(pohled na) SDN

Radek Boch
Systems Engineer, CCIE #7095, rboch@cisco.com

5.10.2015

What is *SDN* ?

SDN
Many things to Many people

"An open solution for customized flow forwarding control in the Data-Center"

"A way to reduce the CAPEX of my network and leverage commodity switches"

"An open solution for VM mobility in the Data-Center"

"A means to scale my fixed/mobile gateways and optimize their placement"

"A solution to build virtual topologies with optimum multicast forwarding behavior"

"A way to distribute policy/intent, e.g. for DDoS prevention, in the network"

"A platform for developing new control planes"

"A way to avoid lock-in to a single networking vendor"

Software Defined Networking

"A way to define virtual networks with specific topologies for my multi-tenant Data-Center"

"A way to configure my entire network as a whole rather than individual devices"

"A way to optimize link utilization in my network, through new multi-path algorithms"

"With SDN I can develop solutions to my problems far faster – "at software speeds". I don't have to work with my network vendor or go through length standardization"

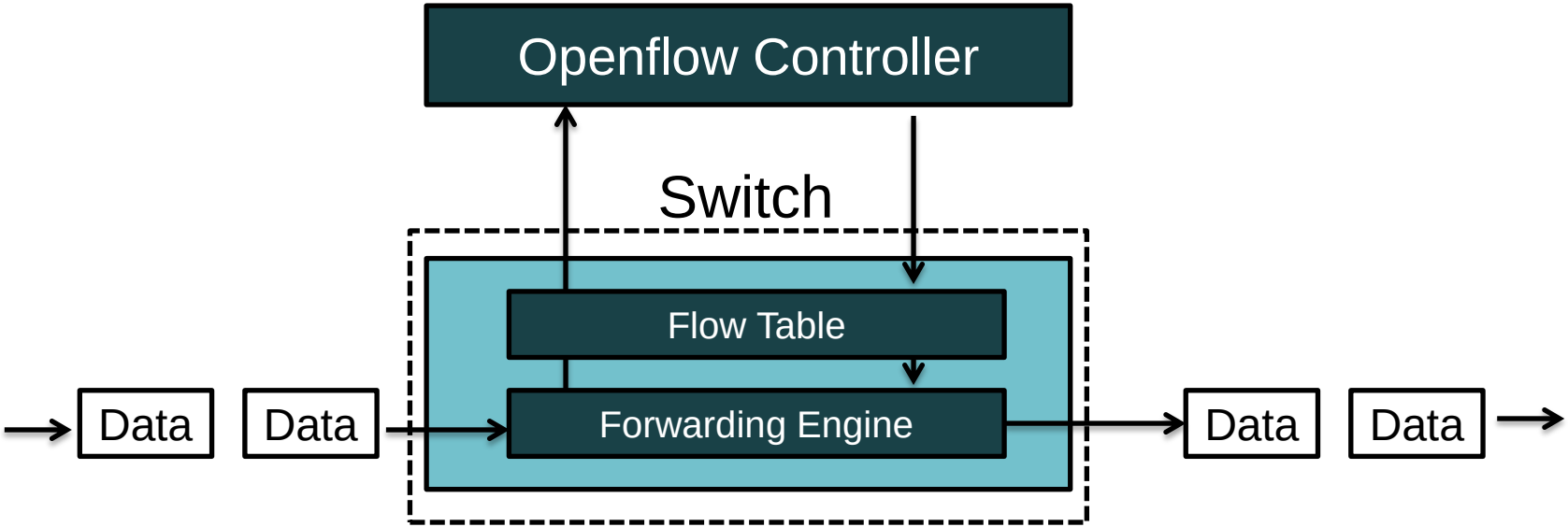
"A means to do traffic engineering without MPLS"

"A solution to build a very large scale layer-2 network"

"A way to build my own security/encryption solution, avoiding RSA"

"A way to scale my firewalls and loadbalancers"

"A solution to get a global view of the network – topology and state"

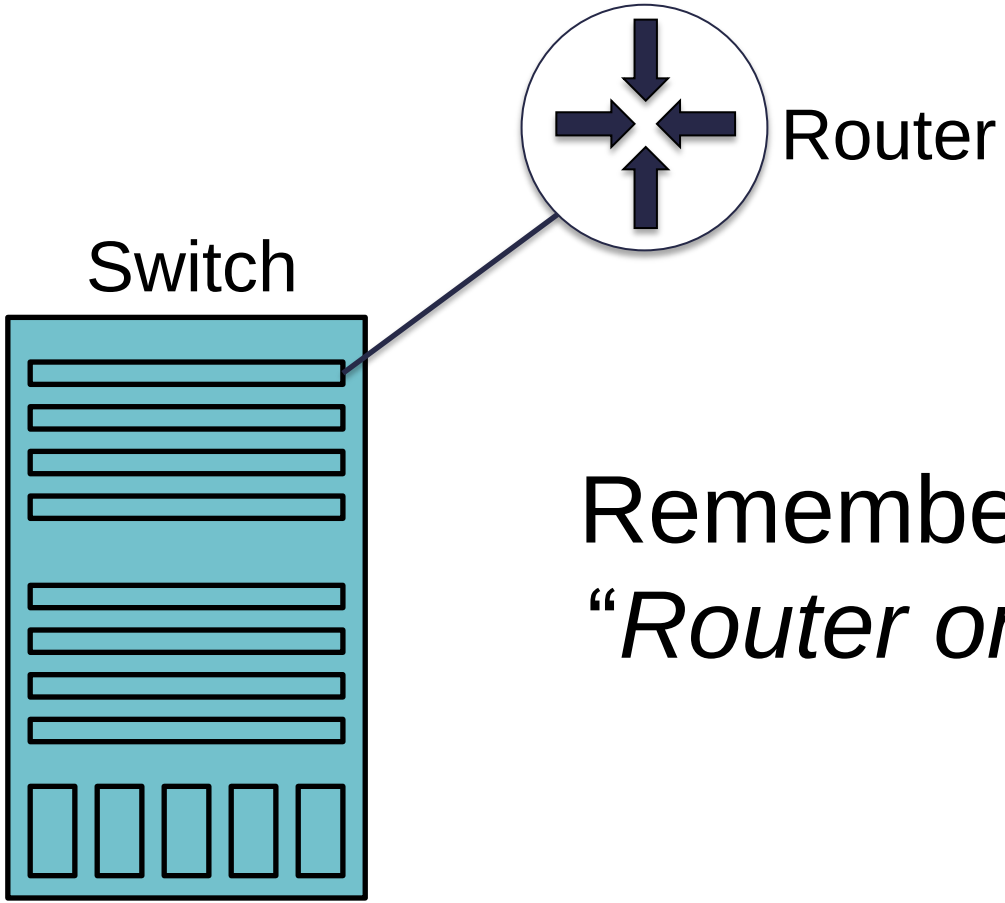


Openflow Forwarding Model

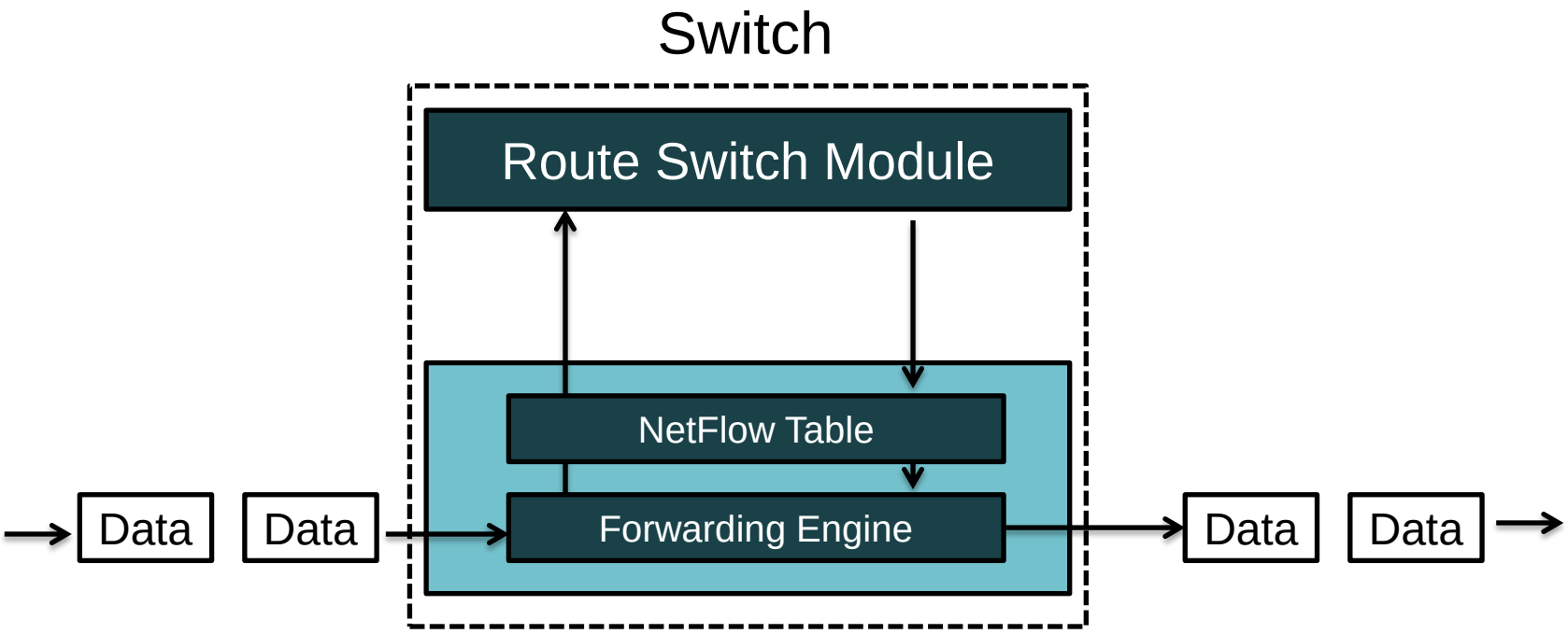
(Does this look familiar?)

Is this a ***revolutionary*** idea?

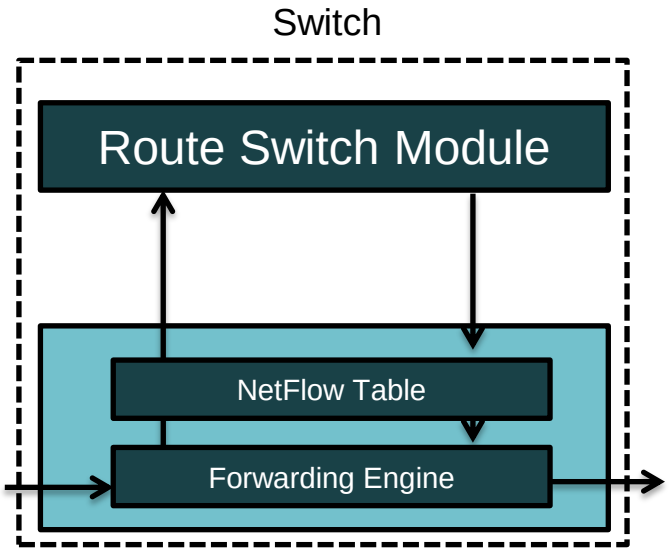
Let us go back to the late 1990's



Remember the term "*Router on a stick*"?

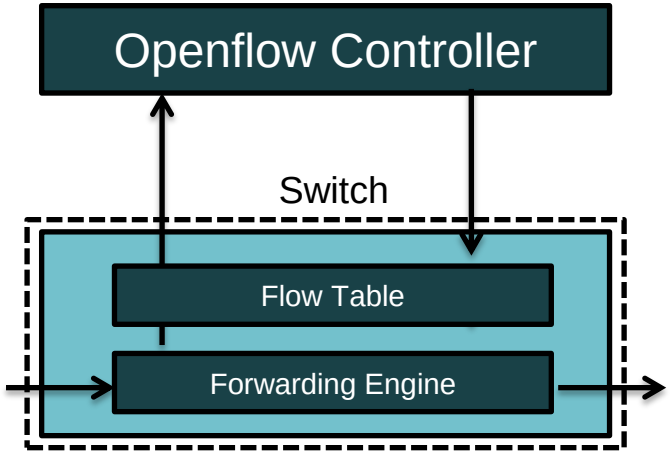


MLS – Multi Layer Switching



1997

Innovation
(MLS)



Today's

Innovation

A small problem with MLS

IT DID NOT <u>SCALE</u>

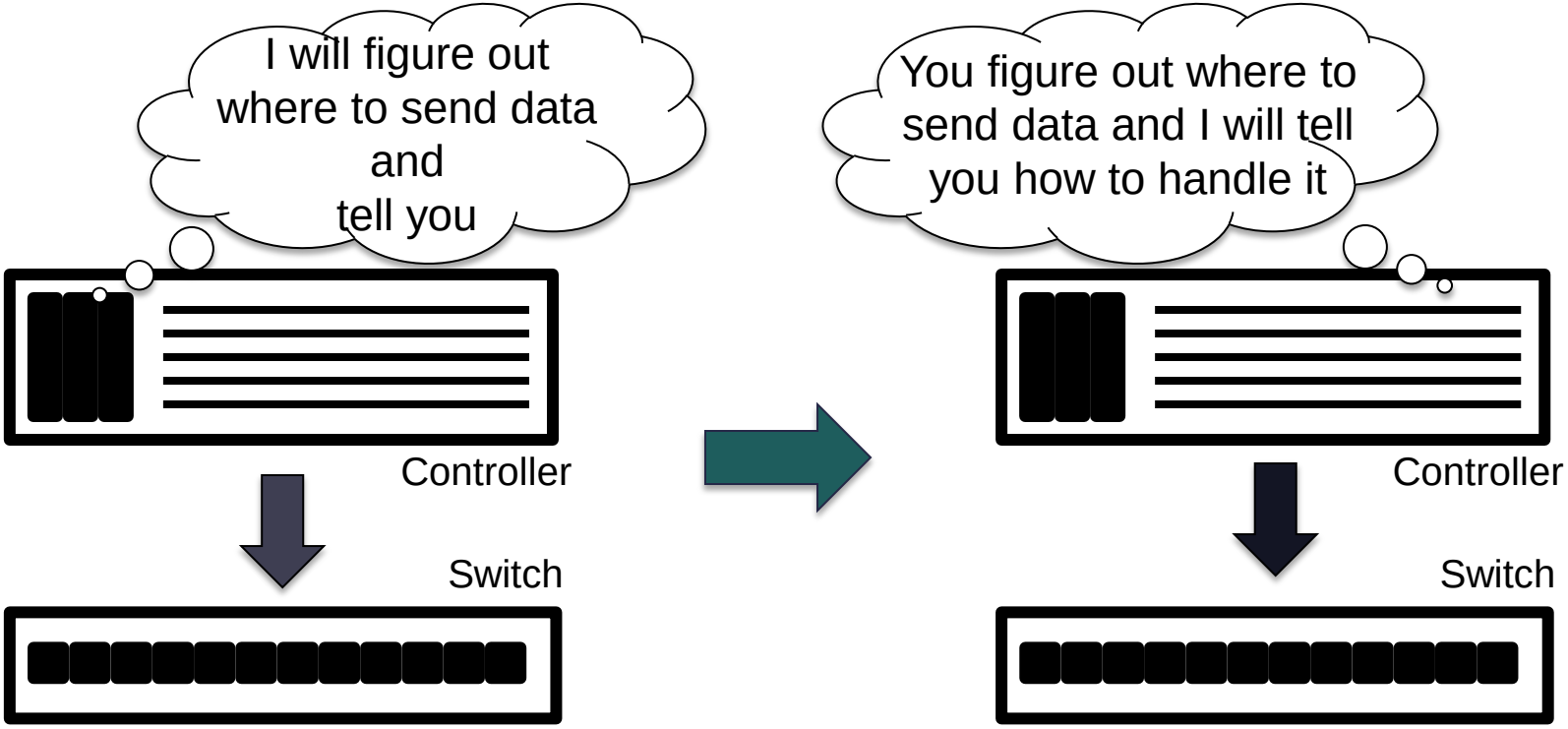
Cisco's *Forwarding* Evolution

MLS
Multi-Layer Switching

→

CEF
Cisco Express Forwarding

Cisco moved to CEF to overcome MLS ***Scalability*** issues



Imperative Model
(Openflow Forwarding Model)

