BCNET

Shared IT Services for Higher Education & Research

Conference 2018

Next Generation Campus Architectures Based on Software Defined Networking

Robert Barton, Principal Systems Engineer

Cisco

Unprecedented Demands on the Network

Digital Disruption

63 million new devices online every second by 2020[1]

Lack of Business and IT Insights

Complexity

3X spend on network operations vs network[2]

Slow and Error Prone Operations

Security

6 months to detect breach[3]

Unconstrained Attack Surface

1: Gartner Report - Gartner's 2017 Strategic Roadmap for Networking
2. McKinsey Study of Network Operations for Cisco – 2016
3. Ponemon Research Institute Study on Malware Detection, Mar 2016

Key Challenges for Traditional Networks

Difficult to Segment

Ever increasing number of users and endpoint types

Ever increasing number of VLANs and IP Subnets

Complex to Manage

Multiple steps, user credentials, complex interactions

Multiple touch-points

Slower Issue Resolution

Separate user policies for wired and wireless networks

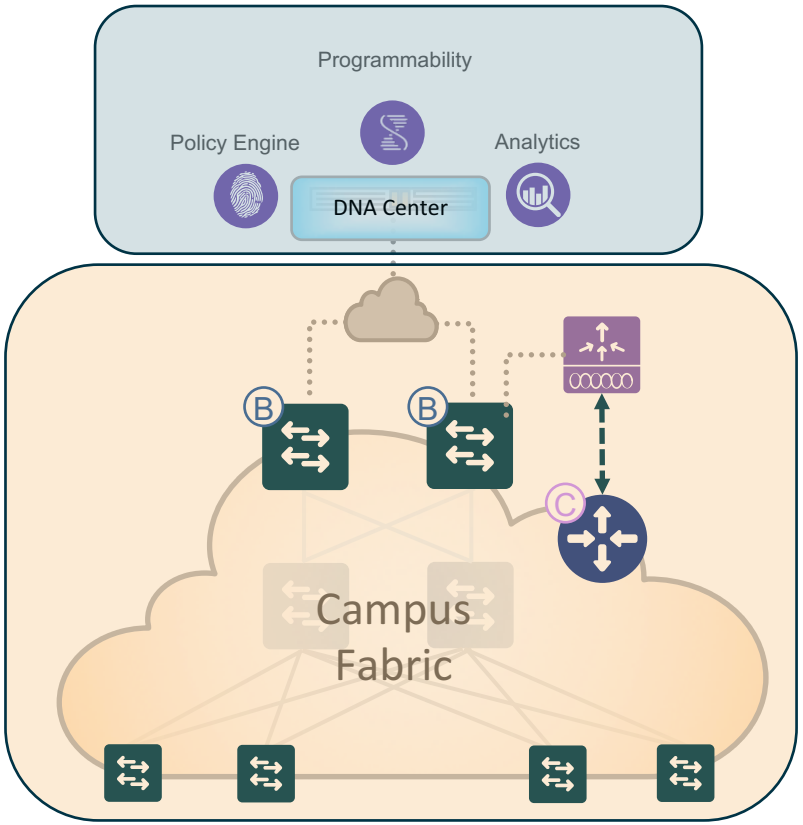
Unable to find users when troubleshooting

Rewriting the Networking Playbook

Hardware centric	 Software driven (SDN)
Manual Configuration	 Automated and end-to-end
Silo’d Security and Policies	 Integrated Security / Policy
Network Monitoring	 Analytics and Insights

Software-Defined Access (SDA)

Software Defined Access (SDA):
The Campus Fabric + DNA-Center



SD-Access

- DNA-Center GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy.
- Leverages DNA Center to integrate external Service Apps, to orchestrate your entire LAN, Wireless LAN and WAN access network.
- A new paradigm for campus network based on overlay technologies and agile security policy

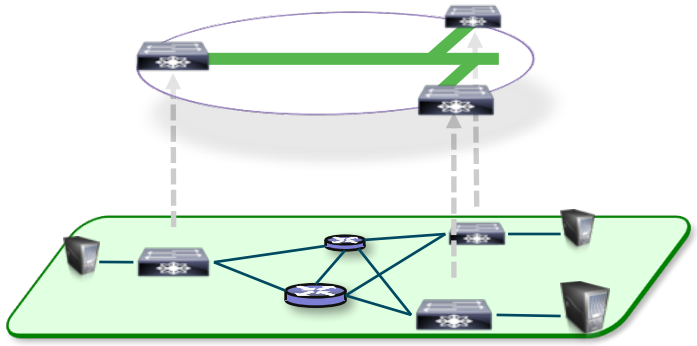
Software Defined Access (SDA)

What exactly is a Fabric?

