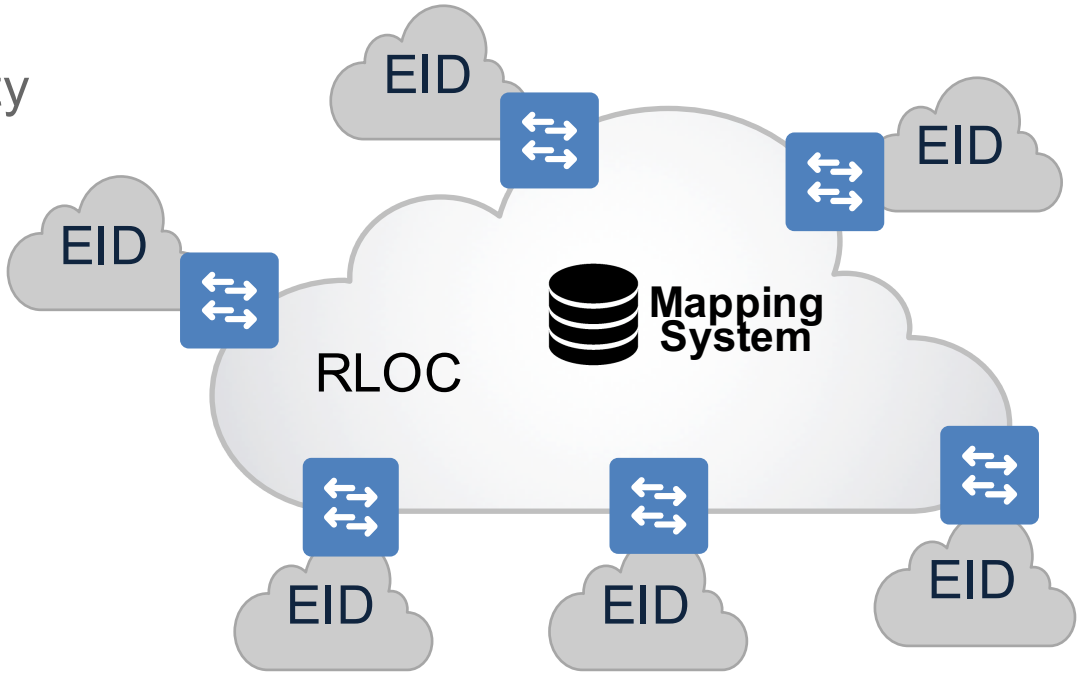
- End-point Identifiers (EID)
- Routing locators (RLOC)

A Control Plane Protocol

A system that maps end-point identities to their current location (RLOC)

A Data Plane Protocol

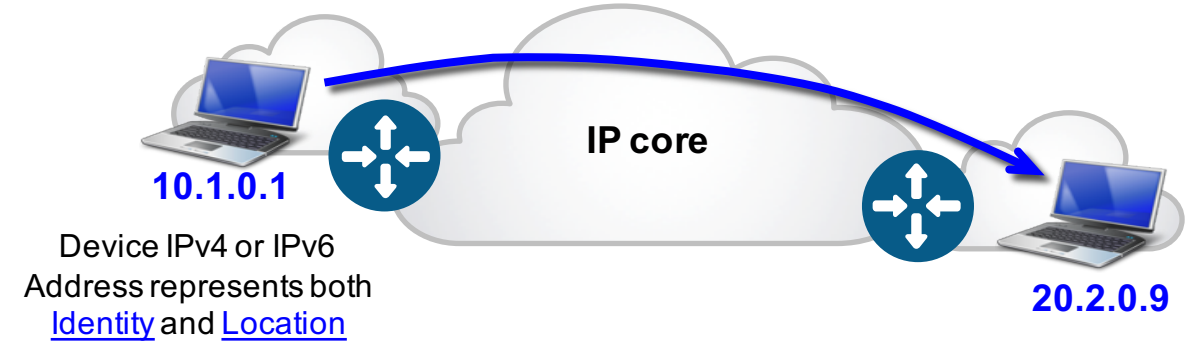
Encapsulates EID-addressed packets inside RLOC-addressed headers



Locator / ID Separation Protocol

Location and Identity Separation

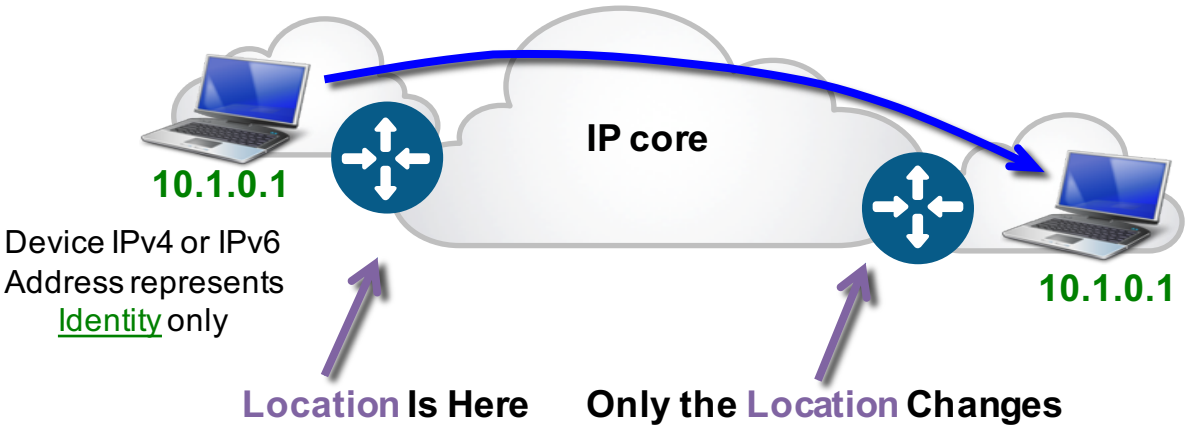
Cisco Connect



Device IPv4 or IPv6 Address represents both Identity and Location

Traditional Behavior -

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



Device IPv4 or IPv6 Address represents Identity only

Location Is Here

Only the Location Changes

Overlay Behavior -

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

How is LISP used in Campus Fabric?