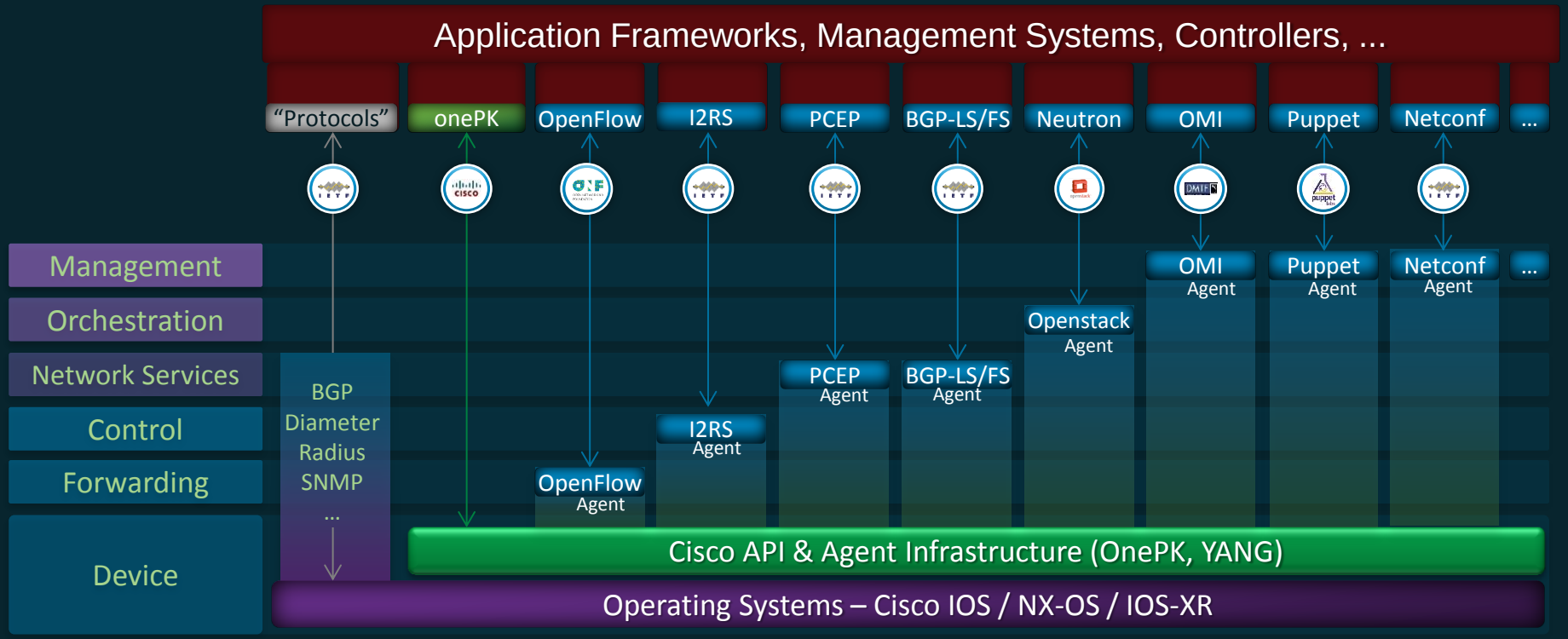
Declarative Model
(ACI Group Policy Model)

SDN

It’s Not About Southbound Protocols

It’s About Controlling Network Behavior through Software in a Programmatic way

SDN Internet protocols



L3 device: Specific API's & Protocols

Router has different tables to control

- Higher-level abstraction

SDN Controller

If I want something simple…

- add route, delete route
- add VRF, add ACL
- create new LSP/Tunnel…

BGP-LS/FS/EVPN, SR

I2RS

PCEP, I2RS

IPSE, OVSDB

Openflow focus

Routing Protocols

BGP | OSPF | ISIS | LDP | … | XYZ

RIB

FIB

Features (QoS, ACL, Netflow…)

Interface Mgmt.

Platform Specific Control Plane

Drivers, HAL, SDK

ROUTER FORWARDING ENGINE (NPU)

Router

Problem Statement

What Does It Really Mean?

Complexity

Higher
OPEX

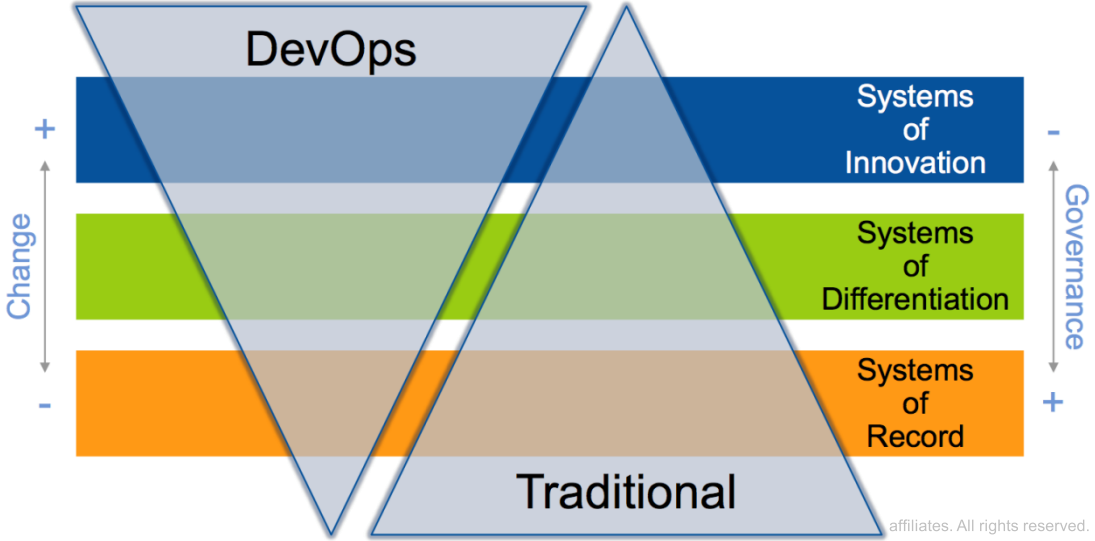
Lower
Business Agility

The Pace of IT – Bimodal IT

Gartner

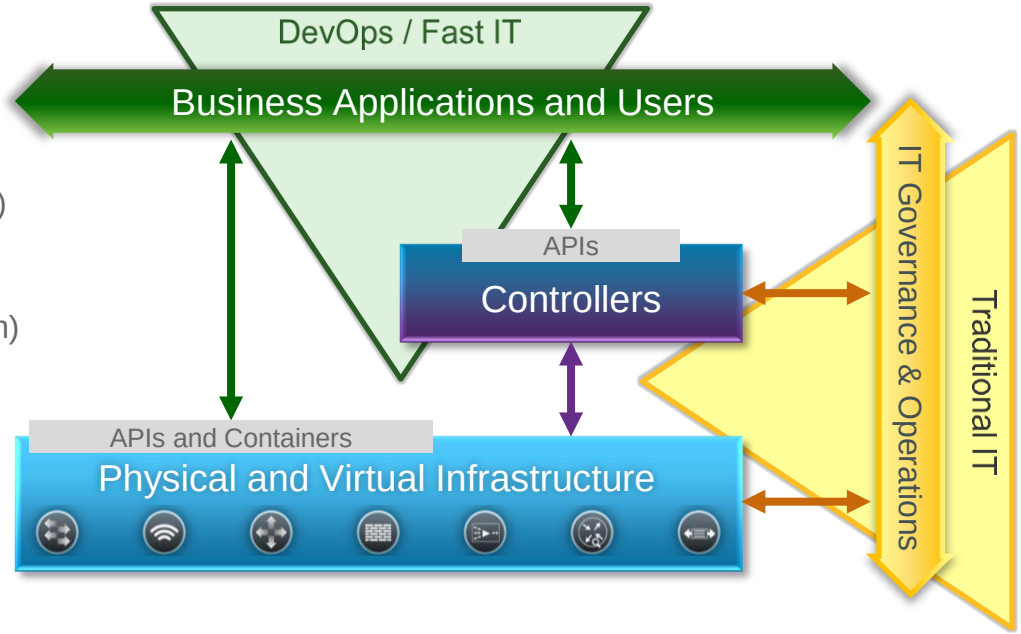
Problem: CIOs are challenged to keep running existing IT more efficiently and safely, while enabling business innovation and differentiation at a quickening pace.

Solution: Bimodal IT, enabling developers and enabling governance



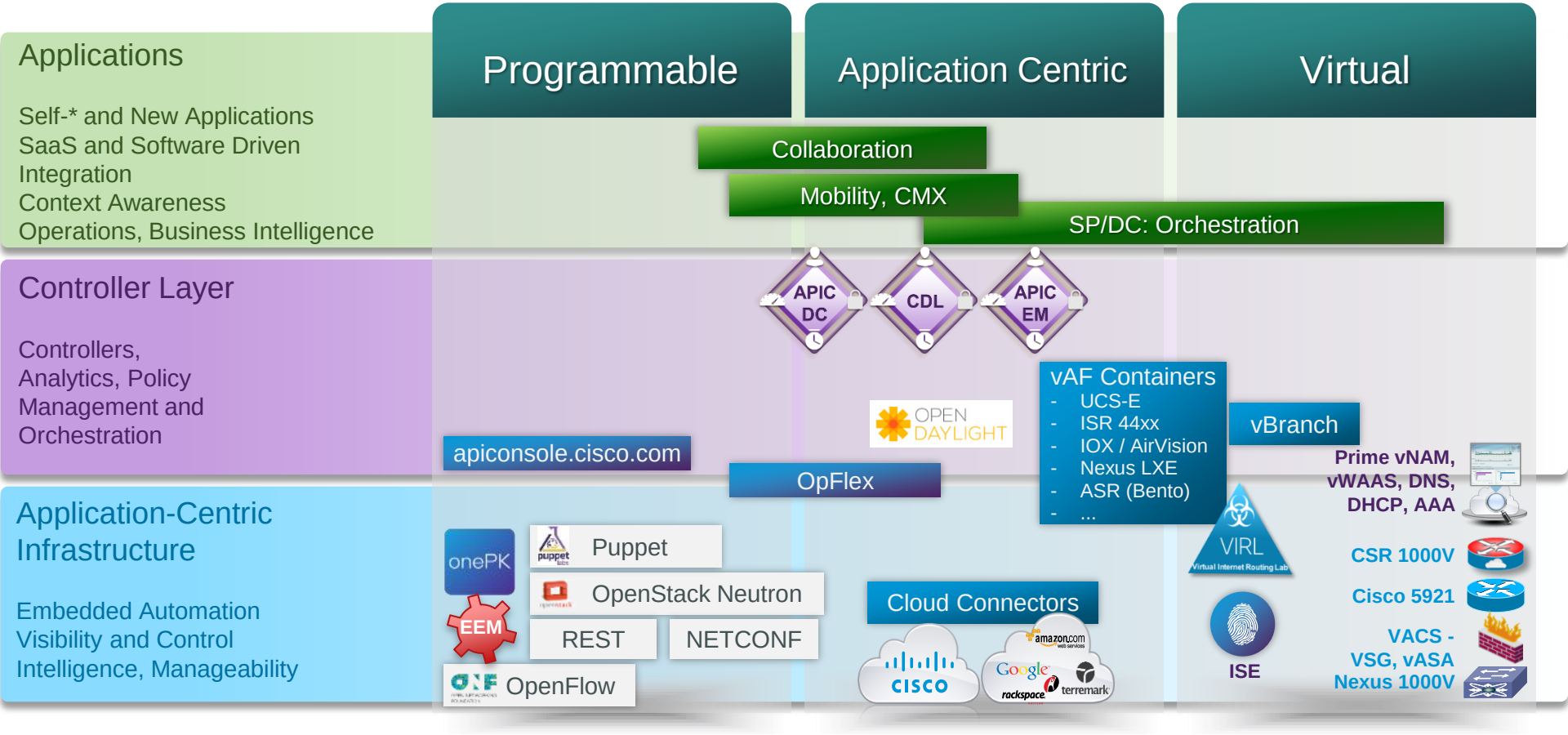
Ingredients of Bimodal Architectures

- **Application Centricity**
- **Programmability** of
  - Infrastructure (RESTCONF + many)
  - Controllers (REST)
  - Services (apiconsole.cisco.com)
- **Virtualization** of
  - vAF: Application Functions
  - vMF: Management Functions
  - vNF: Network Functions

