TOMORROW starts here.
Cisco Enterprise SDN: APIC-EM

René Andersen SE Cisco DK
Transforming How Your Company Functions

Bring your own device (BYOD)  The cloud  X-as-a-Service (XaaS)

Salesforce.com
How Are You Handling These Changes?

Today’s IT Model
Challenges of operating networks at scale and enabling innovation

Box-by-Box Manual Configuration

Security  QoS  Path Optimization

IT time spent: 80-90% in network operations; 10-20% enabling innovation

100s  1000s  10,000s  IoE Scale

Complex and Tedious  Difficult to Provision Apps  Difficult to Troubleshoot  Slow Deployment of Services

Presentation_ID
Cisco and/or its affiliates. All rights reserved.
Cisco Public
Software Architecture Principles of the Application Centric Infrastructure

- Configuration-driven
- Infrastructure-centric
- Element management

- Policy-based
- Application-centric
- Network-wide management

Built on Existing Platforms
Software Defined Networking

**High Level Overview**

**Current Network Architecture**

**Network Architecture with SDN**
SDN - A New Way of Looking at Networking

- Applications layered on top
-Operating System controlling entire network
-Hardware controlled through API

Controller

OpenFlow or “South Bound” API

“North Bound” API

App App App App

Cisco and/or its affiliates. All rights reserved.
Agents and Controllers are a component of Open Network Environments and a key component of the evolving "Software Defined Network" concept.

The Concept of Agents and Controllers exists in the Industry for quite some time.

Observation: Current Agent-Controller pairs always serve a specific task (or set of tasks) in a specific domain.
NETWORK EVOLUTION

MORE USERS, DEVICES, AND APPLICATIONS → ENABLING THE INTERNET OF EVERYTHING
SDN Enterprise Architecture

- Layered Architecture: Orchestration can occur at multiple layers

- **Controller Layer**
  - Network-Aware Applications (aware of network services)
  - Infrastructure Layer: Compute, Storage, and Network Elements (physical & virtual)
  - Endpoint Layer (PCs, handhelds, TPs, DC workloads)

- **NB abstraction, API’s, & common object model**

- **Communities**
  - NE
  - NE/C/S
  - Endpoints
  - Data Center
  - Controller
Controller Managed: Separating “What” from “How”

Over time customers only interact through “what” (e.g., eliminating need for user configuration)
Solution-Driven Approach to Design Architecture

Customer-identified use cases drive architecture design

Solutions define architectural requirements

Solution-driven approach provide requirements across the layers
Extending API Controller to WAN and Access

Cisco Application Policy Infrastructure Controller (APIC)

ONE DevKit (Northbound API’s)

ONE PK (Southbound API’s)

DC

WAN

ACCESS

Physical and Virtual
Common Policy Engine
Network Wide Security and Services
Investment Protection
Flexible Licensing
### Cisco ONE Enterprise Networks Architecture

**Network Application Layer**
- Cisco Prime
- Cisco ISE
- Cloud Services
- Security Services
- Mobility Services
- Application Services

**Control Layer**
- Cisco APIC Enterprise Module (Network Services APIs)
- Discovery
- Topology
- QoS
- Location

**Network Element Layer**
- Device API – OnePK™, OpenFlow, CLI
- Cisco Network Operating Systems (Enterprise, Data Center, Service Provider)
  - ASIC Data Plane
  - Software Data Plane
The Cisco Application Policy Infrastructure Controller (APIC) Enterprise Module

Promoting Fast IT for Business Agility and Innovation

Automate Network Configuration and Provisioning for Fast IT

Offered as software or appliance

Open Daylight, REST CLI, OpenFlow, OnePK™

Greenfield and brownfield Catalyst®, Cisco® ISR, ASR

Network Agility for Your Business Needs
Simplifying networks for an application economy
APIC EM Benefits

- Network Information Database
- Network Topology Visualization
- Zero-touch deployment
- Identity Manager
- Policy Manager
- Support for business innovation, open interface
APIC EM Topology Discovery and Management
(Network Elements and Hosts)

Device Configurations Are Retrieved and Stored in a Network Information Base (NIB)

File or Manual Inventory Input Formats

CLI Interface Utilizes Multiple Communications Methods (SSH, TELNET, SNMP,...)
Abstracted policies