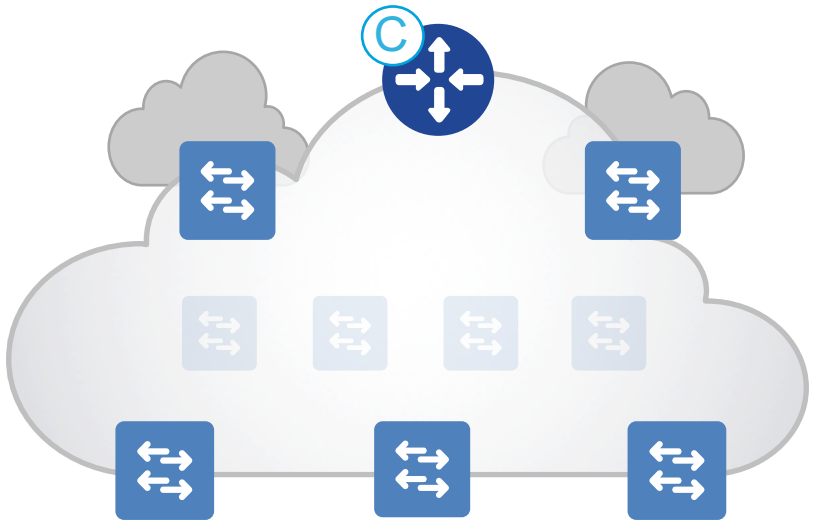
Campus Fabric
Control-Plane Nodes – A Closer Look

Cisco Connect

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

Runs the LISP Host Tracking Database to provide overlay reachability information

- A simple Host Database, that tracks Endpoint ID to Edge Node bindings, along with other attributes
- Host Database supports multiple Endpoint ID lookup keys (**IPv4 /32**, IPv6 /128 or MAC)
- Receives prefix registrations from Edge Nodes with local Endpoints
- Resolves lookup requests from remote Edge Nodes, to locate local Endpoints



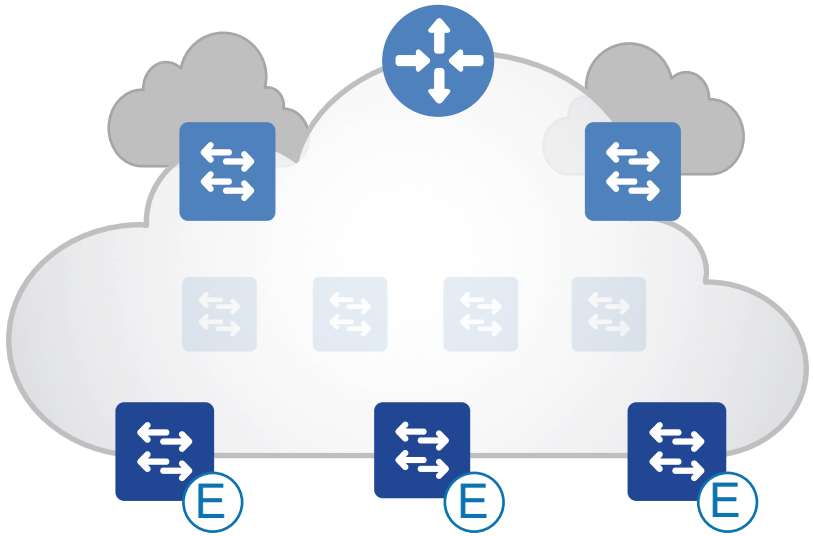
Campus Fabric
Edge Nodes – A Closer Look

Cisco Connect

Fabric Edge Node is based on a LISP Tunnel Router (xTR)

Provides connectivity for Users and Devices connected to the Fabric

- Responsible for Identifying and Authenticating Endpoints
- Register Endpoint ID information with the Control-Plane Node(s)
- Provides Anycast L3 Gateway for connected Endpoints
- Must encapsulate / decapsulate host traffic to and from Endpoints connected to the Fabric



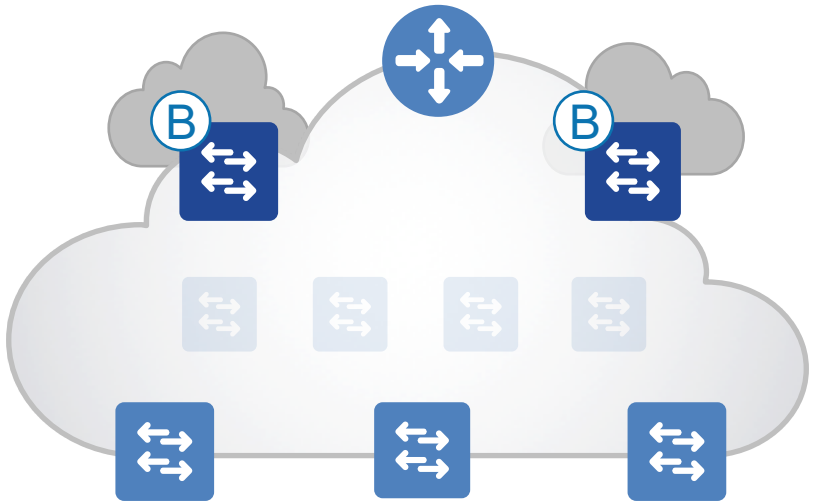
Campus Fabric
Border Nodes – A Closer Look

Cisco Connect

Fabric Border Node is based on a LISP Proxy Tunnel Router (PxTR)

All traffic entering or leaving the Fabric goes through this type of node

- Connects traditional L3 networks and / or different Fabric domains to the local domain
- Where two domains exchange Endpoint reachability and policy information
- Responsible for translation of context (VRF and SGT) from one domain to another
- Provides a domain exit point for all Edge Nodes



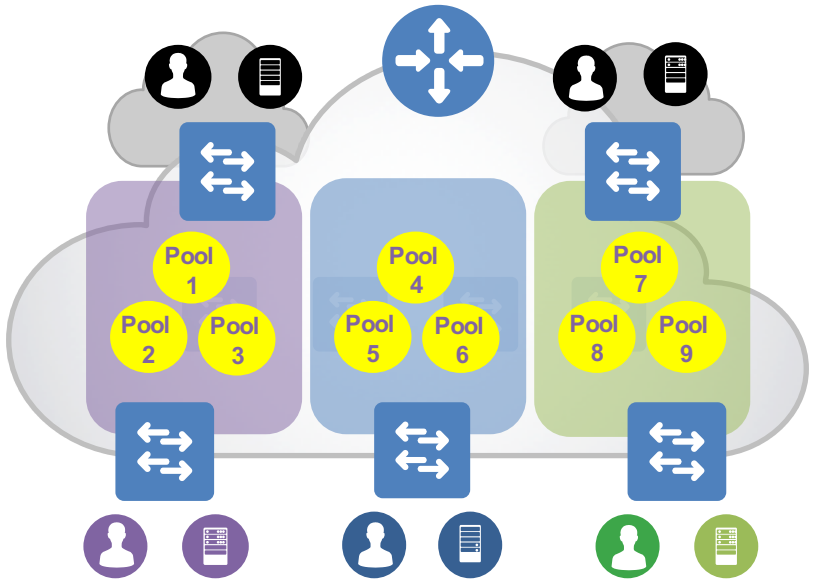
LISP Mobility in Campus Fabric

Cisco Connect

Host Pool is based on an IP Subnet + VLAN ID

Provides the basic IP constructs, including "Anycast Gateway" for each Host Pool

- Edge Nodes maintain a Switch Virtual Interface (SVI), with IP Subnet, Gateway IP, etc. for each Host Pool
- LISP uses Dynamic EID to advertise each Host Pool (within each Instance ID)
- LISP Dynamic EID allows Host-specific (**/32**, /128, MAC) advertisement and mobility
- Host Pools can either be assigned Statically (per port) or Dynamically (using Host Authentication)