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

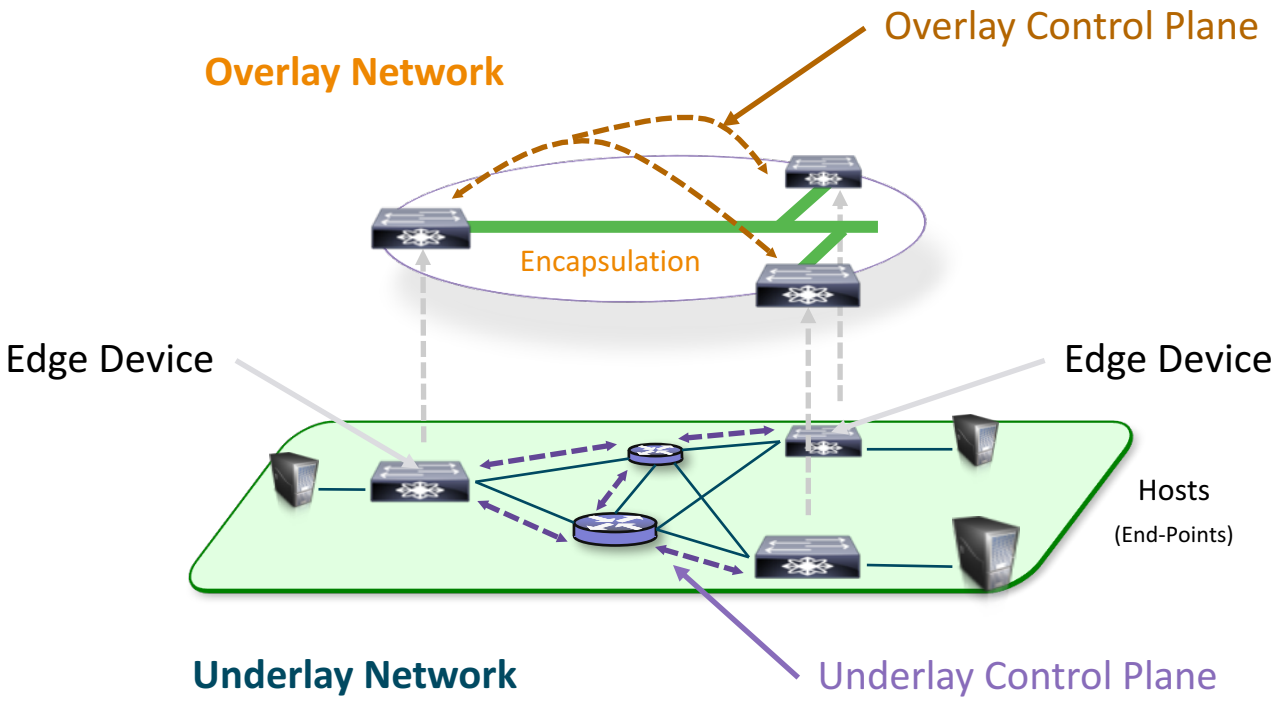
- An *Overlay network* is a *logical topology* used to *virtually connect* devices, built *on top* of some arbitrary physical *Underlay* topology.
- An *Overlay network* network often uses *alternate forwarding attributes* to provide *additional services,* not provided by the *Underlay*.

Examples of Network Overlays	
• GRE or mGRE	• LISP
• MPLS or VPLS	• OTV
• IPSec or DMVPN	• DFA
• CAPWAP	• ACI



SD-Access

Fabric Terminology



SD-Access

Campus Fabric - Key Components

1. **Control-Plane** based on **LISP** (RFC 6830)
2. **Data-Plane** based on **VXLAN** (RFC 7348)
3. **Policy-Plane** based on **CTS** (RFC 3514)