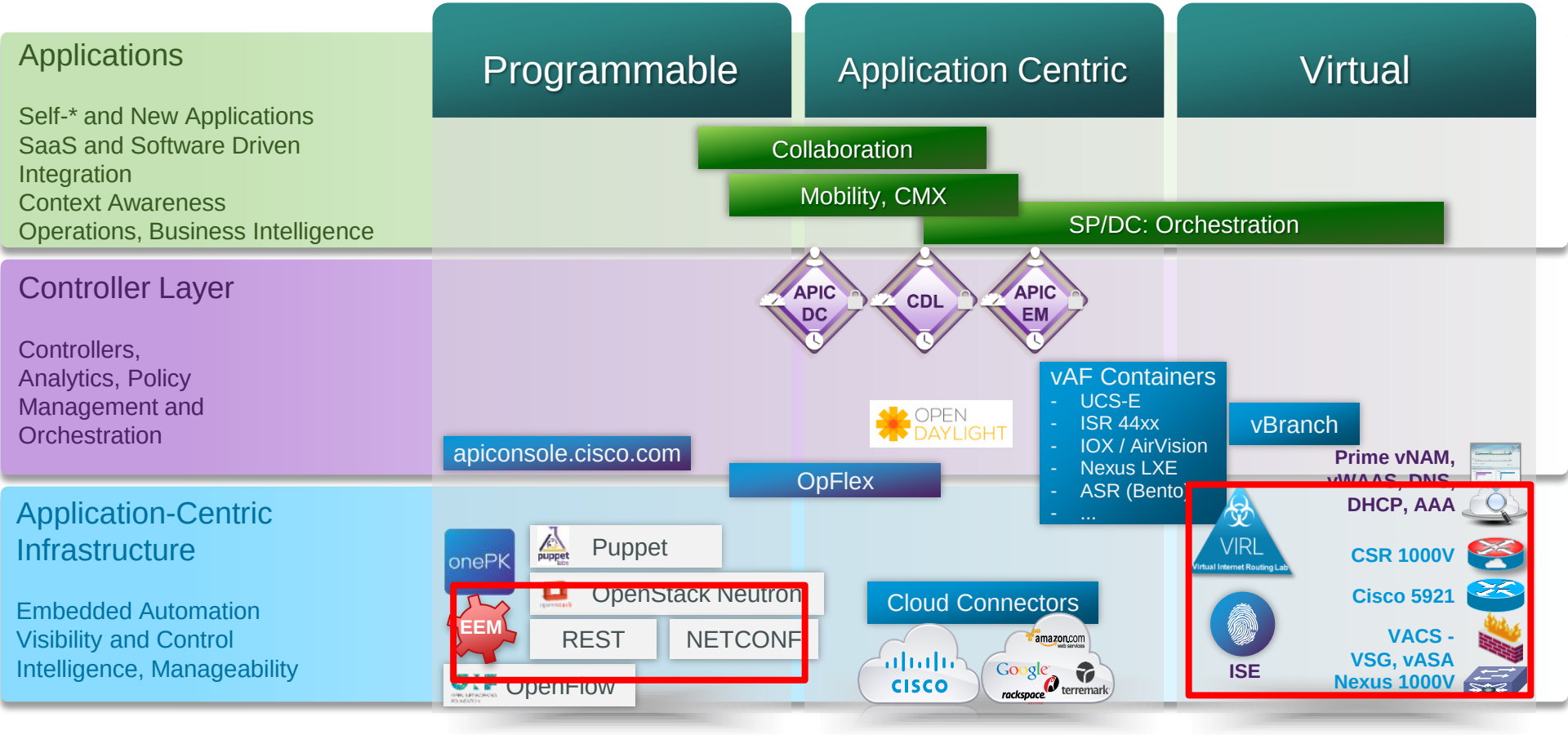


Bimodal IT Architectures to support Fast IT Business Needs

Cisco Enterprise ACI – 3x3 Portfolio (Subset)

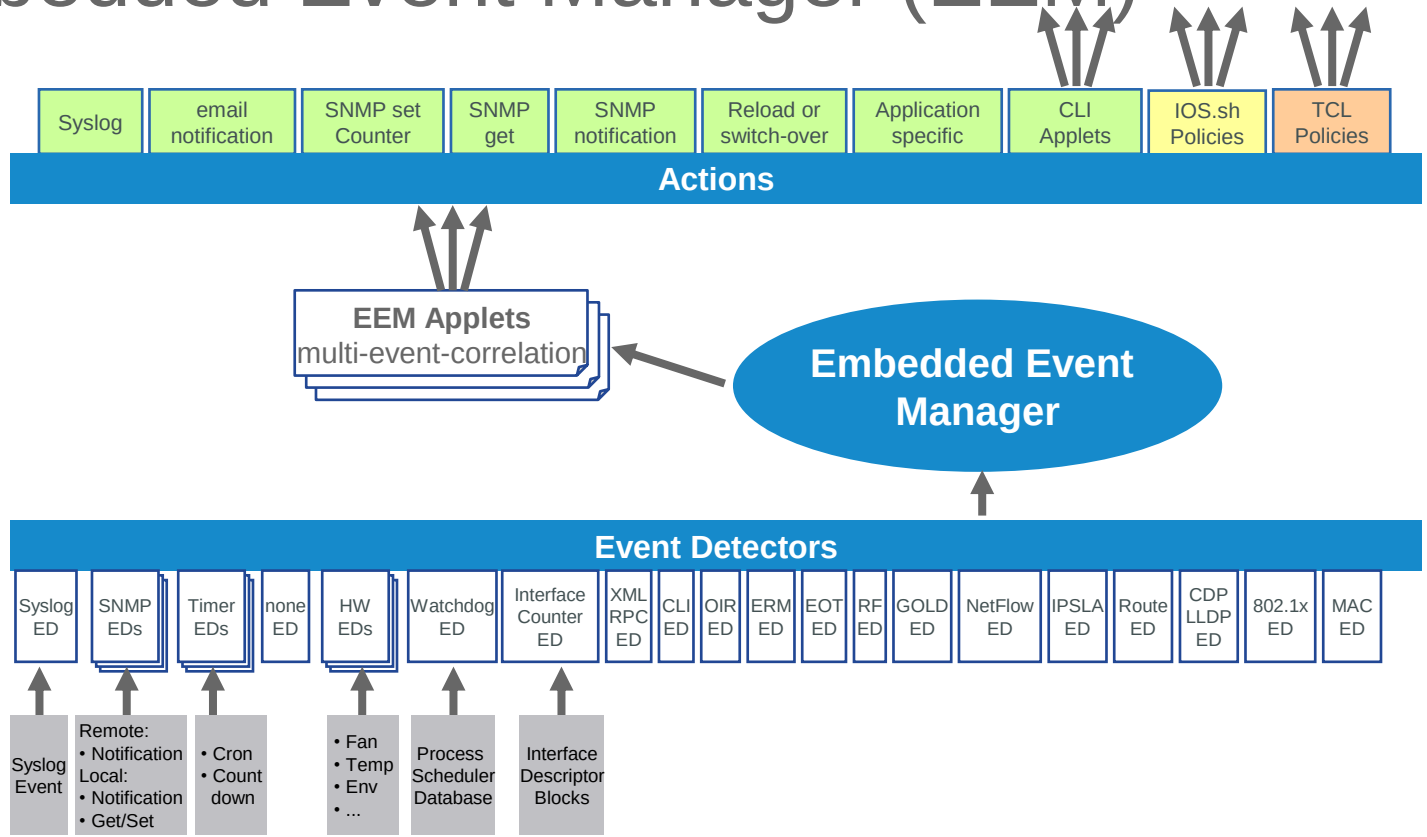


Cisco Enterprise ACI – 3x3 Portfolio (Subset)

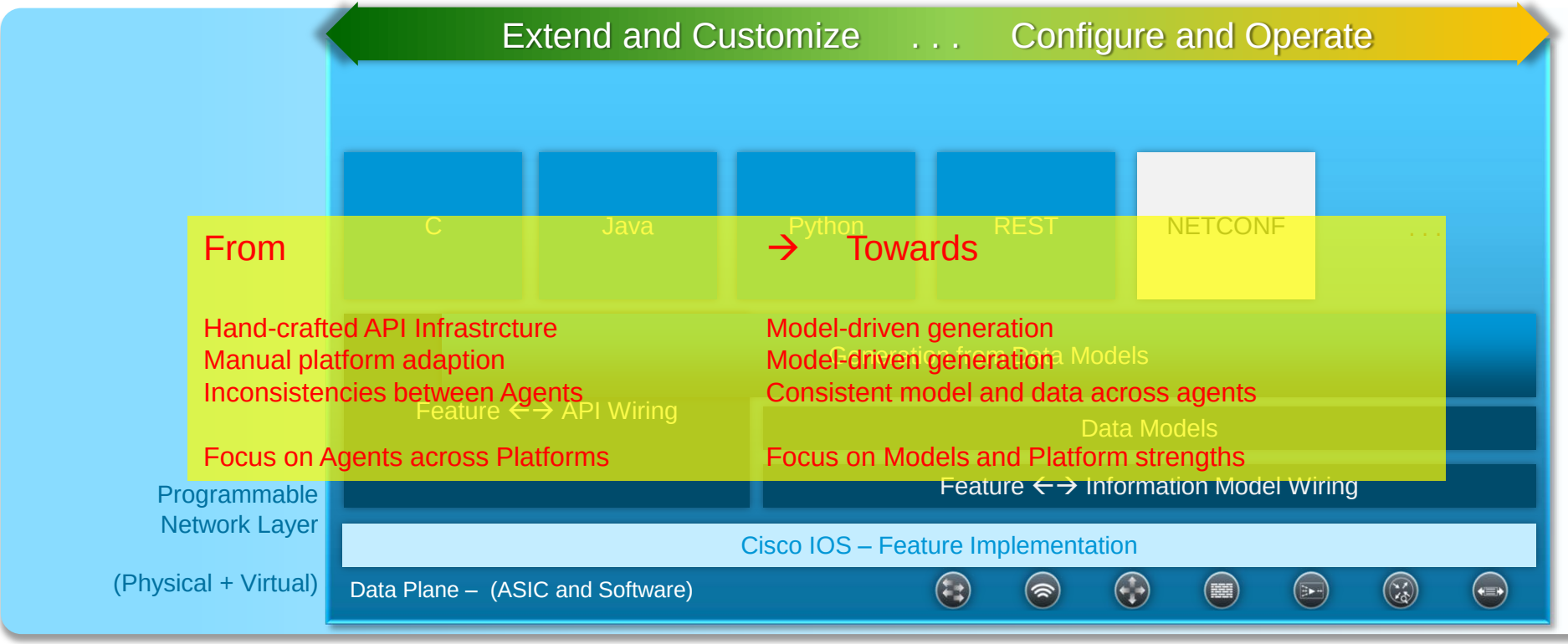


Focus: Programmable Network Layer

Embedded Event Manager (EEM)



Programmable Network Layer – Evolution



From

Hand-crafted API Infrastrcture
Manual platform adaption
Inconsistencies between Agents

Focus on Agents across Platforms

→ **Towards**

Model-driven generation
Model-driven generation
Consistent model and data across agents

Focus on Models and Platform strengths

Programmable Network Layer – Hosting Models

Choice of 3 Hosting Models

"Process"

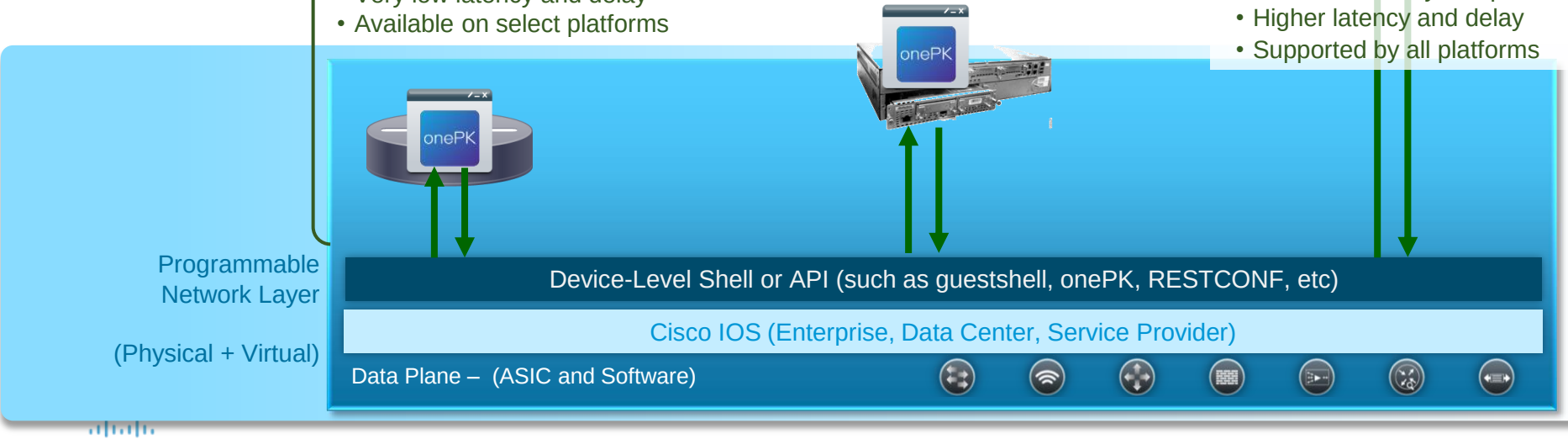
On the Node
- Shared memory/compute
- Very low latency and delay
- Available on select platforms

"Blade"

On A Hardware Blade
- Dedicated memory/compute
- Low latency and delay
- Requires modular hardware blade

"End-Node"

On An External Server
- Plentiful memory/compute
- Higher latency and delay
- Supported by all platforms



vAF

Focus: Virtual

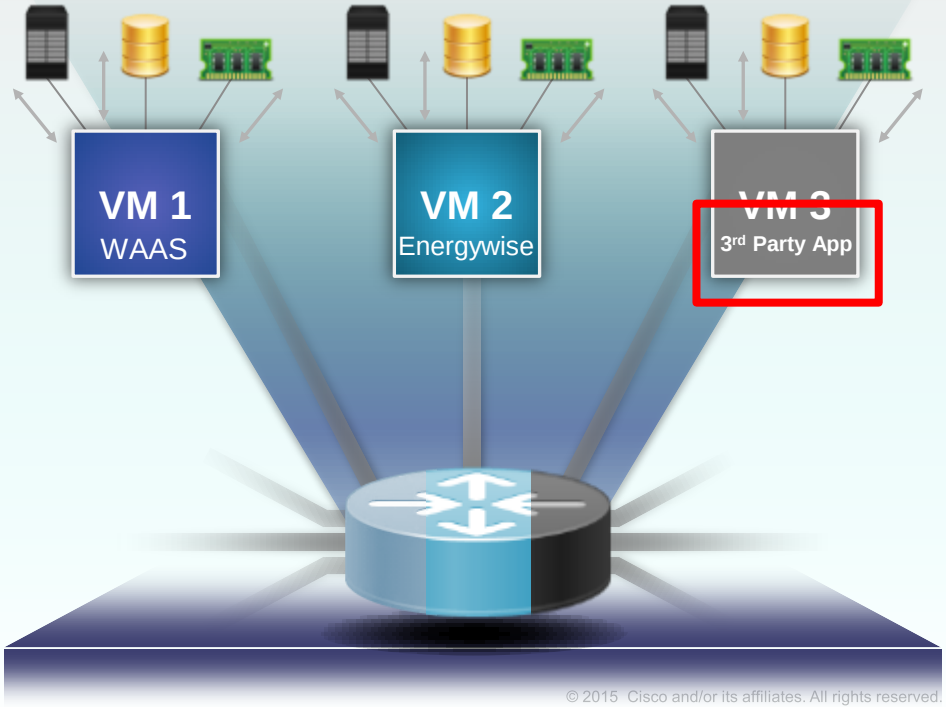
Virtual Containers – ISR 4400 Series

Service Containers

- Dedicated virtualized compute resources
- CPU, disk, memory for each service
- Easily repurpose resources
- Industry-standard hypervisor