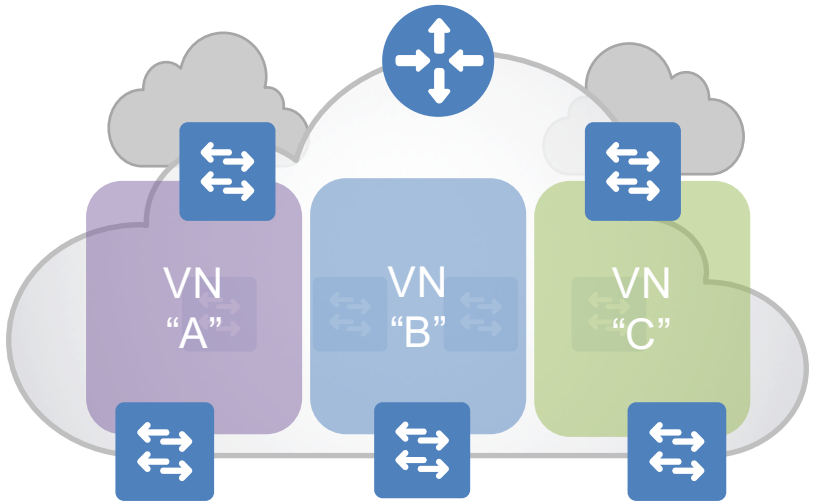
LISP Secure Segmentation in Campus Fabric

Cisco Connect

Virtual Network (VN) based on Virtual Routing and Forwarding (VRF)

Maintains a separate Routing and Switching instance for each Virtual Network

- LISP uses Instance ID to maintain independent VRF topologies ("Default" VRF is Instance ID "0")
- LISP adds VNID to the LISP / VXLAN encapsulation
- Endpoint ID prefixes (Host Pools) are advertised within the LISP Instance ID



How does LISP work?

Locator / ID Separation Protocol

LISP Mapping System

Cisco Connect

LISP "Mapping System" is analogous to a DNS lookup

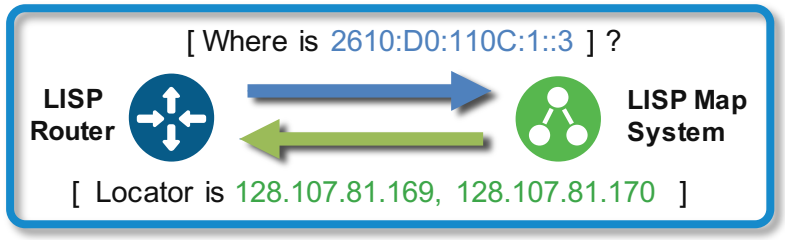
– DNS resolves IP Addresses for queried Name

Answers the "WHO IS" question

DNS
Name -to- IP
URL Resolution

– LISP resolves Locators for queried Identities

Answers the "WHERE IS" question



LISP
ID -to- Locator
Map Resolution

Want to know more about LISP?

Locator / ID Separation Protocol (LISP)

Would you like to know more?

Cisco Connect

At Cisco Live Berlin 2017 – www.ciscolive.com

BRKRST-3800 - DNA Campus Fabric – A Look Under the Hood

BRKRST-3045 - LISP - A Next Generation Networking Architecture

BRKRST-3047 - Troubleshooting LISP

LTRDCT-2224 - Enhancing VXLAN/EVPN Fabrics with LISP

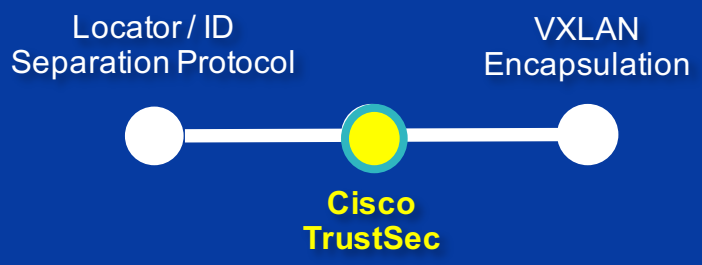
Other References

Cisco LISP Site	http://lisp.cisco.com
Cisco LISP Marketing Site	http://www.cisco.com/go/lisp/
LISP Beta Network Site	http://www.lisp4.net or http://www.lisp6.net
IETF LISP Working Group	http://tools.ietf.org/wg/lisp/
Fundamentals of LISP	https://www.youtube.com/watch?v=lKrV1qB8uqA

Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Solution Overview
What are the components ?



What is Cisco TrustSec (CTS)?