SD-Access Fabric

Key Components – LISP

1. Control-Plane based on LISP

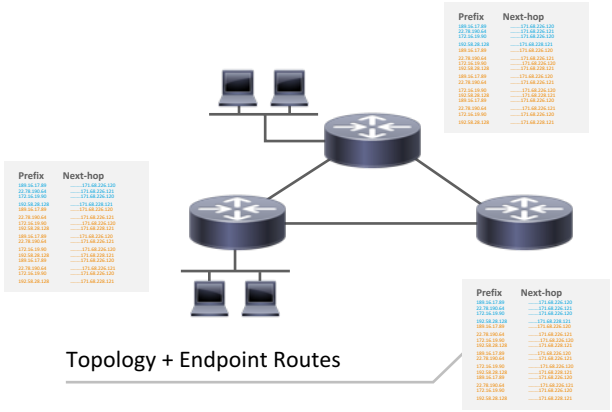
Host Mobility

Routing Protocols = **Big Tables** & **More CPU**
with Local L3 Gateway

LISP DB + Cache = **Small Tables** & **Less CPU**
with Anycast L3 Gateway

BEFORE

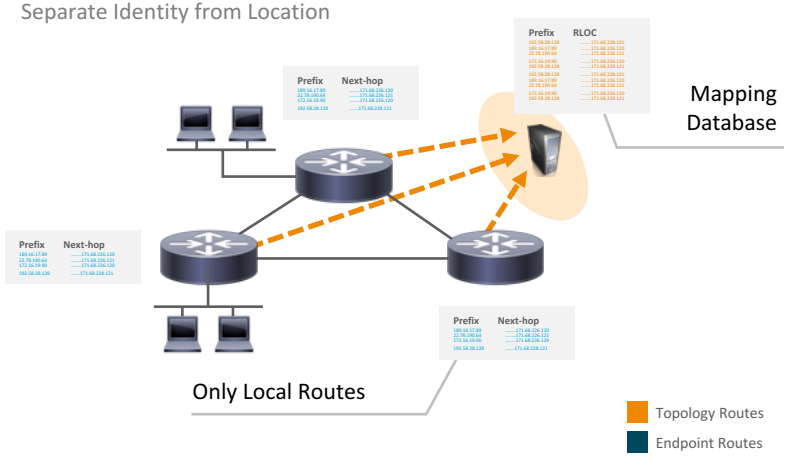
IP Address = Location + Identity



Endpoint Routes are Consolidated to LISP DB

AFTER

Separate Identity from Location



Locator / ID Separation Protocol

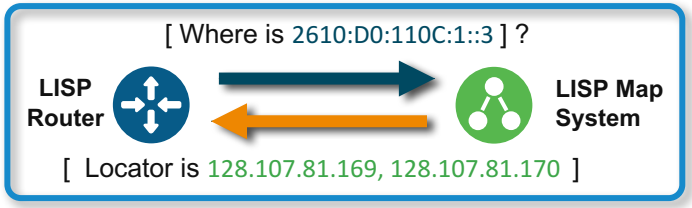
LISP Mapping System

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

Locator / ID Separation Protocol

LISP Roles & Responsibilities

Map Server / Resolver

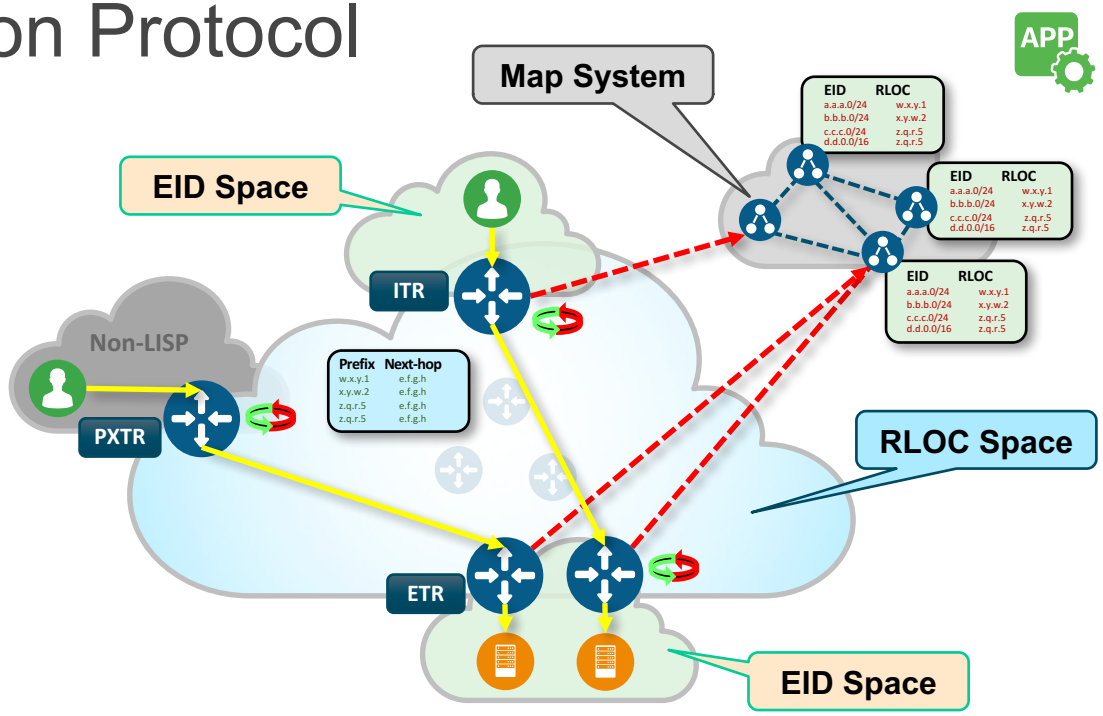
- EID to RLOC Mappings
- Can be distributed across multiple LISP devices

Tunnel Router - XTR

- Edge Devices Encap / Decap
- Ingress / Egress (ITR / ETR)