Benefits

- Better performing network services
- Ease of deployment with zero footprint; no truck roll
- Greater security through fault isolation
- High reliability
- Flexibility to upgrade network services independent of router IOS® Software



vNF

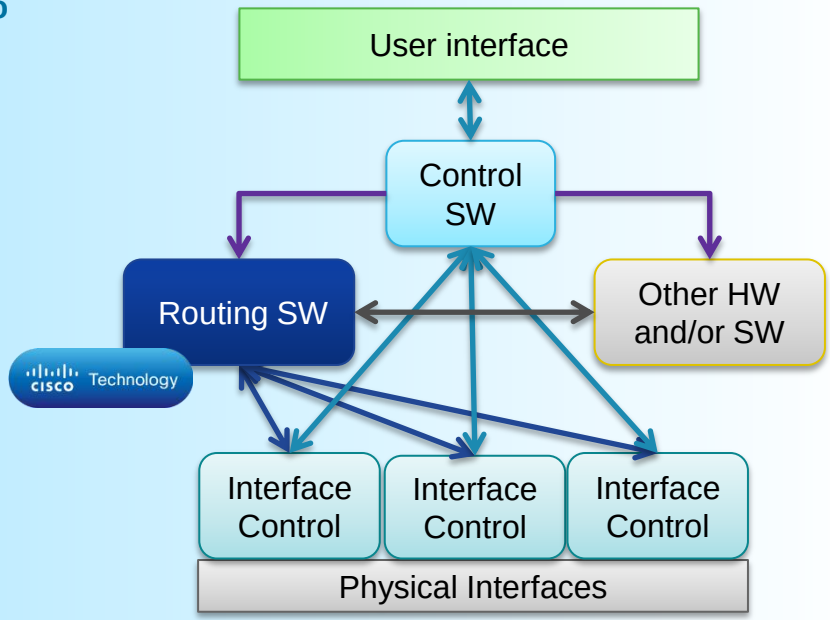
Focus: Virtual

vNF – **Embedded** Services Router – ESR 5921

The Cisco 5921 Embedded Services Router (ESR) is a Cisco IOS® software router application designed to operate on small, low power Linux-based platforms to extend the use of Cisco IOS into extremely mobile and portable communications systems.

- based on IOS 15.2(4)GC , synched to 15.2(4) M
- Includes special mobility features (Radio Aware Routing, ...)
- Up to 20 virtual Eth ports
- x86 compatible, 32 bit Linux application
  - Can run on any x86 compatible hardware with sufficient resources:
    - x86 - e.g., Intel Atom and Intel Core i3/i5/i7
    - 512 MB RAM minimum
    - 300 MB Disk minimum
    - glibc compiled Linux
- Embedded by SI into final Product, using "Cisco Technology Inside" software
  - Sensors, Portable Communications, Vehicular Communications, ...

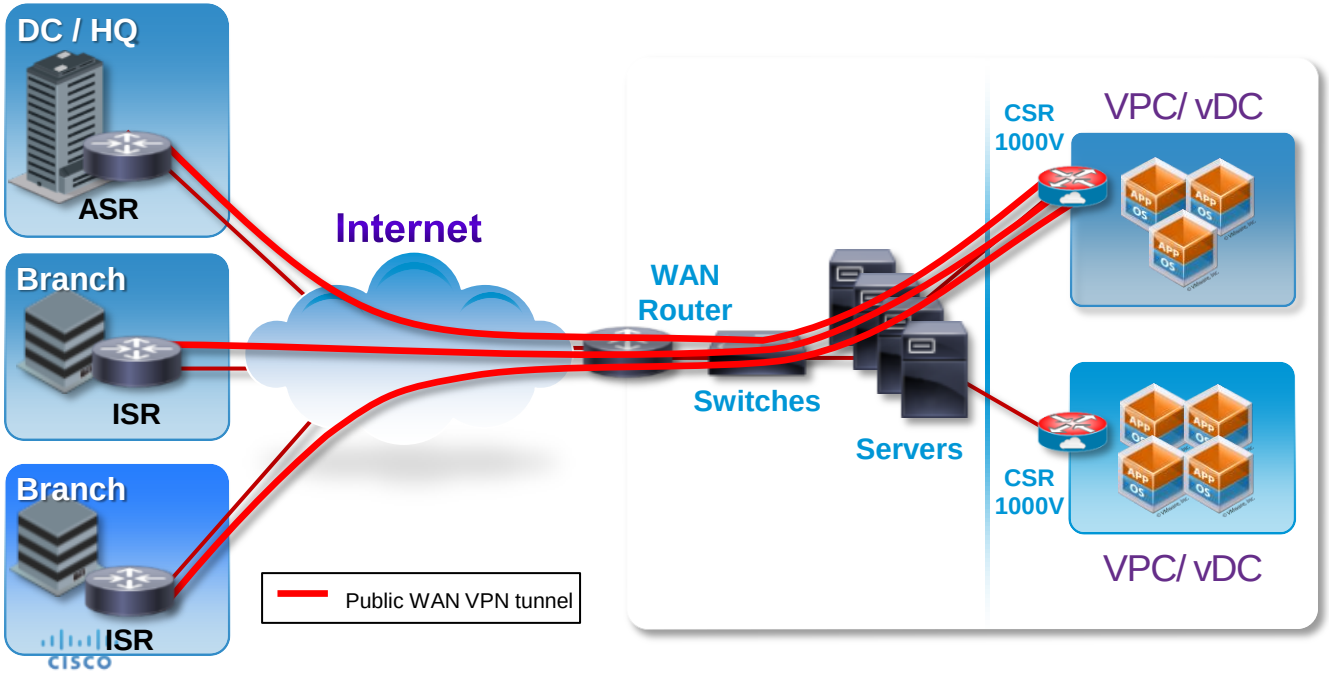
Typical Use Case



Example: Secure VPN Gateway

Problem: How to securely connect to a virtual private cloud or virtual Data Centre where we can't deploy Hardware – across the public Internet?

Solution: Deploy VPN Gateway on Cloud Services Router 1000v



Challenges

- Inconsistent Security
- High Network Latency
- Limited Scalability

Solutions

- IPSec VPN, DMVPN, EZVPN, FlexVPN
- Routing and Addressing
- Firewall, ACLs, AAA

Benefits

- Direct, Secure Access
- Scalable, Reliable VPN
- Operational Simplicity

vNF – Network Simulations

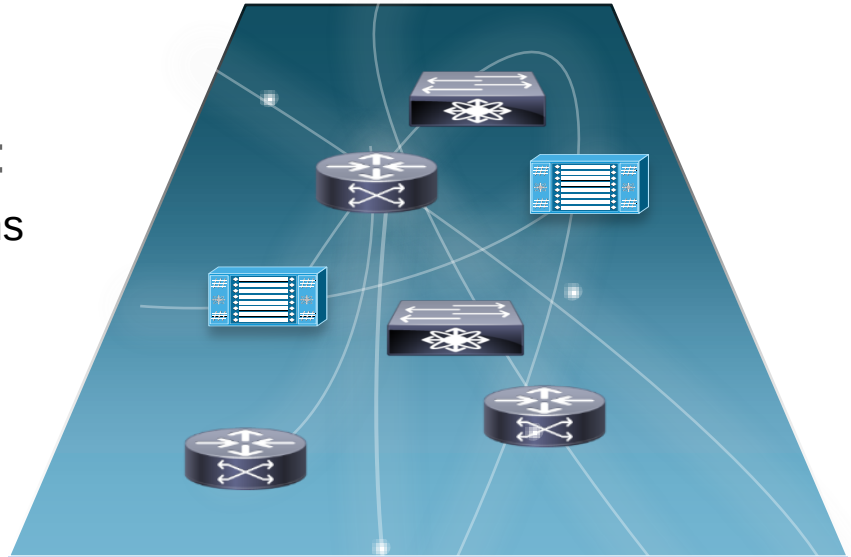
The Challenge

Developers have a compelling need to:

- Create new network applications and solutions
- Learn and test new features and facilities
- Innovate to solve business problems

To do this they need a Lab that is:

- Easy to build
- Easy to (re-)configure
- Easy to scale
- Easy to access
- Portable
- Inexpensive



Network Simulation

Such a Lab did not exist … until VIRL.cisco.com

vMF

Focus: Virtual

vMF – Driving Visibility from Network Control

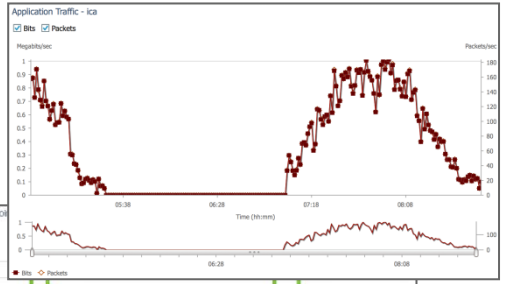
Problem: How to dynamically provide application visibility into remote sites or per virtualized tenant?

Solution: Deploy vNAM into the virtual workload POD

Network Application

REST/XML API

Cisco Daylight (XNC)

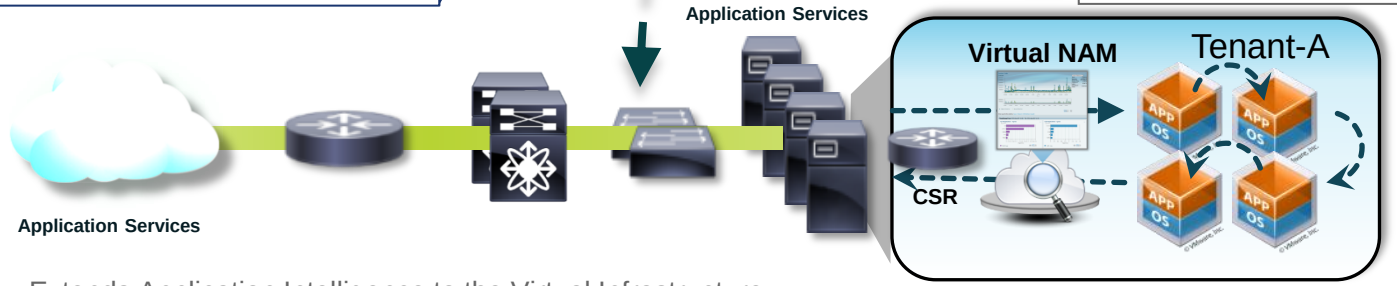


Service Assurance Actions (Examples)

- Apply Service Policies (Police, Mark, Shape, Queue) for reprioritization
- Implement custom routing optimized for specific application topology
- Set ACLs to establish the access rules