Cisco TrustSec

Traditional segmentation is extremely complex

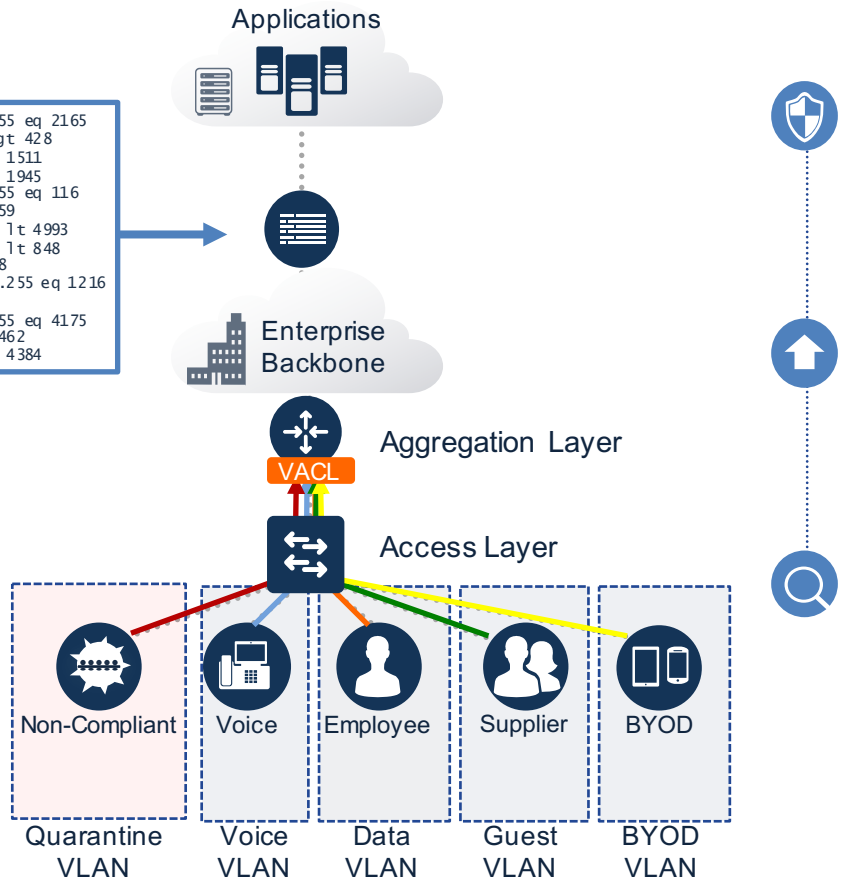
Cisco Connect

```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

- Static ACL
- Routing
- Redundancy
- DHCP Scope
- Address
- VLAN

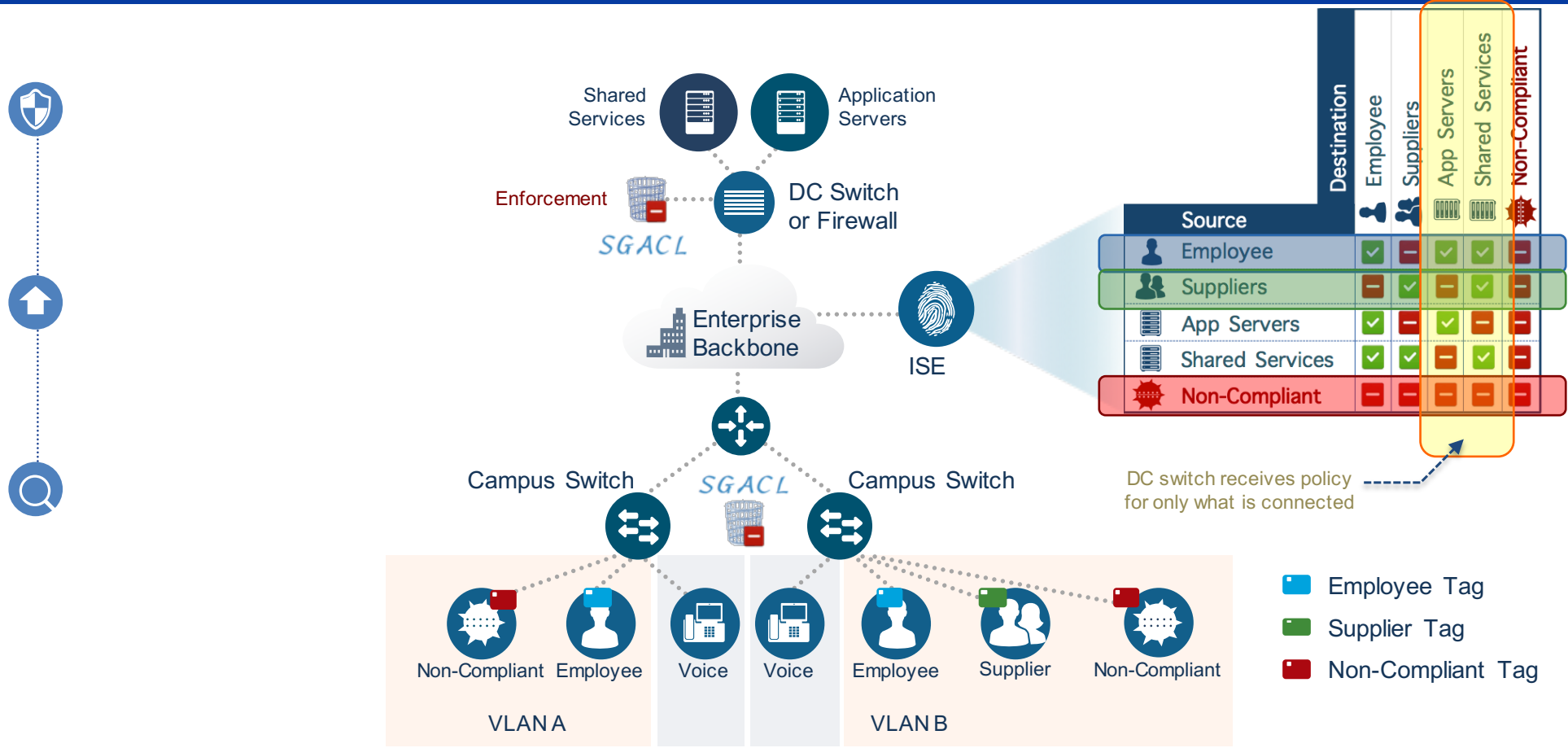
Limits of Traditional Segmentation

- Security Policy based on Topology (Address)
- High cost and complex maintenance



Cisco TrustSec
Simplified segmentation with Group Based Policy

Cisco Connect



How is Cisco TrustSec used in Campus Fabric?

Cisco Trust Security

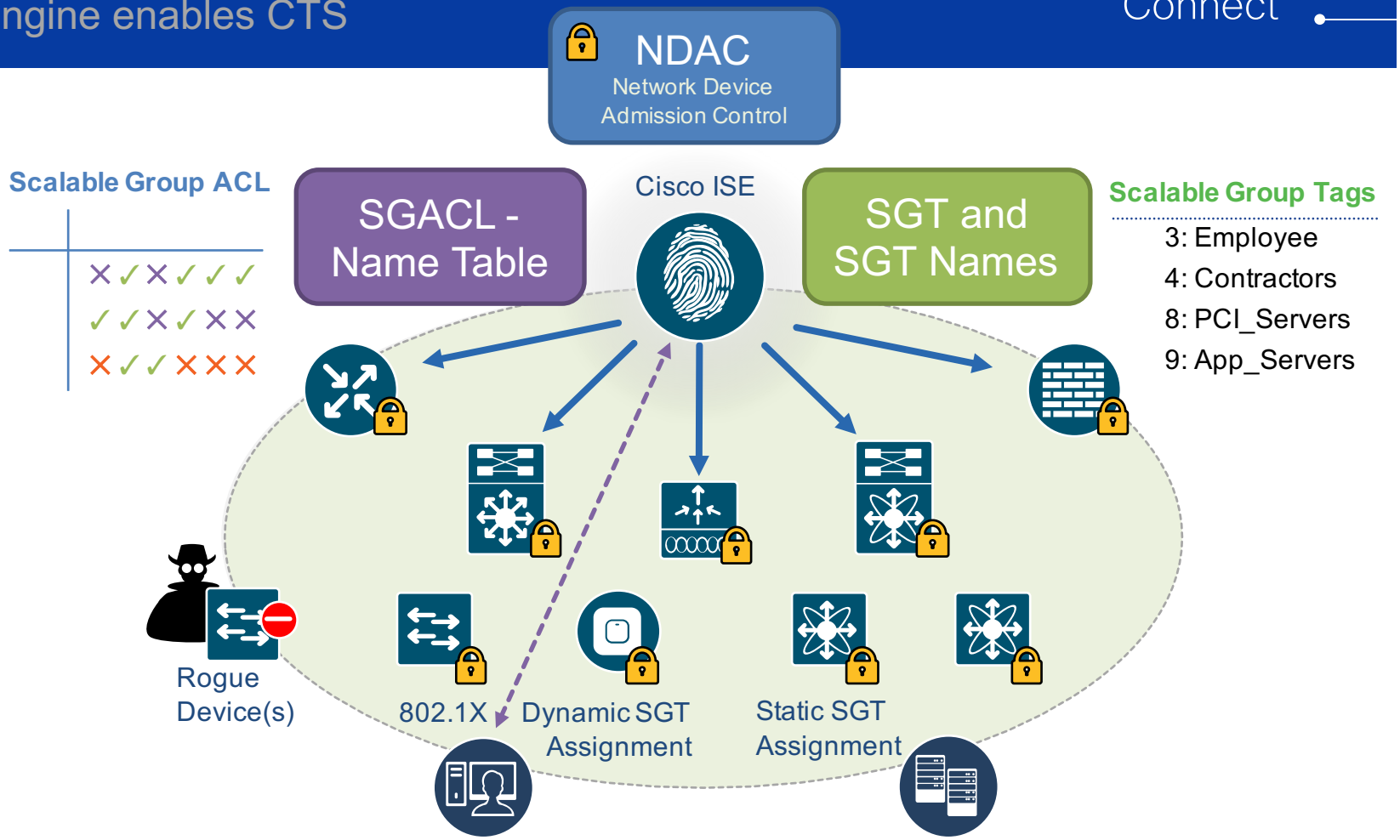
Identity Services Engine enables CTS

Cisco Connect

NDAC
Network Devices for a trusted CTS domain

SGT and SGT Names
Centrally defined Endpoint ID Groups

SGACL - Name Table
Policy matrix to be pushed down to the network devices



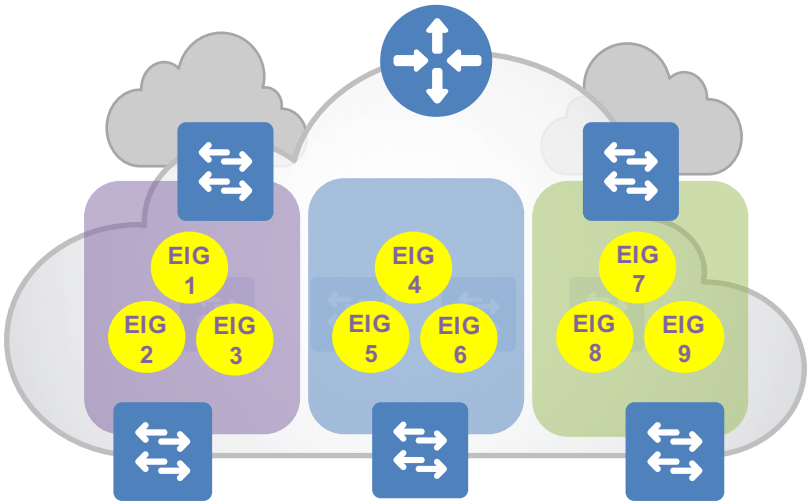
Campus Fabric
Endpoint ID Groups – A Closer Look

Cisco Connect

Endpoint ID Group is based on a Scalable Group Tag (SGT)

Each User or Device is assigned to a unique Endpoint ID Group (EIG)

- CTS uses Endpoint ID "Groups" to assign a unique Scalable Group Tag (SGT) to Host Pools
- LISP adds SGT to the LISP / VXLAN encapsulation
- CTS EIGs are used to manage address-independent "Group-Based Policies"
- Individual Edge and Border Nodes use SGT to enforce local Scalable Group ACLs (SGACLs)



Want to know more about TrustSec?

Cisco Trust Security (CTS)

Would you like to know more?

Cisco Connect APP

At Cisco Live Berlin 2017 – www.ciscolive.com