Proxy Tunnel Router - PXTR

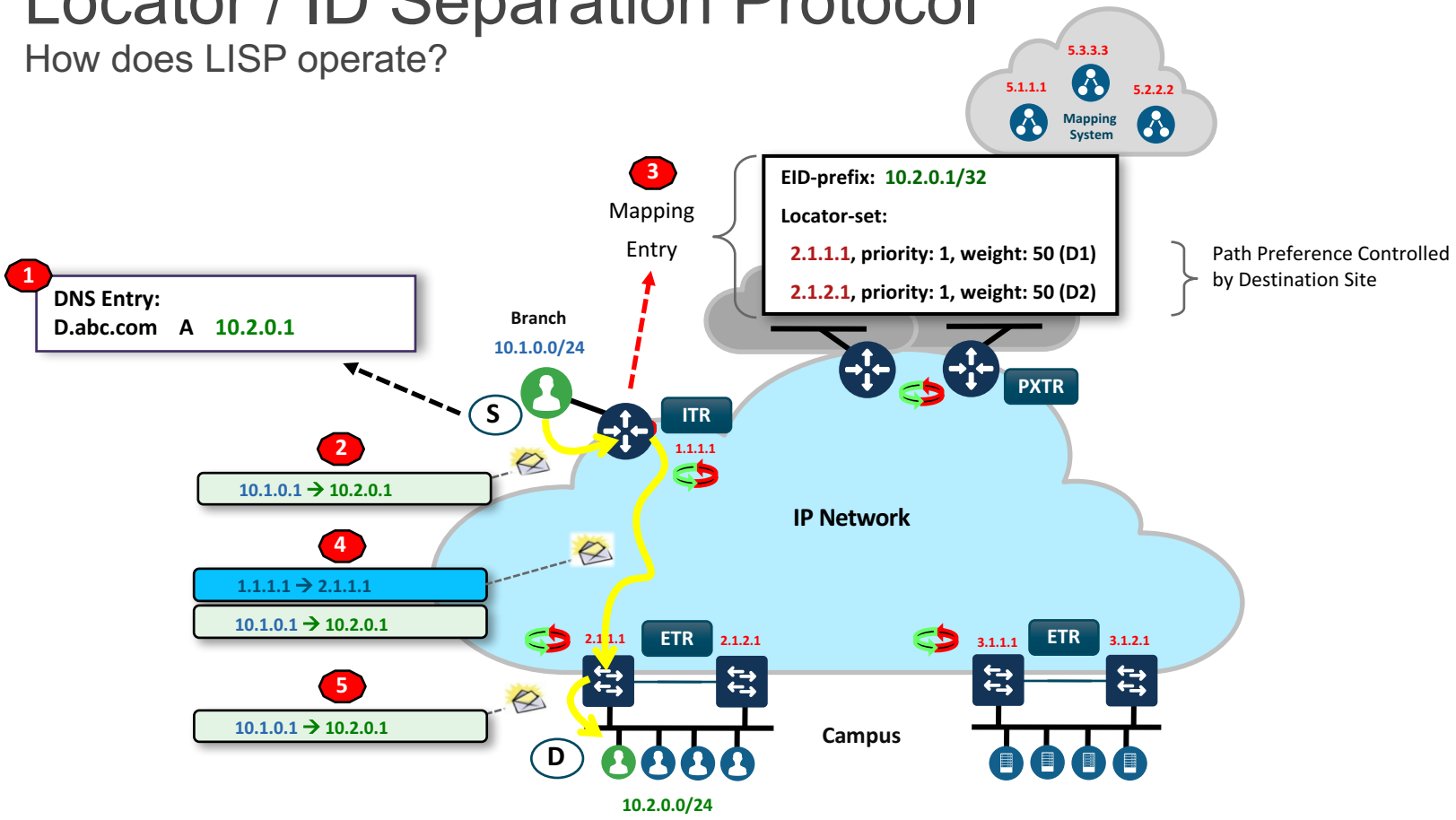
- Connects between LISP and non-LISP domains
- Ingress / Egress (PITR / PETR)



- **EID = End-point Identifier**
  - Host Address or Subnet
- **RLOC = Routing Locator**
  - Local Router Address