PROGRAMMABILE

Traffic Steering
Path Setup
Traffic Engineering

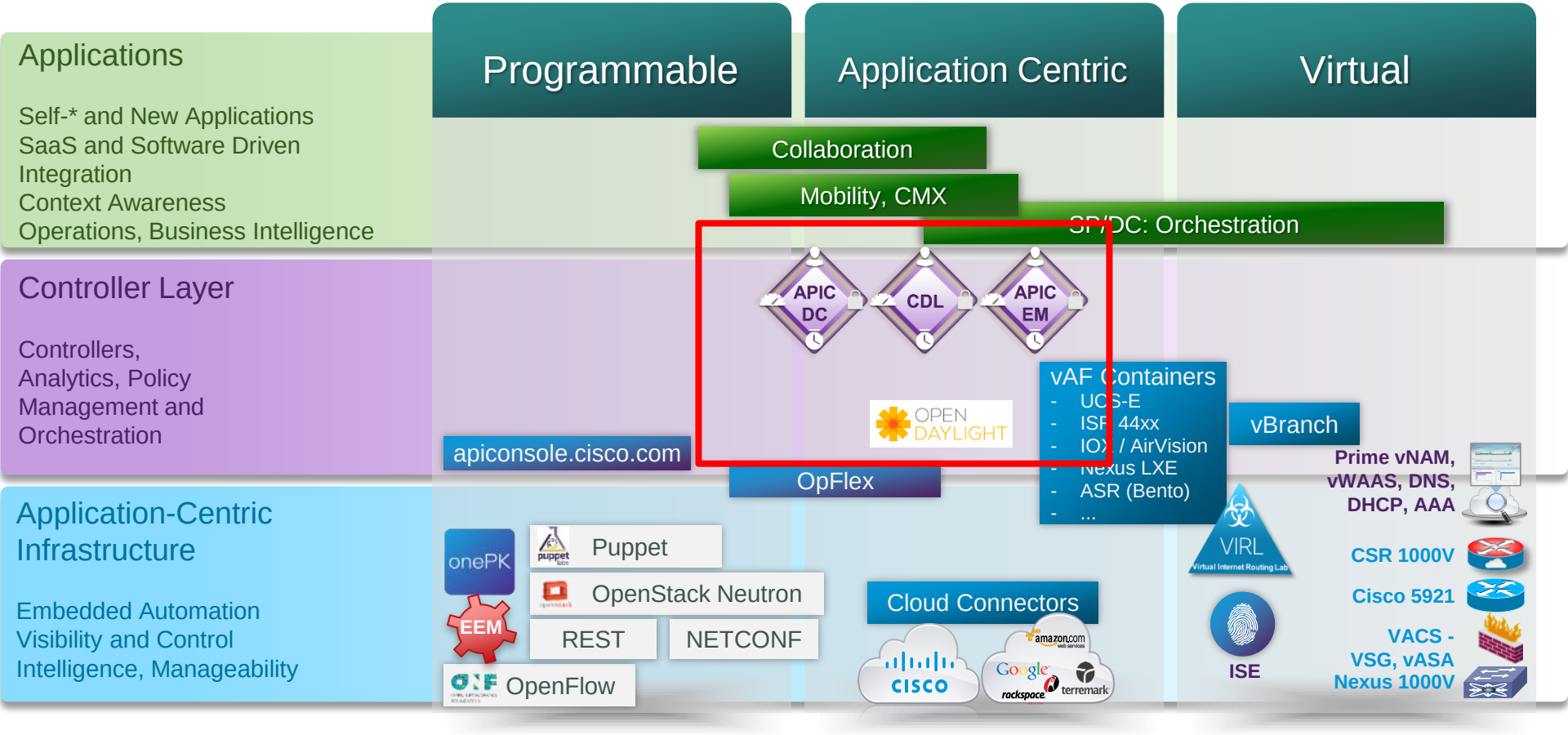


Hosted Workload for Tenant

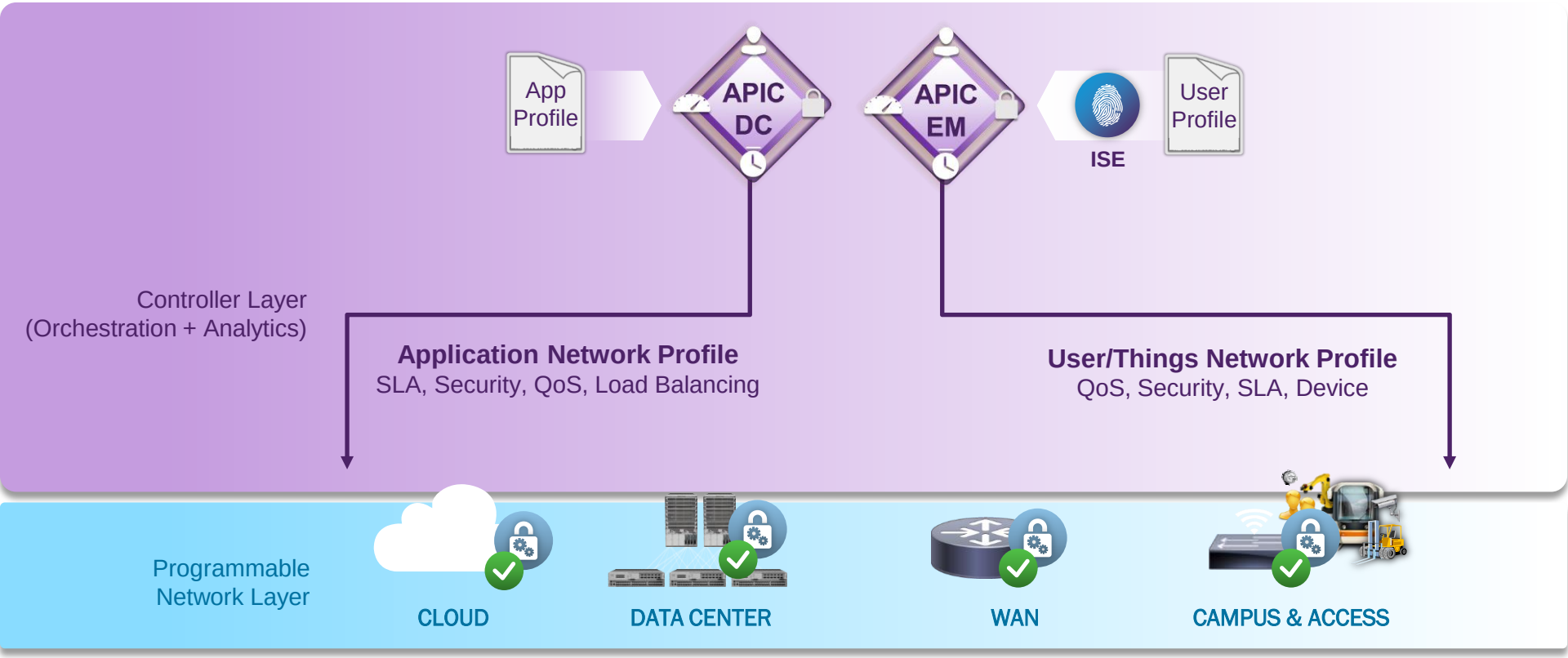
Extends Application Intelligence to the Virtual Infrastructure

Focus: Controller Layer

Cisco Enterprise ACI – 3x3 Portfolio (Subset)

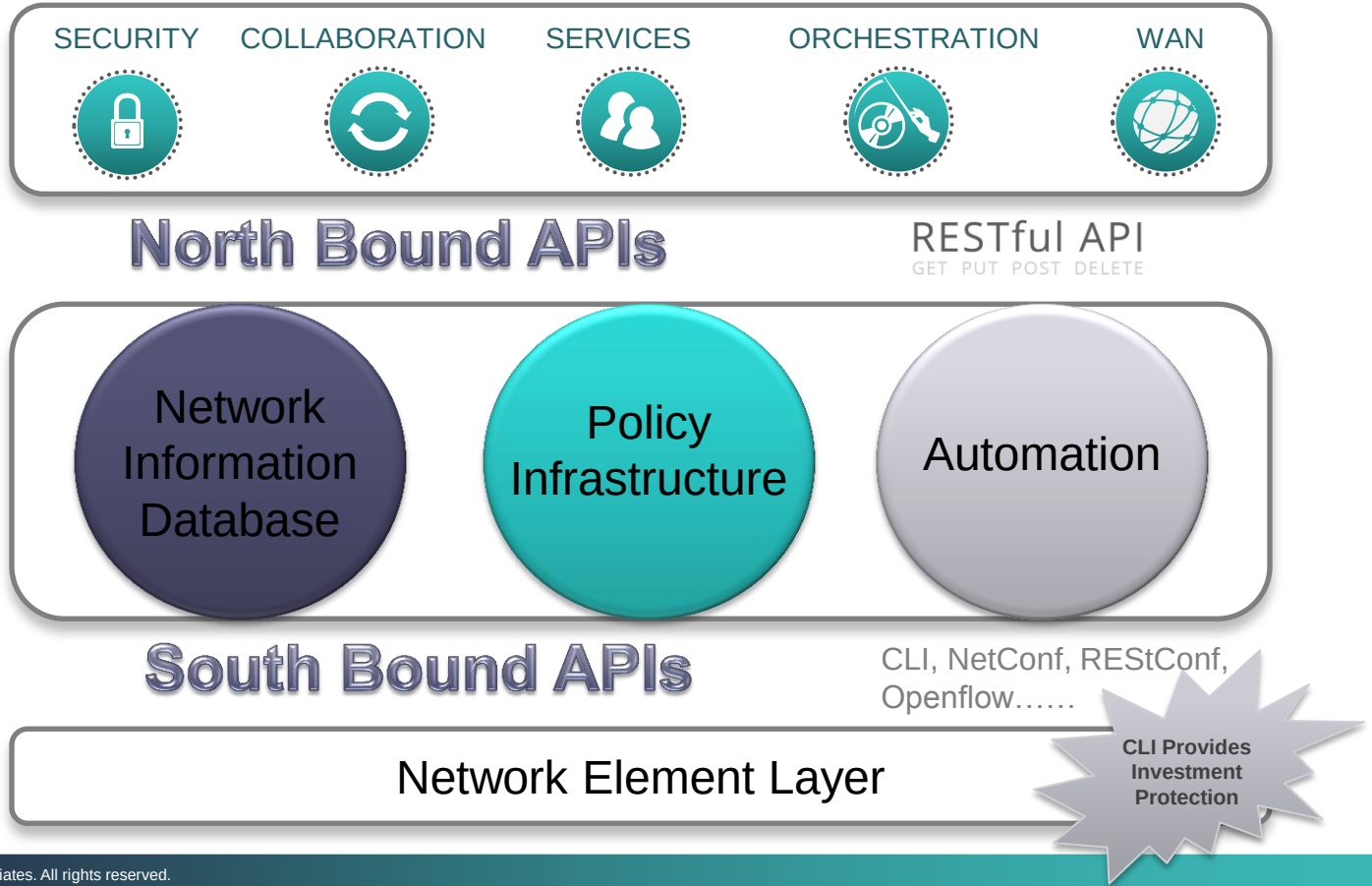


Common Policy Across Domains



Controller Architecture

High Level



Conventional

Admin Driven

The **What**

"Security Policy for Branches A-N"

The **How**

"Change ACLs in the Following Elements"

ACI Policy Model

The **What**

"Security Policy for Branches A-N"

Admin Driven

API

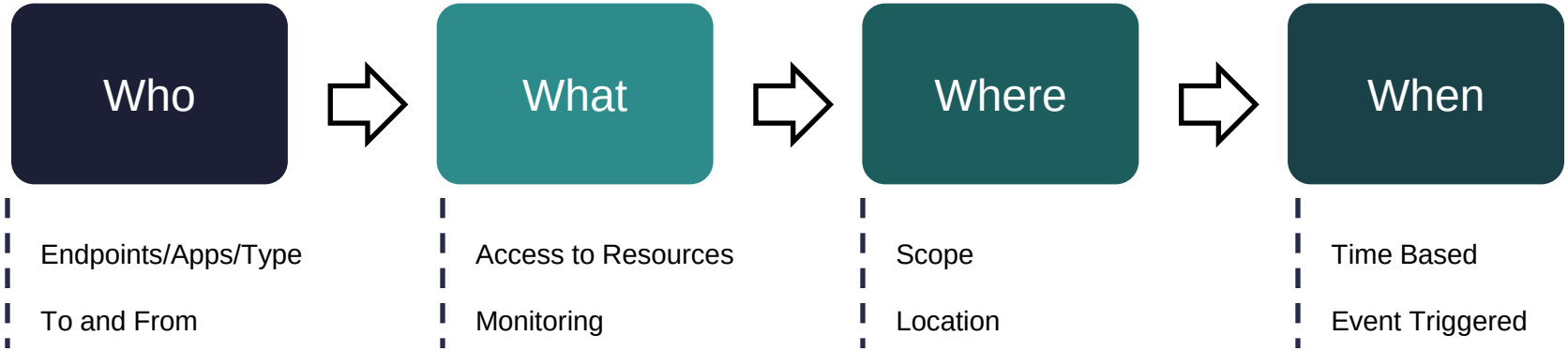
The How

"Change ACLs in the Following Elements"

APIC EM Driven

Lower OPEX and Better LOB Alignment Agility

What is a Policy…



Policy Examples….

- Engineering Group (Who: From)
  - Engineering Applications (Who: To)
    - Laptop (Who: Device Type)
      - Permit (What: Action)
        - Properties: priority level - high, trust level – high (What: Action Properties)

- Tom (Who: From)
  - Netflix(Who: To)
    - Permit (What: Action)
      - Properties: priority level – Low, trust level – low (What: Action Properties)
        - 11AM-1PM (When: Time)

Under The Covers

```
{"policyName":"tomweballow","policyOwner":"Admin","policyP[illegible]ty":4095,"
networkUser":{"userIdentifiers":["tom"]},"resource":{"[illegible]s":["80,80,tcp"]},
"actions":["PERMIT"]}
```

```
CompositeNetworkPolicy [networkPolicy=NetworkPoli[illegible]0be-adaf-4f41-bfb7-
d1d9ee01e0f8,
creatorUserId=Admin, policyName=bradweball[illegible]y=4095,
businessPolicyId=10d7e374-c1e0-4190-b3[illegible]
flowId=7ba2034a-3cb0-4877-ae14-4a6[illegible]
actionId=70fb3b4c-ccf8-4561-b49[illegible]
flow=Flow [flowId=7ba2034a-[illegible]c33aac312,
srcIp=10.10.30.2, srcIpM[illegible] protocol=tcp, srcTptPortLower=0,
srcTptPortUpper=0, d[illegible], dstTptPortUpper=80], flowAction=FlowAction
[actionId=70fb3b4c-[illegible]684e5dc8d3cd, action=permit, actionPropDscp=-1, ]]
```

```
CLI = config t, ip acc[illegible]s-list extended User-Acl--8653840507576742282,
10 permit tcp host 10.10.30.2 any eq 80,
interface GigabitEthernet1/0/4, ip access-group User-Acl--8653840507576742282 in, end
20:22:28.992 EST DEBUG c.c.c.qos.acl.AclPolicy - Acl Policy Created Successfully on the
Device : d29d175f-aacc-4c9c-a290-2392fc80a0e3
```

Completely Hidden!