BRKCOC-2255 - Inside Cisco IT: How Cisco deployed ISE and TrustSec, globally

BRKSEC-2203 - Intermediate - Enabling TrustSec Software-Defined Segmentation

TECSEC-2222 - Securing Networks with Cisco TrustSec

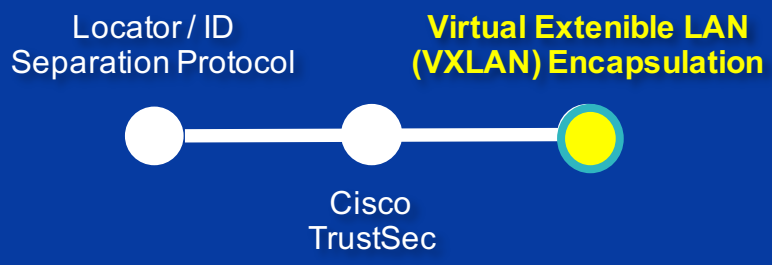
Other References

Cisco TrustSec Marketing Site	http://www.cisco.com/go/trustsec/
Cisco TrustSec Config Guide	cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec.html
CTS Architecture Overview	cisco.com/docs/switches/lan/trustsec/configuration/guide/trustsec/arch_over.html
CTS 2.0 Design Guide	cisco.com/td/docs/solutions/Enterprise/Security/TrustSec_2-0/trustsec_2-0_dig.pdf
Fundamentals of TrustSec	https://www.youtube.com/watch?v=78-GV7Pz18I

Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Solution Overview
What are the components ?

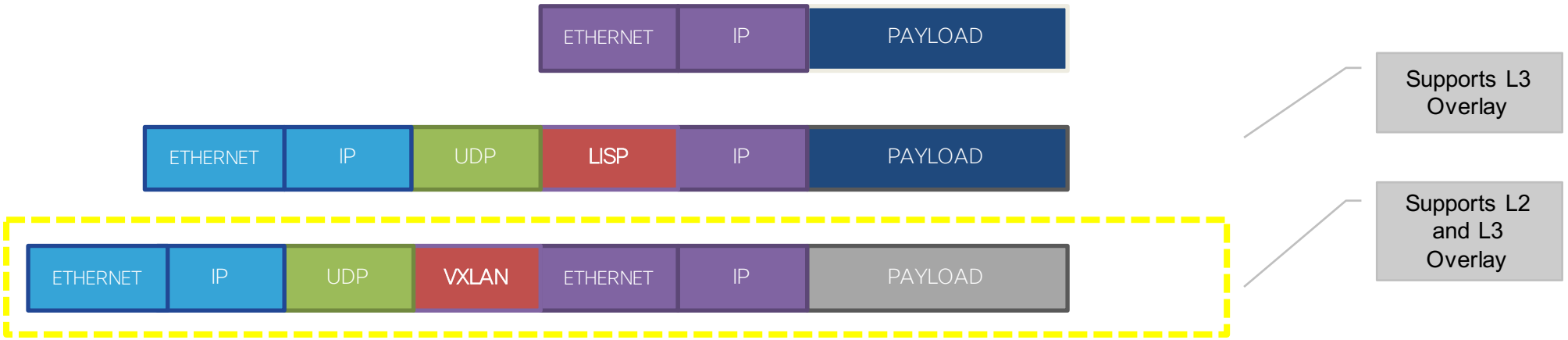


What is Virtual Extensible LAN (VXLAN) Encapsulation?

VXLAN Encapsulation

Cisco Connect

VXLAN is the Data Plane



Data-Plane Overview
Fabric Header Encapsulation

Cisco Connect

Fabric Data-Plane provides the following:

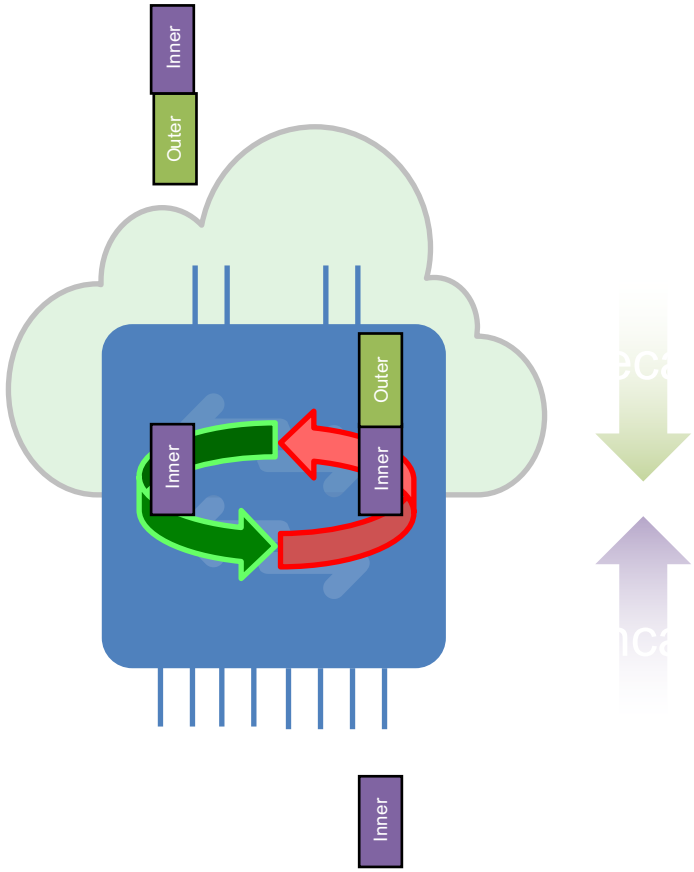
- Underlay address advertisement and mapping
- Automatic tunnel setup (Virtual Tunnel End-Points)
- Frame encapsulation between Routing Locators

Support for LISP or VXLAN header format

- Nearly the same, with different fields and payload
- LISP header carries IP payload (IP in IP)
- VXLAN header carries MAC payload (MAC in IP)

Triggered by LISP Control-Plane events

- ARP or NDP Learning on L3 Gateways
- Map-Reply or Cache on Routing Locators



Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Putting It Together

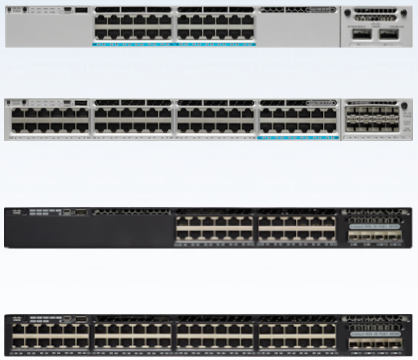
How do I build it?

What Cisco switches support Campus fabric?

Platform Support
Fabric Edge Nodes - Options

Cisco Connect

Catalyst 3K



- **Catalyst 3650**
- **Catalyst 3850**
- 1G/MGIG (Copper)
- **IOS-XE 16.3.1+**

Catalyst 4K

- **Catalyst 4500**
- Sup8E (Uplinks)
- 4700 Cards
- **IOS-XE 3.9.1+**

Platform Support
Fabric Border Nodes - Options

Cisco Connect

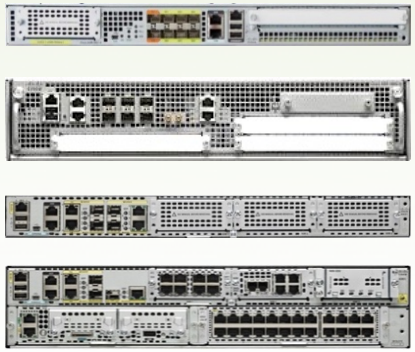
Catalyst 3K

- **Catalyst 3850**
- 12/24 or 48XS
- 1/10G (Fiber)
- **IOS-XE 16.3.1+**

Catalyst 6K

- **Catalyst 6800**
- Sup2T or 6T
- 6880 or 6840-X
- **IOS 15.4.1SY+**

ASR1K & ISR4K



- **ASR1000-X**
- ISR4430/4450
- X or HX Series
- **IOS-XE 16.4.1+**

Nexus 7K

- **Nexus 7700**
- Sup2E
- M3 Cards
- **NXOS 7.3.2+**

Platform Support
Fabric Control-Plane - Options

Cisco Connect

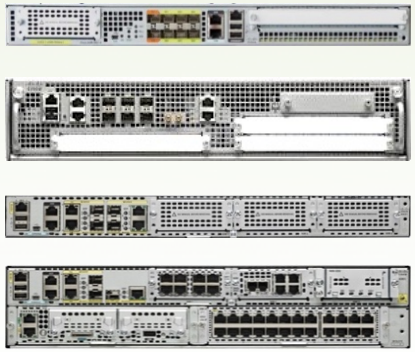
Catalyst 3K

- **Catalyst 3850**
- 12/24 or 48XS
- 1/10G (Fiber)
- **IOS-XE 16.3.1+**

Catalyst 6K

- **Catalyst 6800**
- Sup2T or 6T
- 6880 or 6840-X
- **IOS 15.4.1SY+**

ASR1K & ISR4K



- **ASR1000-X**
- ISR4430/4450
- X or HX Series
- **IOS-XE 16.4.1+**

How do I configure Campus Fabric?

What is Smart CLI?

- Its **a new configuration mode** to simplify config and management of Campus Fabric
- Invoked by a new Global command "**fabric auto**"
- Provides a simple set of **easy-to-understand CLI**
- **Auto-generates** all of the equivalent (traditional) LISP, VRF, IP, CTS, etc. CLI commands