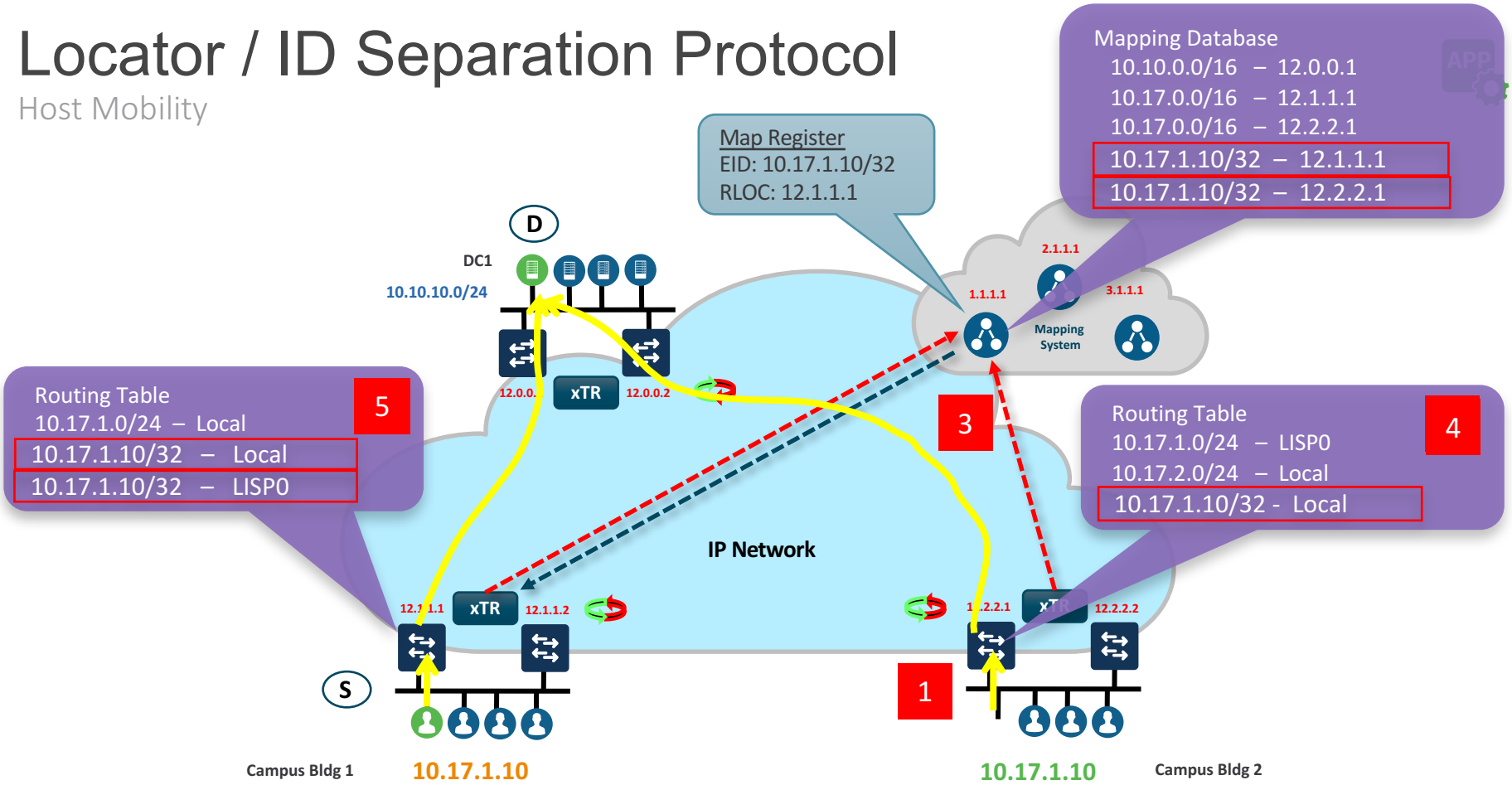
Locator / ID Separation Protocol

How does LISP operate?