Let’s Look At Some Apps

Network Information Base

One Source of Truth

APIC - Enterprise Module

API | Sign Out | 0

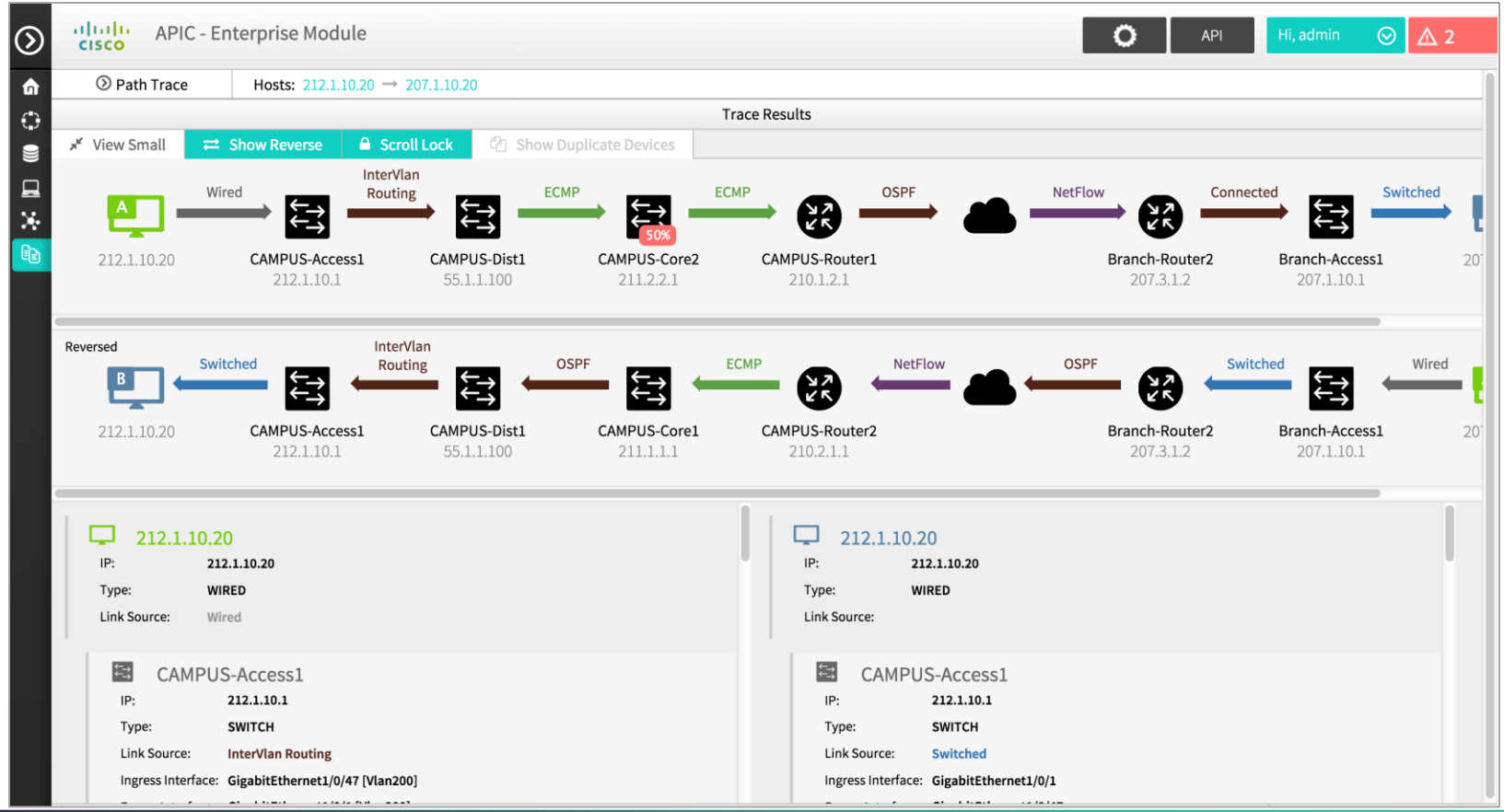
Filters | Layout: Hardware

	Device Name	MAC Address	IP Address	IOS/Firmware	Platform	Serial Number	Config	Device Role
	SDN-BRANCH-2960S	5C:50:15:BF:6D:C0	40.0.5.4	15.2(1)E2	WS-C2960S-24TS-L	FOC1612W32Z	View	Access
	SDN-BRANCH-2960S-STACK	00:26:52:7D:2C:C0	40.0.7.5	15.2(1)E2	WS-C2960S-48FPD-L	FOC1412Z2KG	View	Access
	SDN-BRANCH-3560CG	1C:AA:07:63:8B:40	40.0.5.7	12.2(55)EX	WS-C3560CG-8PC-S	FOC1516W4XR	View	Access
	SDN-BRANCH-3560X	60:73:5C:EF:13:40	40.0.5.9	15.2(1)E2	WS-C3560X-48U	FDO1634Z049	View	Access
	SDN-BRANCH-3650	F8:72:EA:0D:67:47	40.0.7.3	03.03.00SE	WS-C3650-24PD	FDO1733Q02X	View	Access
	SDN-BRANCH-3750X	2C:54:2D:93:1E:40	40.0.7.4	15.2(1)E1	WS-C3750X-48P	FDO1612P1XA	View	Access
	SDN-BRANCH-AP1252-1	00:26:CB:7E:D2:DC	40.0.5.39	15.2(20130113:221158)$	AIR-LAP1252AG-A-K9	FTX133590NE	View	Access
	SDN-BRANCH-ASR1002	78:DA:6E:13:5E:00	40.0.3.6	15.2(4)S3	ASR1002	FOX1737GJVL	View	Border Router
	SDN-BRANCH-C2960S-L	70:10:5C:5A:47:C0	40.0.5.6	15.2(1)E2	WS-C2960S-48TS-S	FOC1709Z006	View	Access
	SDN-BRANCH-C4K	A8:0C:0D:98:CA:7F	40.0.5.2	03.03.00.XO	WS-C4510R+E	FXS1749Q1LC	View	Distribution

10 | 25 Devices | First Previous 1 Next Last

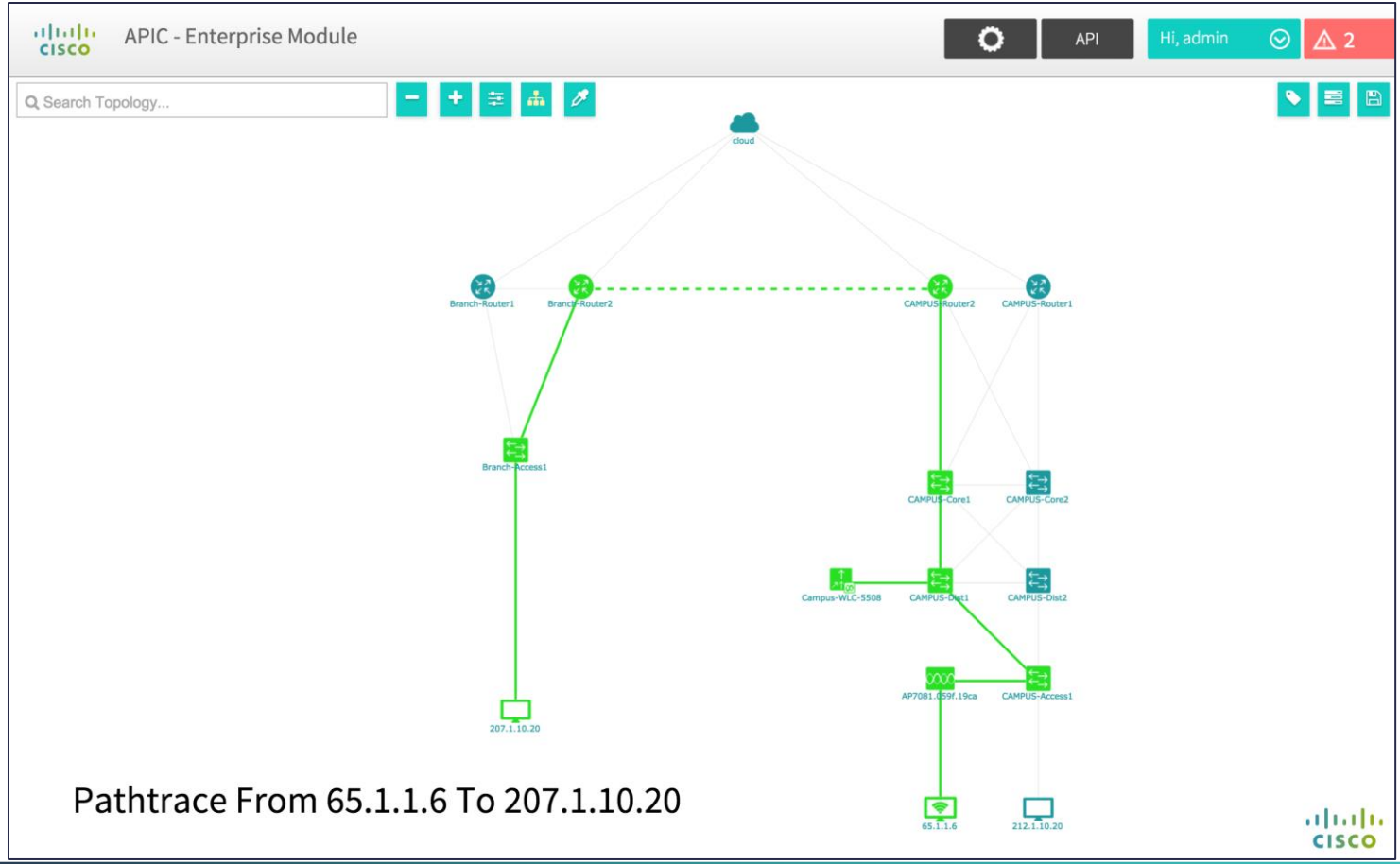
Path Trace

Enhanced Application Flow Visibility



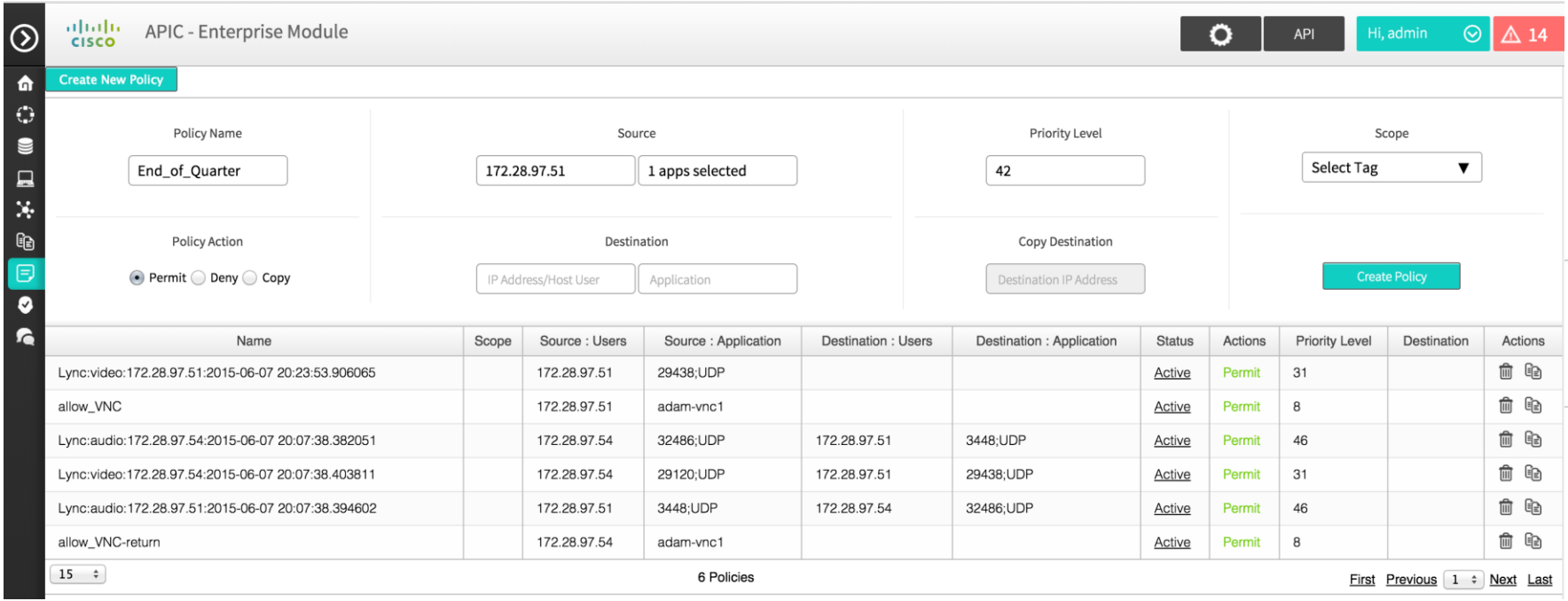
Path Trace

Topology View



Intent Based Policies - Controller View

Easily Express Business Requirements



- Based on Users, Resources, Actions and Priorities
  - Integrates with IS/AAA/LDAP for Host user
    - Supports Tagging - e.g. can apply an ACL to a given site/branch

Plug and Play
Auto Device Provisioning

APIC - Enterprise Module

API | Sign Out | 0

Status | Sites | Image Management | Unclaimed Devices

Site: Building1

Load | Create | Clone | Delete

☐ Deploy devices that Do not Support Cisco PnP Protocol (Unsecure)

☐ Specify additional site information

Serial Number | * Device Name | * Product ID | Add Rule | Refresh

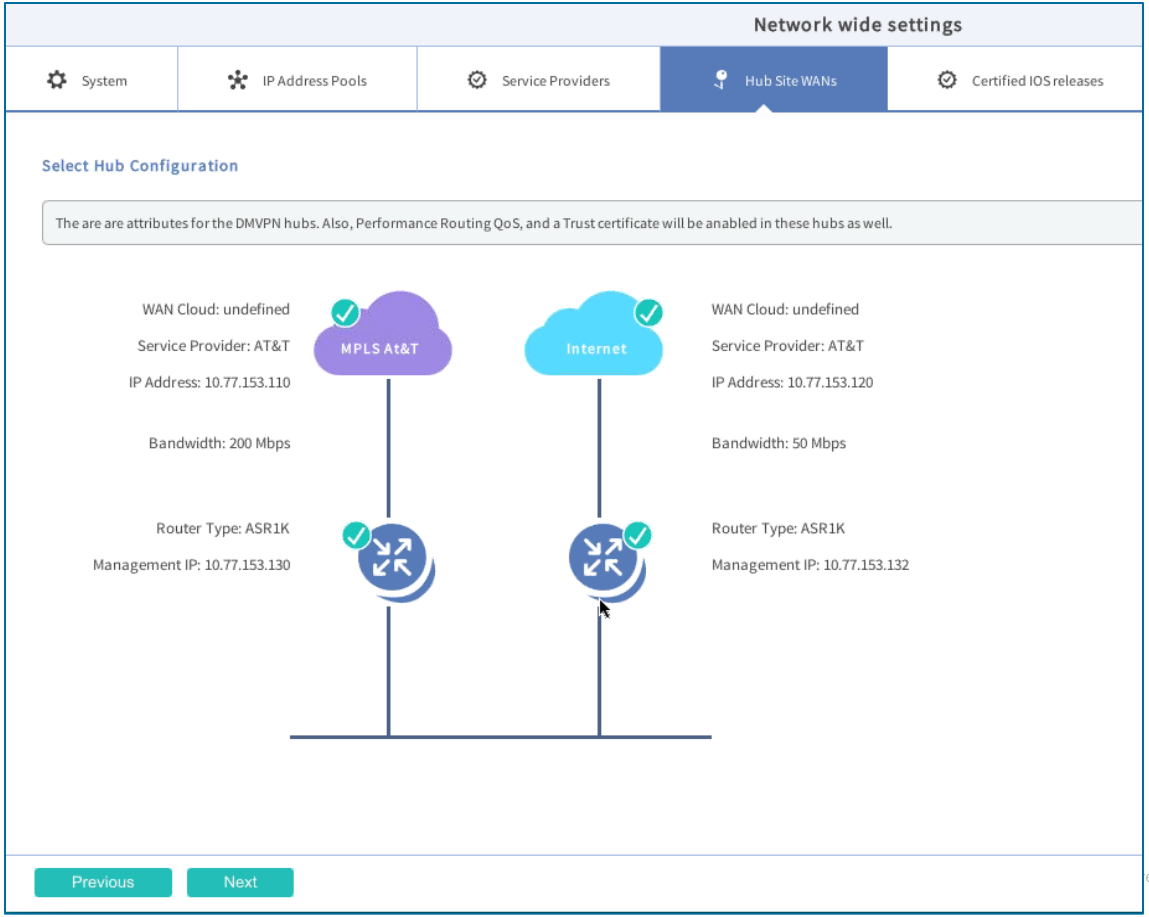
Building1 Devices

Serial Number	Device Name	Product ID	Config	Bootstrap	Image	Details	Status	Delete
FAC1539W110	BLDG1_Floor2_Room1	WS-C3560CG-8PC-S	C3560CX_test1.cfg			Details	PENDING	