```
fabric_device(config)# fabric auto
```

Smart CLI – Example
Adding a new Edge Node

Cisco Connect

- Generate all LISP XTR baseline configs
- Set up Loopback0 as locator address
- Creates default neighborhood as instance ID 0
- Enables VXLAN encapsulation
- Adds SGT to VXLAN encapsulation


```
Edge(config)# fabric auto
Edge(config-fabric-auto)# domain default
Edge(config-fabric-auto-domain)# control-plane 2.2.2.2 auth-key key1
Edge(config-fabric-auto-domain)# border 4.4.4.4
Edge(config-fabric-auto-domain)# exit
```

Smart CLI – Example
Show Fabric Domain

Cisco Connect

```
Edge# show fabric domain
Fabric Domain : "default"
Role : Edge
Control-Plane Service: Disabled
Border Service: Disabled

Number of Control-Plane Nodes: 1
IP Address          Auth-key
--------------------------------
2.2.2.2             key1

Number of Border Nodes: 1
IP Address
--------------------------------
4.4.4.4

Number of Neighborhood(s): 4
 Name               ID        Host-pools
-----------------------------------------
default             0          2
guest               50         1
pcie                60         1
cisco               70         *
```

More to Come! ☺

- **Underlay Network**
  and Protocols to bring up the Underlay network
- **Endpoint ID Groups**
  CTS commands for Static & Dynamic ID
- **Group Based Policy**
  SGACL policies