Locator / ID Separation Protocol

Host Mobility

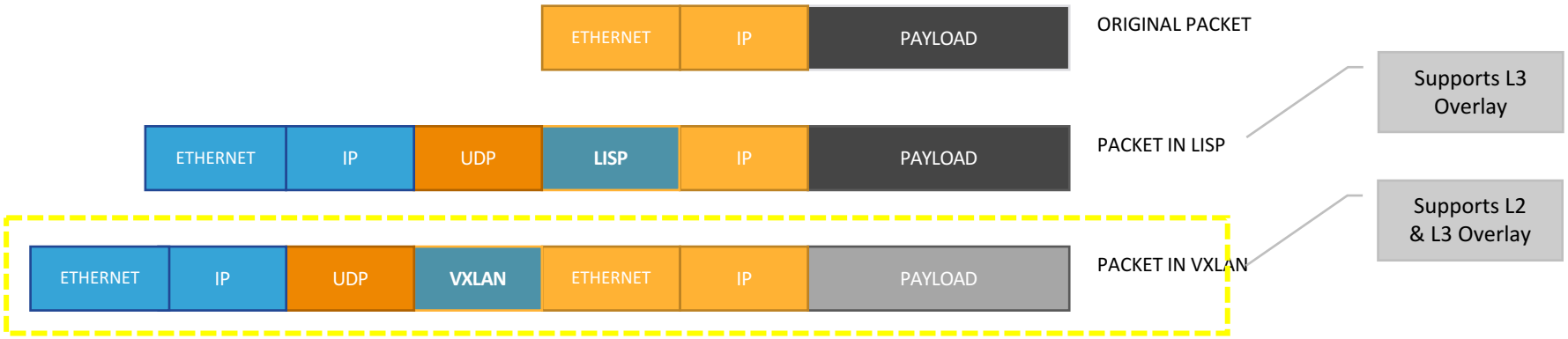


VXLAN Data Plane and Policy / Security Plane

SD-Access Fabric

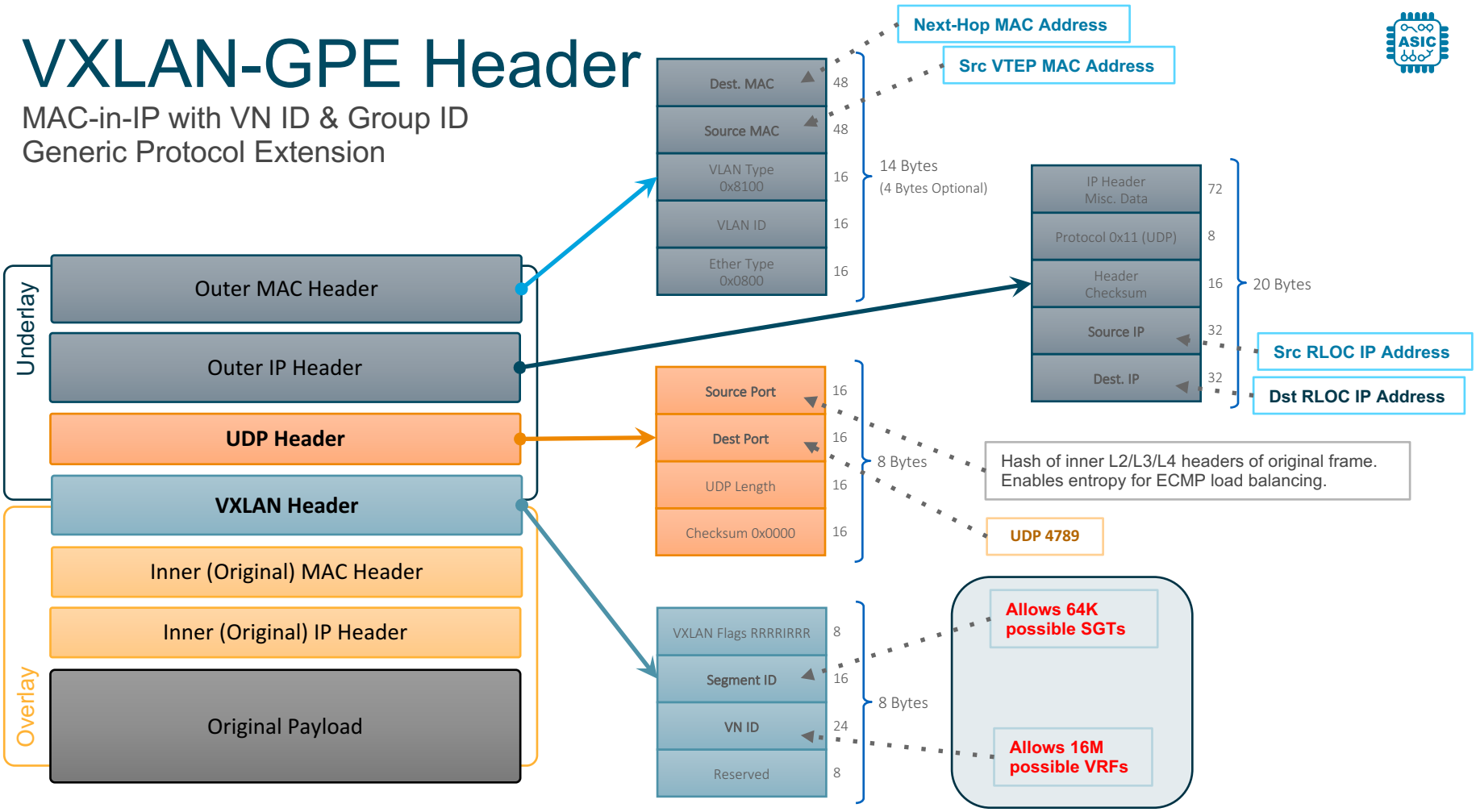
Key Components – VXLAN

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



VXLAN-GPE Header

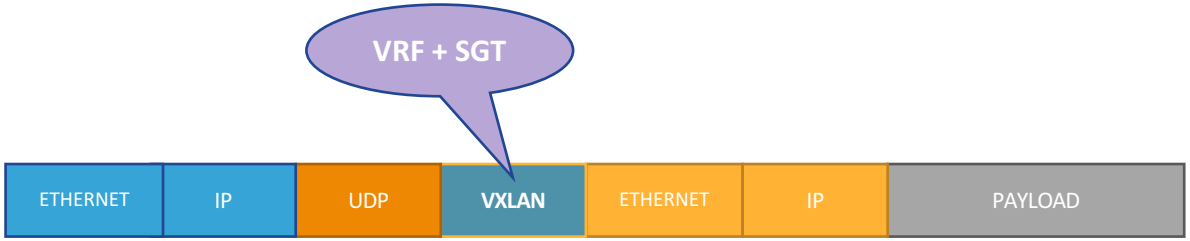
MAC-in-IP with VN ID & Group ID
Generic Protocol Extension



SD-Access Fabric

Key Components – CTS

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



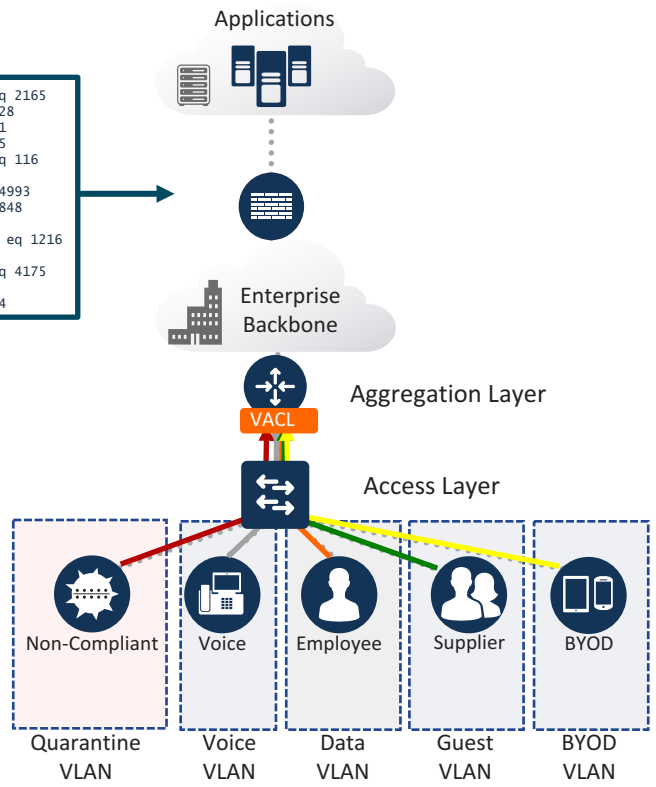
Virtual Routing & Forwarding
Scalable Group Tagging