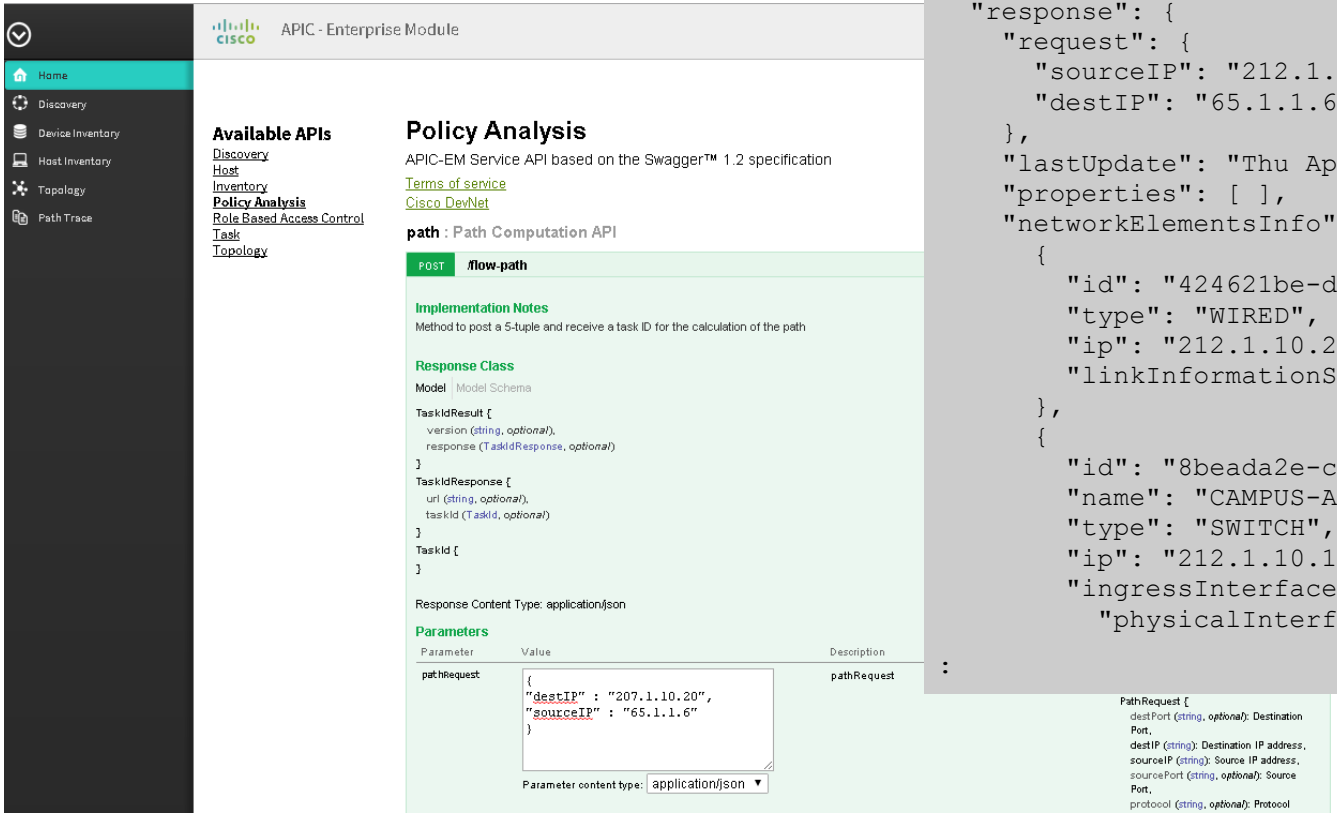
Displaying 1 of 1 Device

APIC-EM IWAN App

Network Wide Settings



API example: APIC-EM Path Visualization and ACL Analysis




```
"response": {
  "request": {
    "sourceIP": "212.1.10.20",
    "destIP": "65.1.1.6"
  },
  "lastUpdate": "Thu Apr 23 01:23:21 UTC 2015",
  "properties": [ ],
  "networkElementsInfo": [
    {
      "id": "424621be-d2b4-4d42-ad16-92d4d5c19fa4",
      "type": "WIRED",
      "ip": "212.1.10.20",
      "linkInformationSource": "Wired"
    },
    {
      "id": "8beada2e-cd2c-421d-941f-3ba42696c489",
      "name": "CAMPUS-Access1",
      "type": "SWITCH",
      "ip": "212.1.10.1",
      "ingressInterface": {
        "physicalInterface": {
```

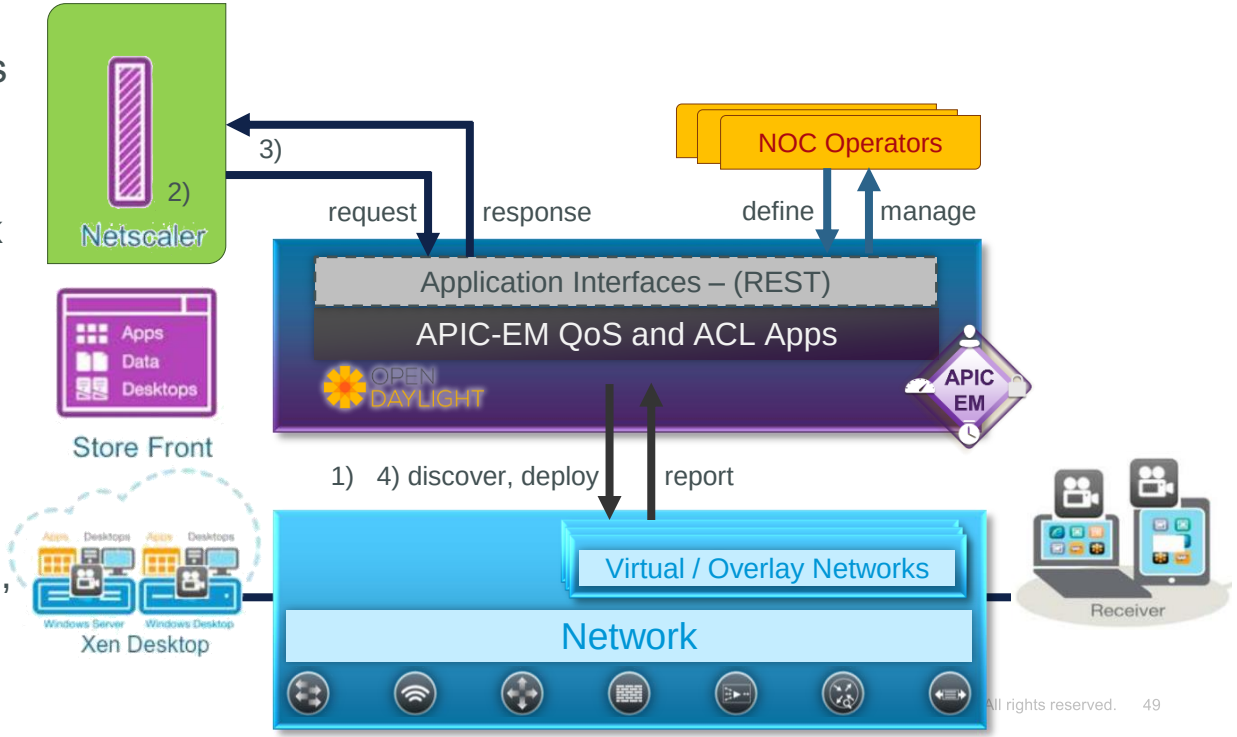

:

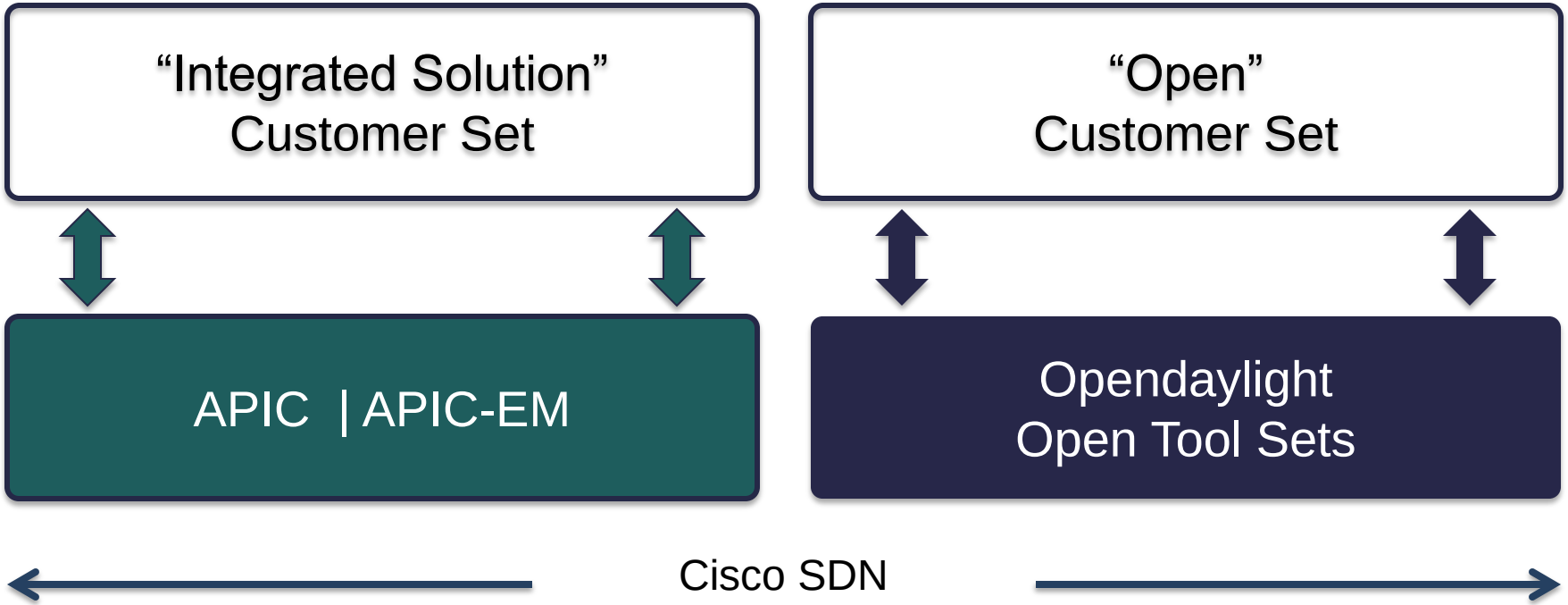
Example: Dynamic Policy for Citrix Clients

Problem: How to provide dynamic application-specific Policy to Citrix XenDesktop users ?

Solution: Use Citrix NetScaler's integration with APIC-EM:

1) APIC-EM discovers network and endpoints
2) NetScaler detects start of (video) data transfer
3) NetScaler requests QoS Policy via APIC-EM's API
4) APIC-EM validates, deploys, and reports the change





Credit: Carl Solder

Controller Layer – Major Milestones

Controller Layer
(Orchestration + Analytics)

Major Milestones of Controller Development

CSDN Controller	CiscoONE Controller	Open Daylight Controller	Cisco XNC Controller	Cisco APIC-EM Controller	Cisco Open SDN Controller
Experimental for Academia	Early Adopter Deployments	Open Source Community Driven	Production Release	Production Release	Best of Both
Indiana University Uni Wisconsin	12+ Customers (Enterprise and Academia)	OPEN DAYLIGHT	XNC 1.0 GA September 2013	Announced CiscoLive '14	OPEN DAYLIGHT EFT Q1 2015
Q4 2011	Q2 2012	April 2013	Sept 2013	Q1 2015	2015 …

Programmable
Network Layer

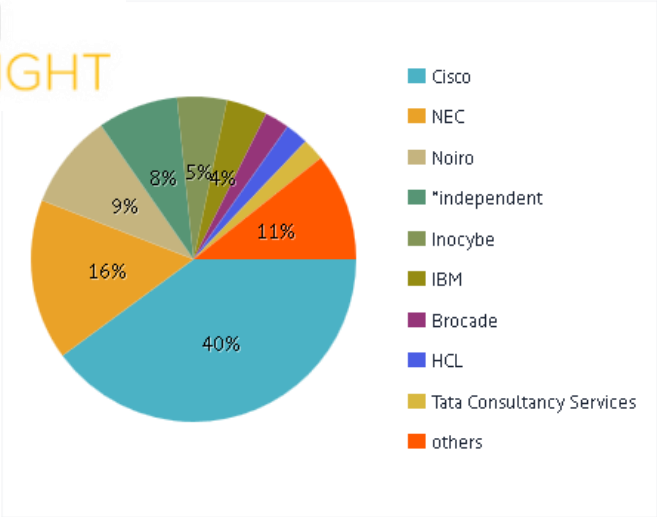
Network

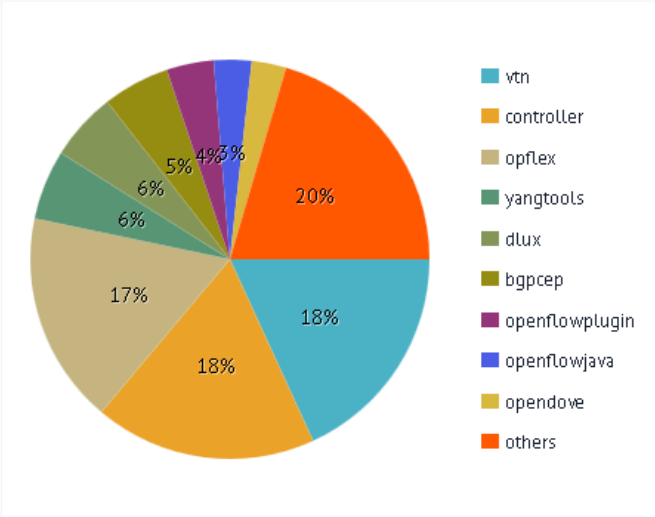
Data Plane – (ASIC and Software)

OpenDaylight – Who is Contributing?

Question: Who are today's top contributors to Open Daylight?

