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

Lack of Business and IT Insights

Complexity

3X spend on network operations vs network

Slow and Error Prone Operations

Security

6 months to detect breach

Unconstrained Attack Surface

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

Traditional Networks Cannot Keep Up!
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

- 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.
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
- MPLS or VPLS
- IPSec or DMVPN
- CAPWAP
- LISP
- OTV
- DFA
- ACI
SD-Access
Fabric Terminology

Overlay Network

Overlay Control Plane

Encapsulation

Edge Device

Underlay Network

Underlay Control Plane

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

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

BEFORE
IP Address = Location + Identity

---

**Endpoint Routes are Consolidated to LISP DB**

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

AFTER
Separate Identity from Location

---

**SD-Access Fabric**
Key Components – LISP
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**

```
[ Who is lisp.cisco.com ] ?

Host

[ Address is 153.16.5.29, 2610:D0:110C:1::3 ]

DNS Server

DNS
Name -to- IP
URL Resolution
```

- LISP resolves **Locators** for queried **Identities**  
  **Answers the “WHERE IS” question**

```
[ Where is 2610:D0:110C:1::3 ] ?

LISP Router

[ Locator is 128.107.81.169, 128.107.81.170 ]

LISP Map System

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?

1. DNS Entry: D.abc.com A 10.2.0.1

2. 10.1.0.1 → 10.2.0.1

3. Branch 10.1.0.0/24

4. 1.1.1.1 → 2.1.1.1
   10.1.0.1 → 10.2.0.1

5. 10.1.0.1 → 10.2.0.1

EID-prefix: 10.2.0.1/32
Locator-set:
   2.1.1.1, priority: 1, weight: 50 (D1)
   2.1.2.1, priority: 1, weight: 50 (D2)

Path Preference Controlled by Destination Site

IP Network

Campus

ITR

ETR

PXTR

Mapping System

5.1.1.1
5.2.2.2
5.3.3.3

Locator / ID Separation Protocol
Locator / ID Separation Protocol

Host Mobility

Routing Table
10.17.1.0/24 – Local
10.17.1.10/32 – Local
10.17.1.10/32 – LISPO

Map Register
EID: 10.17.1.10/32
RLOC: 12.1.1.1

Mapping Database
10.10.0.0/16 – 12.0.0.1
10.17.0.0/16 – 12.1.1.1
10.17.0.0/16 – 12.2.2.1
10.17.1.10/32 – 12.1.1.1
10.17.1.10/32 – 12.2.2.1

Mapping Database
10.10.10.0/24 – 12.0.0.1
12.0.0.2

Routing Table
10.17.1.0/24 – LISPO
10.17.2.0/24 – Local
10.17.1.10/32 – Local

DC1
10.10.10.0/24

Campus Bldg 1
10.17.1.10

Campus Bldg 2
10.17.1.10
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

Underlay
- Outer MAC Header
- Outer IP Header
- UDP Header
- VXLAN Header
- Inner (Original) MAC Header
- Inner (Original) IP Header

Overlay
- Original Payload

Dest. MAC 48
Source MAC 48
VLAN Type 0x8100
VLAN ID 16
Ether Type 0x0800 16

IP Header 72
- Misc. Data 72
- Protocol 0x11 (UDP) 8
- Header Checksum 16
- Source IP 32
- Dest. IP 32

Checksum 0x0000
UDP Length 16
Dest. Port 16
Source Port 16

VXLAN Flags RRRRIRRR 8
Segment ID 16
VN ID 24
Reserved 8

Src VTEP MAC Address
Next-Hop MAC Address
Src RLOC IP Address
Dst RLOC IP Address

Hash of inner L2/L3/L4 headers of original frame. Enables entropy for ECMP load balancing.

Allows 16M possible VRFs
Allows 64K possible SGTs
UDP 4789
SD-Access Fabric

Key Components – CTS

1. **Control-Plane** based on LISP
2. **Data-Plane** based on VXLAN
3. **Policy-Plane** based on CTS
Redesigning Network Policy with SGTs

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

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

**Classification**
- Static or Dynamic VLAN assignments

**Enforcement**
- IP Based Policies - ACLs, Firewall Rules

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

---

**Limits of Traditional Segmentation**

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

---

**Static**
- ACL
- Routing
- Redundancy
- DHCP Scope

**VLAN**
- Non-Compliant
- Voice
- Employee
- Supplier
- BYOD

**Access Layer**

**Aggregation Layer**

**Enterprise Backbone**

**Applications**

---

**Example Access Policy Configuration**

```bash
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 1512
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 116.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 116.196.101.101 0.0.0.127 eq 132 19.94.101.166 0.0.0.255 eq 993
access-list 102 deny udp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 gt 4993
access-list 102 deny tcp 203.10.10.140 255.255.255.255 eq 3914 119.130.241.93 0.0.0.127 gt 4048
access-list 102 deny udp 10.10.10.140 255.255.255.255 eq 4962 207.4.250.132 0.0.31.255 gt 1111
access-list 102 deny udp 32.15.78.227 0.0.0.127 eq 1493 72.92.54.255 0.0.0.127 gt 4878
access-list 102 deny icmp 100.211.144.227 0.0.31.255 lt 6470 94.127.214.49 0.0.31.255 eq 921
access-list 102 deny tcp 88.91.79.30 0.0.0.255 gt 2587 119.130.241.93 0.0.31.255 eq 4048
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 3843 239.16.35.18 0.0.0.127 eq 4384
```
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

### Scalable Group ACL

<table>
<thead>
<tr>
<th>Sources</th>
<th>Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
<tr>
<td>✓ ✓ ✓ ✓ ✓</td>
<td>✓ ✓ ✓ ✓ ✓</td>
</tr>
</tbody>
</table>

### Cisco ISE

- **Dynamic SGT Assignment**
- **Static SGT Assignment**
- **802.1X**

### Scalable Group Tags

- 3: Employee
- 4: Contractors
- 8: PCI_Servers
- 9: App_Servers

### Rogue Device(s)

**Scalable Group Tags**

- 3: Employee
- 4: Contractors
- 8: PCI_Servers
- 9: App_Servers
Bringing it all Together: DNA Center
Cisco DNA
Cisco Enterprise Portfolio

DNA Center
Simple Workflows

Identity Services Engine
Data Analytics

Routers
Switches
Wireless Controllers
Wireless APs

BCNET Conference 2018
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!!