18

Redesigning Network Policy with SGTs

Traditional access control is extremely complex – aka “Cisco TrustSec”

```
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

Enforcement
IP Based Policies - ACLs, Firewall Rules

Propagation
Carry “Segment” context through the network using VLAN, IP address, VRF

Classification
Static or Dynamic VLAN assignments

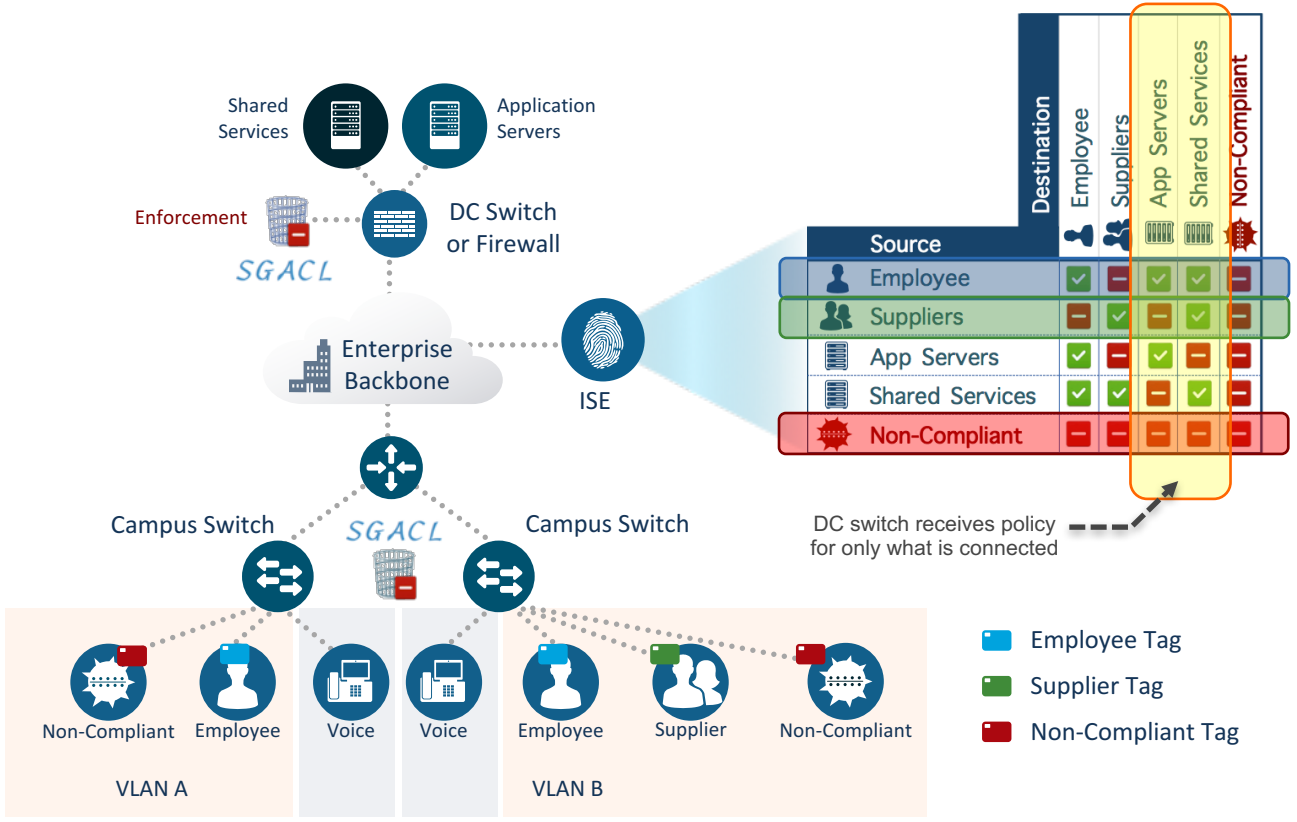
SGTs with Cisco TrustSec

Simplified access control with Group Based Policy

Enforcement
Group Based Policies
ACLs, Firewall Rules

Propagation
Carry "Group" context through the network using only SGT

Classification
Static or Dynamic SGT assignments



Cisco TrustSec

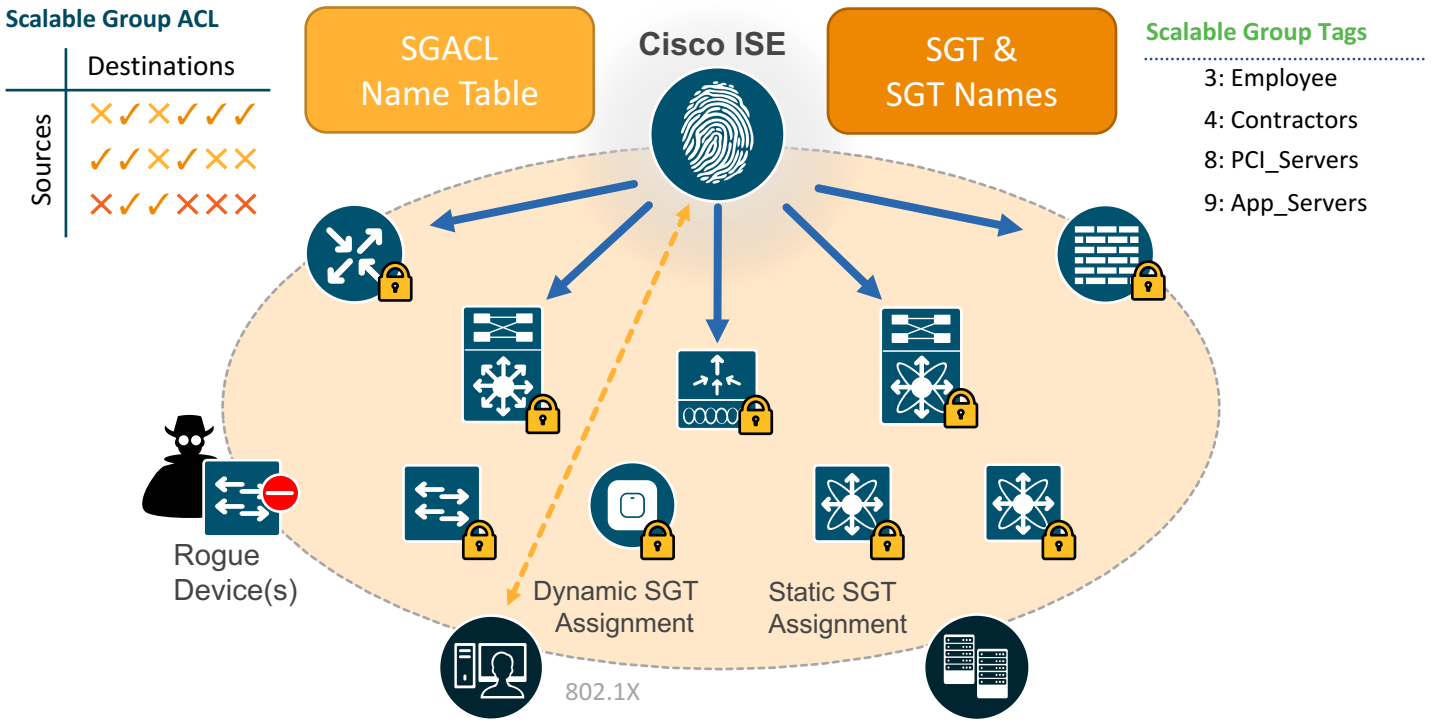
Identity Services Engine (ISE) enables CTS

NDAC authenticates Network Devices for a trusted CTS domain

SGT & SGT Names
Centrally defined Endpoint ID Groups

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

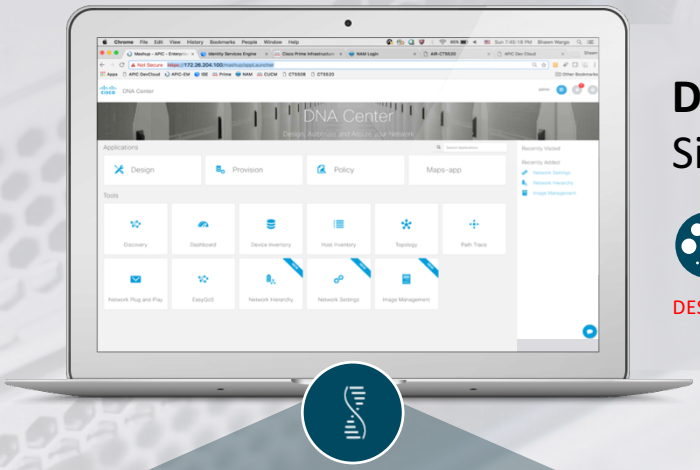
ISE dynamically authenticates endpoint users and devices, and assigns SGTs



Bringing it all Together: DNA Center

Cisco DNA

Cisco Enterprise Portfolio



DNA Center

Simple Workflows