### Current Policies

<table>
<thead>
<tr>
<th>Name</th>
<th>Scope</th>
<th>Users: Users</th>
<th>Users: Application</th>
<th>Resources: Users</th>
<th>Resources: Application</th>
<th>Actions</th>
<th>Priority Level</th>
<th>Destination</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>deny 60123</td>
<td>all</td>
<td>60123,60123,TCP</td>
<td>60123,60123,TCP</td>
<td>DENY</td>
<td>N/A</td>
<td>Active</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>good https for blue</td>
<td>all</td>
<td>bilang</td>
<td>443,443,TCP</td>
<td>PERMIT</td>
<td>50</td>
<td>N/A</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>copy intern ftp traffic to</td>
<td>all</td>
<td>interns</td>
<td>21,21,TCP</td>
<td>COPY,PERMIT</td>
<td>50</td>
<td>192.168.1.10</td>
<td>Inactive</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Displaying Three of Three Policies
CISCO Prime and APIC-EM

**Management & Orchestration Layer**
- Cisco IAC UCSD
- PRIME INFRASTRUCTURE & NAM
- APIC-EM App (I WAN)
- Catalog / Provisioning
- Fault / Events
- User / Data Management
- Performance Monitoring
- Reporting / Analytics

**Control Layer**
- Cisco APIC Common ACI Architecture
- APIC for datacenter
- APIC Enterprise Module
- CLI, OpenFlow, OnePK API

**Device Layer**
- Cisco Devices
- Enterprise Networks, Data Center

**Operational Automation**
- Policy and Service Definition
- Automated Assurance Provisioning
- Visualization, Trending and Analytics

**Network Intelligence**
- Device Layer Abstraction
- Network Control
- Policy Enforcement & Network Change
Prime Infrastructure and APIC-EM

PRIME INFRA
- System of Record
- Device Access

APIC - EM
- System of Change
- Device Access

Devices managed directly by PI

Devices controlled via APIC-EM
Prime Infrastructure and APIC-EM

PRIME INFRA
- System of Record
- Device Access
- Devices managed directly by PI

APIC - EM
- System of Change
- Device Access
- Devices controlled via APIC-EM
APIC EM PLATFORM

FCS 1.0

<table>
<thead>
<tr>
<th>HW</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>6500(Sup2T)</td>
<td>15.1(2)SY2, 15.0(1)SY6</td>
</tr>
<tr>
<td>6500(Sup720-3C/B)</td>
<td>15.1(2)SY2</td>
</tr>
<tr>
<td>6880-X</td>
<td>15.1(2)SY2</td>
</tr>
<tr>
<td>WLC 5500</td>
<td>7.6(110.0), 7.4(121.0)</td>
</tr>
<tr>
<td>WLC Flex 7500</td>
<td>7.6(110.0), 7.4(121.0)</td>
</tr>
<tr>
<td>WLC WSIM2</td>
<td>7.6(110.0)</td>
</tr>
<tr>
<td>4500E(Sup 8E)</td>
<td>3.3(0)XO</td>
</tr>
<tr>
<td>4500E(Sup7E)</td>
<td>3.5(2)E, 3.2(8)SG</td>
</tr>
<tr>
<td>3560CG</td>
<td>15.0(2)SE5, 12.2(55)EX3</td>
</tr>
<tr>
<td>ISR-4451</td>
<td>3.12.0S</td>
</tr>
<tr>
<td>3850-Stack</td>
<td>3.3.2SE, 3.2.3SE</td>
</tr>
<tr>
<td>3750x-Stack</td>
<td>15.2(1)E1, 12.2(55)SE8</td>
</tr>
<tr>
<td>2960s-Stack</td>
<td>15.2(1)E1, 12.2(58)SE2</td>
</tr>
</tbody>
</table>

Post FCS

<table>
<thead>
<tr>
<th>HW</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASR9K</td>
<td>TBD</td>
</tr>
<tr>
<td>3650</td>
<td>TBD</td>
</tr>
<tr>
<td>3650-Stack</td>
<td>TBD</td>
</tr>
<tr>
<td>2960-X</td>
<td>TBD</td>
</tr>
<tr>
<td>2960-Plus</td>
<td>TBD</td>
</tr>
<tr>
<td>2960C</td>
<td>TBD</td>
</tr>
<tr>
<td>6500-VSS</td>
<td>TBD</td>
</tr>
<tr>
<td>6807-XL(Sup2T)</td>
<td>TBD</td>
</tr>
<tr>
<td>6800Xa(PEX)</td>
<td>TBD</td>
</tr>
<tr>
<td>4300X</td>
<td>TBD</td>
</tr>
<tr>
<td>3560V2</td>
<td>TBD</td>
</tr>
<tr>
<td>4348E</td>
<td>TBD</td>
</tr>
<tr>
<td>ISR-800</td>
<td>TBD</td>
</tr>
<tr>
<td>7600S(SUP720, RSP720)</td>
<td>TBD</td>
</tr>
<tr>
<td>ASA-5500x(SSP10/20/40/80)</td>
<td>TBD</td>
</tr>
<tr>
<td>ASA-558x(Blades)(SSP10/20/40/80)</td>
<td>TBD</td>
</tr>
<tr>
<td>WLC 8500</td>
<td>TBD</td>
</tr>
<tr>
<td>WLC 2500</td>
<td>TBD</td>
</tr>
<tr>
<td>Virtual Wireless Controller</td>
<td>TBD</td>
</tr>
<tr>
<td>3850-WLC</td>
<td>TBD</td>
</tr>
<tr>
<td>WLC 5760</td>
<td>TBD</td>
</tr>
<tr>
<td>Nexus 7k</td>
<td>TBD</td>
</tr>
<tr>
<td>Nexus 3k</td>
<td>TBD</td>
</tr>
<tr>
<td>CSR 1000v</td>
<td>TBD</td>
</tr>
<tr>
<td>VIRL</td>
<td>TBD</td>
</tr>
<tr>
<td>&lt;&gt;</td>
<td>&lt;&gt;</td>
</tr>
</tbody>
</table>
SDN APIC-EM use cases
Sample Use Cases
No Brownfield Left Behind