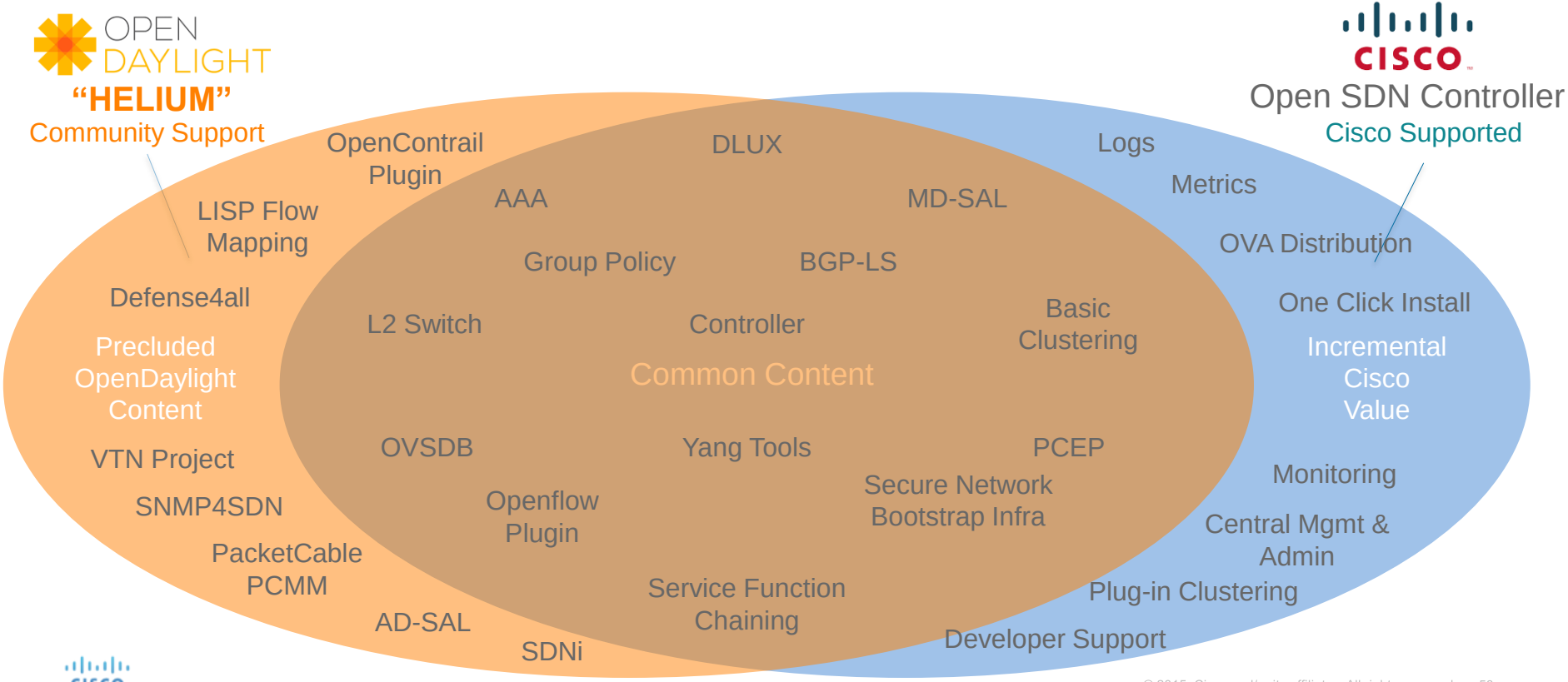
Answer: Check OpenDaylight's Spectrometer (based on OpenStack Stackalytics)





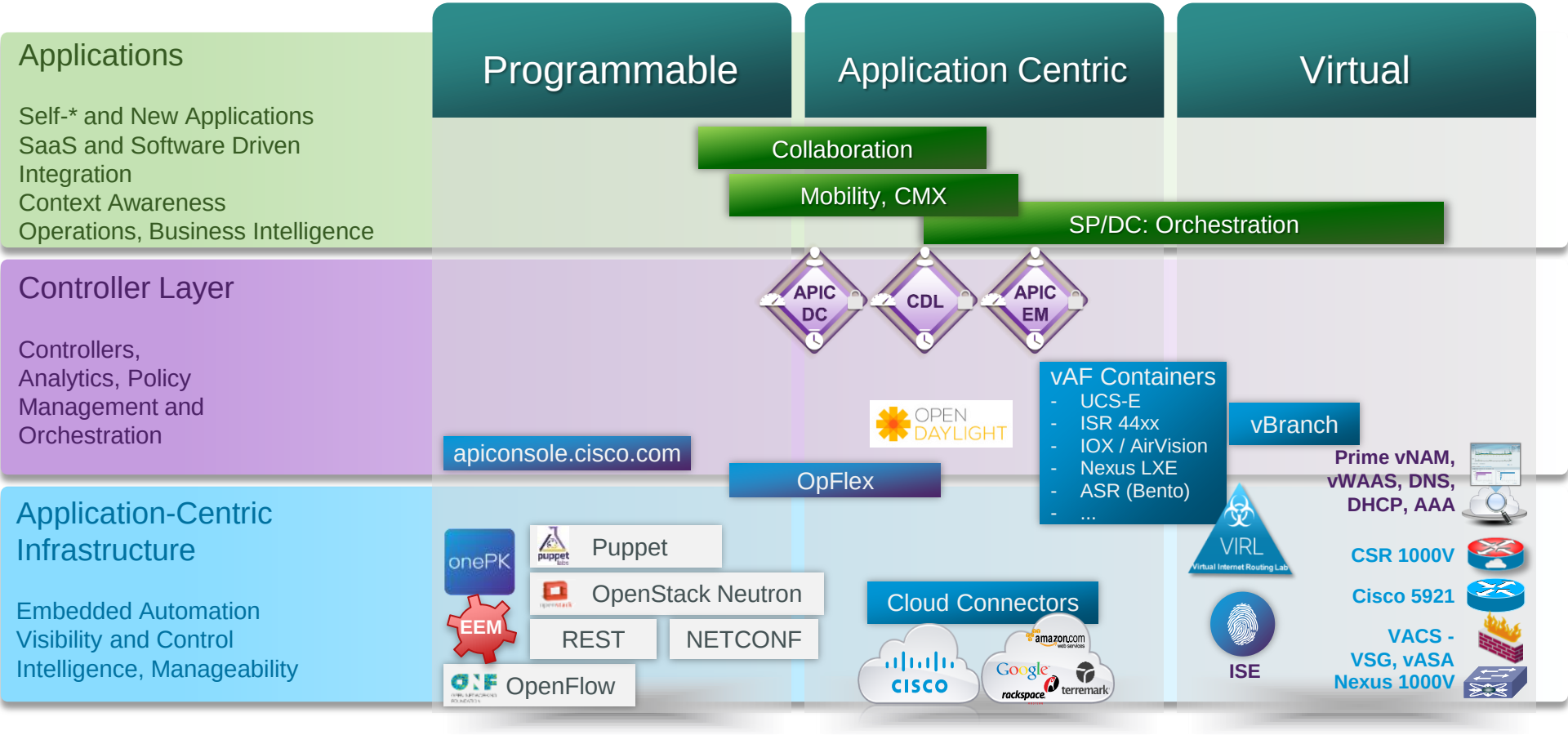
Source: http://spectrometer.opendaylight.org/?metric=loc&project_type=opendaylight

Cisco Open SDN Controller

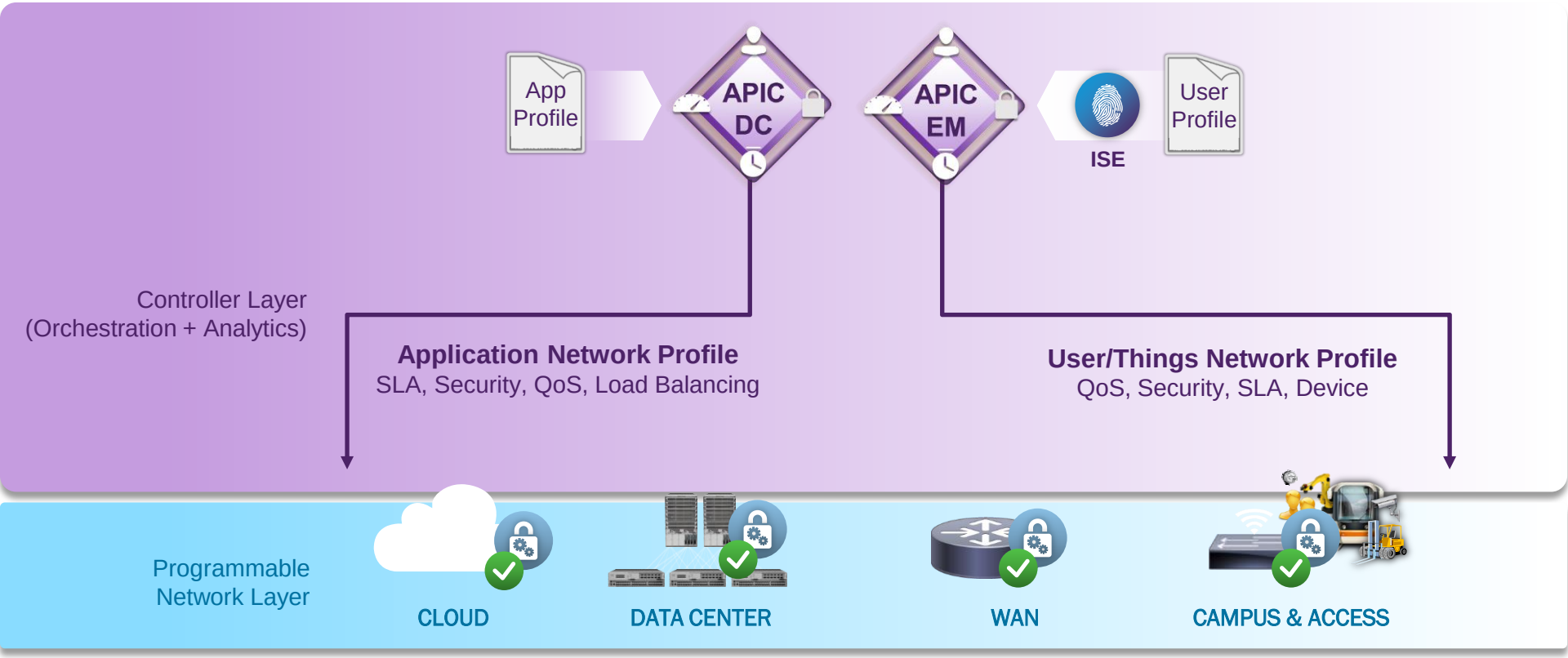


Závěrečná slova

Cisco Enterprise ACI – 3x3 Portfolio (Subset)

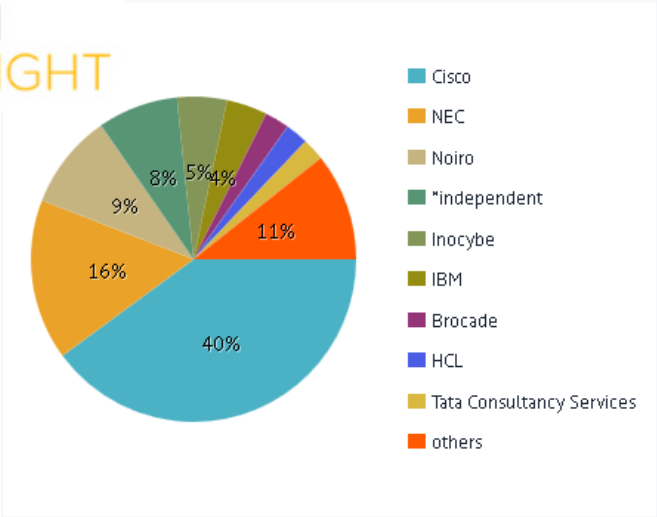


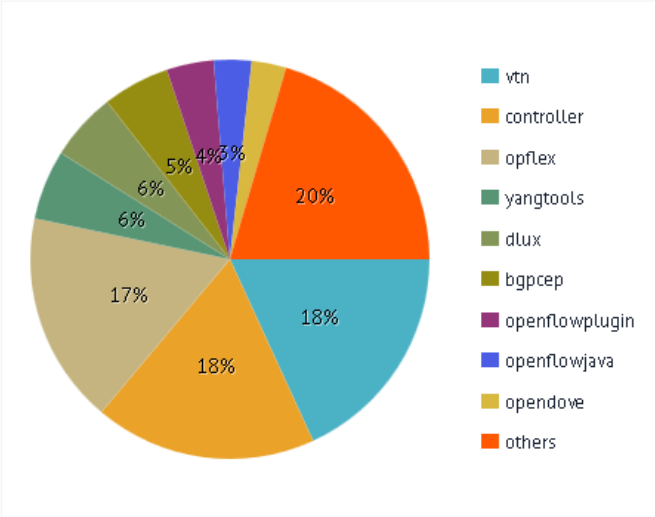
Common Policy End To End



Openness - OpenDaylight Contributions

OpenDaylight's Spectrometer (based on OpenStack Stackalytics)





Source: http://spectrometer.opendaylight.org/?metric=loc&project_type=opendaylight

APIC-EM, OpenSDN in DevNet

DevNet Portal

Developer APIs, SDKs

Community Forum

Integrated with Cisco Communities

DevNet Sandbox

Developer Lab in the Cloud & SW download.

DevNet Zone!

Cisco's Developer Conference

https://developer.cisco.com/site/apic-em/
https://developer.cisco.com/site/openSDN

Open SDN Controller Demos in dCloud

Cisco Open SDN Controller Sandbox v1
Get early access to the new Cisco Open SDN Controller in this sandbox environment.
Start/Schedule More Information *Added : 11/02/2015*

OpenDaylight 2.0 Sample Apps with 8-Nodes v2
This OpenDaylight 2.0 demo showcases the adoption of BGP-LS, ACLs, and PathMan applications for software-defined networking (SDN) that utilize the OpenDaylight Open Source Platform.
Start/Schedule More Information *Added : 30/09/2014*

Cisco OpenDaylight v1.1
The OpenDaylight v1.1 Demo showcases the adoption of BGP-LS and ACLs, which are applications for software-defined networking (SDN) that utilize the OpenDaylight Open Source Platform.
Start/Schedule More Information *Added : 16/06/2014*

Cisco OpenDaylight 1.0 Sandbox v1
Control your own OpenDaylight environment and build your own LSPs
Start/Schedule More Information *Added : 9/07/2014*

Cisco WAN Automation Engine 6.0 with 8-Nodes v1.2
Show how WAE, a network modeling technology, allows for real-time analysis of traffic needs and placement in complex WAN topologies.
Start/Schedule More Information *Added : 8/04/2015*

Cisco Autonomic Networking Sandbox v1
Control your own Autonomic Networking environment with this Cisco Autonomic Networking Sandbox
Start/Schedule More Information *Added : 24/11/2014*

OpenDaylight Helium Sandbox v1.1
Control your own OpenDaylight Helium environment using the Cisco OpenDaylight (ODL) Helium Sandbox
Start/Schedule More Information *Added : 30/03/2015*

- Cloud-based Demos (and Learning)
- Scheduled or on-demand
- Customize and Save your own
- Login to: http://dcloud.cisco.com

CISCO

TOMORROW starts here.