- **And More…**

fabric_device(config)# **fabric auto**

Cisco Connect

- Key Benefits
- Key Concepts
- Solution Overview
- Putting It Together
- Use Case

Use Case

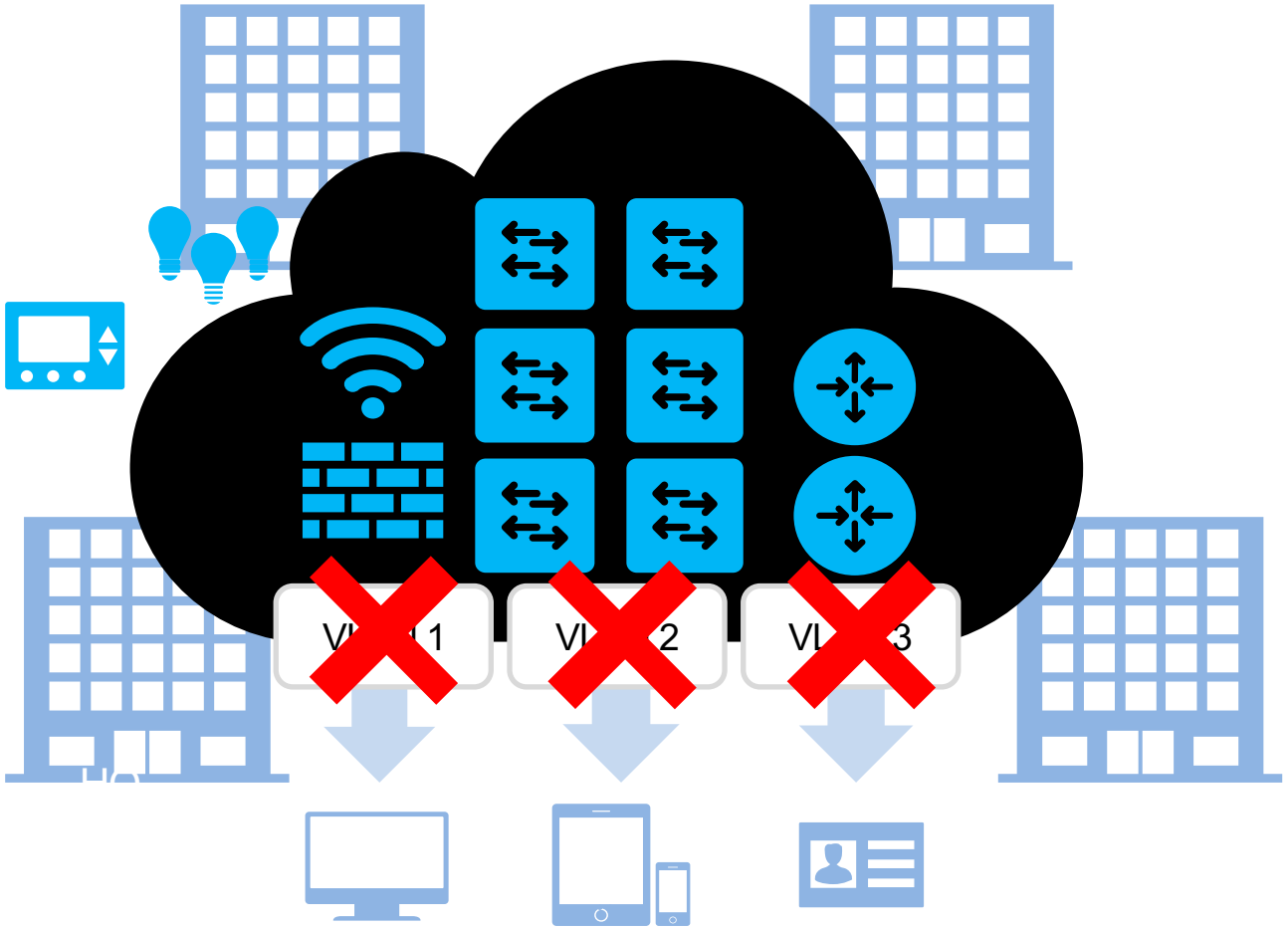
OK, now that I've seen all this, why might I use this in my network?

EU Regulatory Compliance -GDPR

Cisco Connect

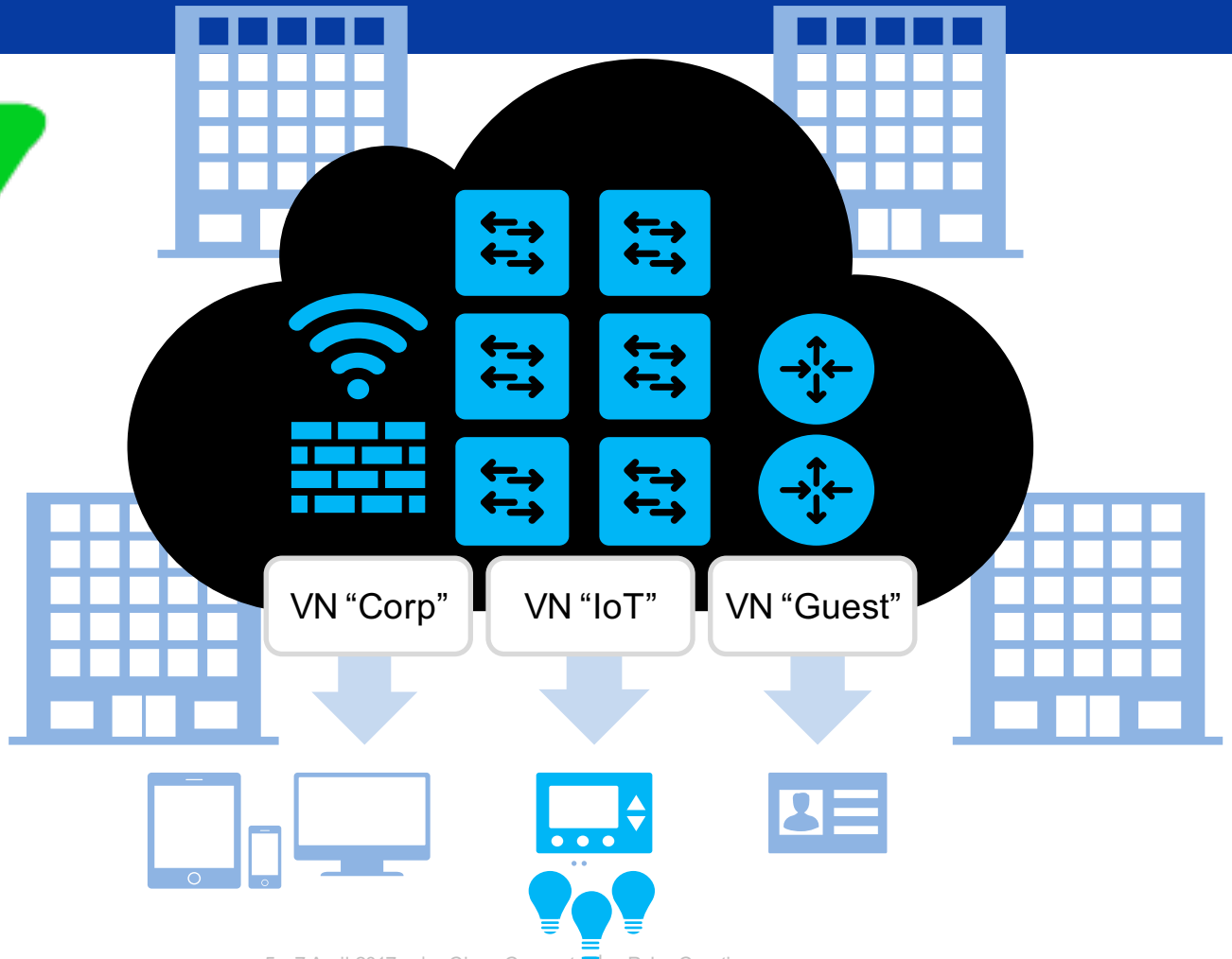
Use Case – Comply with GDPR

Cisco Connect



Use Case – Comply with GDPR

Cisco Connect

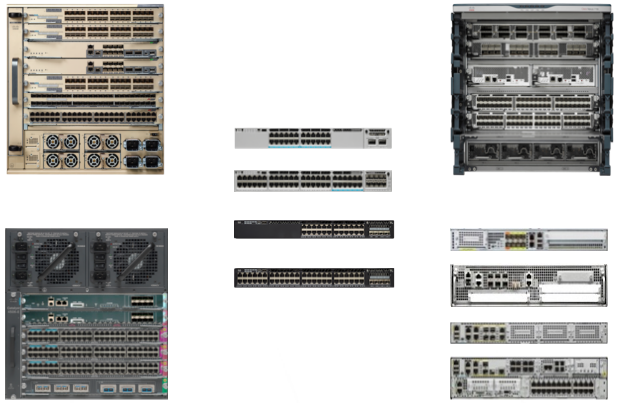


Take-Away

What to do next?

1. Update your Hardware and Software!

- **Catalyst 3650** or **3850** - New **IOS-XE 16.3+**
- **Catalyst 4500** w/ **Sup8E** - New **IOS-XE 3.9+**
- **Catalyst 6807**, **6880** or **6840** - New **IOS 15.4SY+**
- **Nexus 7700** w/ **M3 Cards** - New **NX-OS 7.3.2+**
- **ASR1000-X** or **ISR4400** - New **IOS-XE 16.4+**

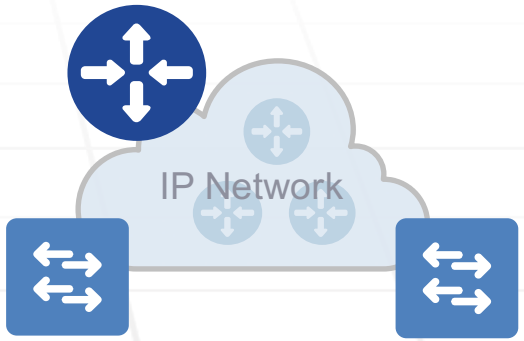


2. Try out "Campus Fabric" in your Lab!

- You only need 2 or 3 (+) switches to test this solution
- At least 1 Control-Plane + Border and 1 Fabric Edge

3. Trial Deployments (Remember: its an Overlay)

- You can install new C-Plane, Border and Edge Nodes without modifying your existing (Underlay) network



Campus Fabric CVD on Cisco.com

Cisco Connect

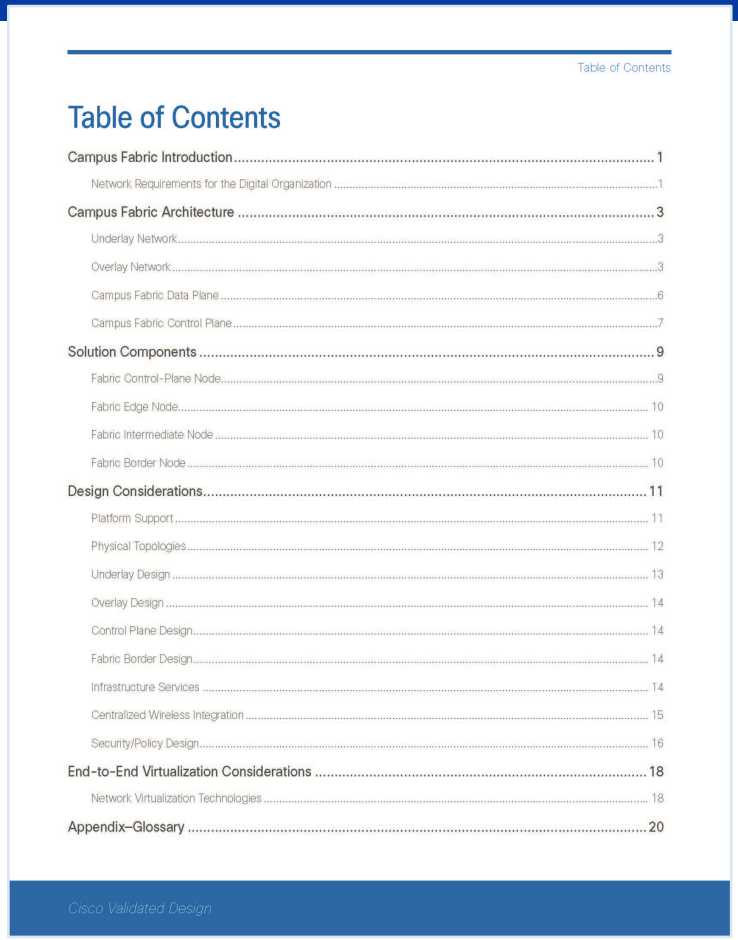


Table of Contents

Table of Contents

Cisco Validated Design


CISCO