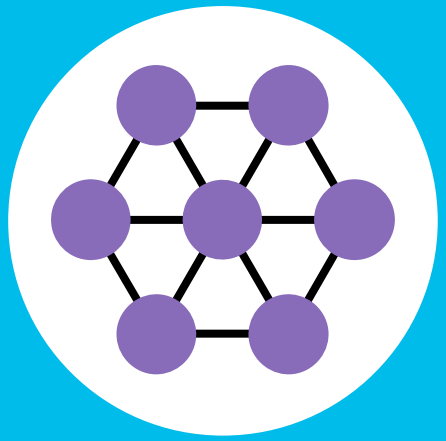
DESIGN PROVISION POLICY ASSURANCE

DNA Center

Identity Services Engine — **Data Analytics**

Routers | Switches | Wireless Controllers | Wireless APs

Data Analytics of the Network



The more you use it, the wiser it gets.

Constantly Learning

Support 100X new devices, apps, users

Constantly Adapting

Respond Instantly to business demands with limited staff and budget

Constantly Protecting

See and predict issues and threats and respond fast

DNA Center Data Analytics – Time Series Analysis

Time series data: (**assurance performance KPIs)**

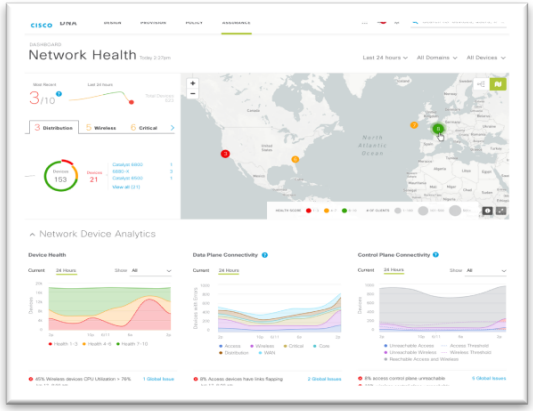
- A set of observations collected at equally spaced time intervals for a variable:

Purpose of Time Series Analytics:

- Study past behavior in order to formulate policies or decisions
- Compare the changes in the values of different time
- Predict or estimate or forecast the future behavior

DNA Center Supports Time Series Operations:

- Statistical computation: mean, std, percentile, histogram, moving_avg, etc.
- Windowing: fix, sliding, session, global
- Lag and missing data
- Preserve raw data for time range queries
- Tenant aware



THANK YOU!!