- Access control list management
  For security

- QoS management
  for better user experience

- IWAN provisioning
  for WAN cost savings

- Topology 2.0 with customization
### SDN Innovation:
Network Information Base Provides One Source of Truth

- Extends Conventional SDN Topology Discovery - Full Network Element Information Retrieved and Stored

- User Defined Group Tagging Allows Applications to Segment Analysis and Control (not shown here)

- User ID and Location Also Retrieved and Stored (not shown here)
Topology 2.0

• **Auto-discovers** and maps devices to a physical topology with **detailed** device-level data, helping to ensure always up-to-date network **topology**
• Complete and accurate picture of devices, systems, and their interconnects for regulatory compliance, audits, etc.
• Auto-visualization of Layer 2 and 3 topologies on top of physical provides a granular view for design planning, simplified troubleshooting, etc.
• Advanced **HTML5 Javascript-based visualizer** that utilizes REST APIs to deliver a highly **interactive** and customized application experience
Can You Handle the Truth About ACLs?

Finding the right place for edits is like finding a needle in a haystack.

Zero automation tools
100s of devices in your network
1000s of lines of ACL for each device
Customers are hesitant to change ACLs for fear of breaking them.
ACL Use Cases Summary

- **Shadow Identification**
  - Identify duplicates

- **Conflict Identification**
  - Identify inconsistency

- **Compliance Assurance**
  - Flag against policy

- **Flow-based**
  - Identify duplicates

- **Trace and Compare**
  - Identify ACL misconfigurations in application path

- **Follow-Me ACL**
  - Automating ACLs for user mobility

Compliance  |  Troubleshooting  |  Mobility
Simplifying Access Control List Management
Flow-Based ACL Trace and Troubleshooting
Simplifying Access Control List Management
Follow-me ACL - Automating ACLs for User Mobility

Cisco® Identity Services Engine (ISE)
Cisco® APIC Enterprise Module
ACL

Future Release
Application: ACL Management

- Enables “System Level” ACL Inspection and Interrogation by Chosen Flows
- Exposes Shadows and Conflicts
- Supports Element by Element Comparisons with Natural Language Search
QoS: What Are You Afraid Of?
Incredibly Difficult to Deploy for Every Application

- Complex and Tedious to Implement
  - Box-by-box configuration, too many controls
- Device-Specific Implementation
  - Router and switch capabilities limit QoS
- Extremely Difficult to Troubleshoot
  - Box-by-box checking

Customers avoid QoS and simply over-provision or live with it.
Application: QoS Classification Management

- Enables system level QoS classification, marking and queuing policies
- Uses Cisco valid design (CVD) templates to ensure faster, more reliable, and fully predictable deployment
- Supports custom classification templates to meet enterprise specific needs
Business Agility Example:
QoS Video Classification Enables Enterprise Wide Jabber

- Single change across all network elements enables high quality user experience
- Optimizes Video Q combining high end fixed video stations and soft client video into same class
Code to Create Policy FOR LYNC – APIC EM

```
serving at port 8000
WARNING:root:Get XML body:
WARNING:root:Found ConnectionInfo b66438a0a7624e9eb84dbf0d55c1830a
WARNING:root:Found Start tag
WARNING:root:Received call type:applicationsharing, src:port is 10.10.10.180:29074 -> dst:port is 10.10.10.205:23200
Create policy "Lync:applicationsharing:10.10.180", src_port:29074, priority:18
Policy created, policyid is:69022b20-009d-4af4-8b19-1ebfdaa4473d Callid is:b66438a0a7624e9eb84dbf0d55c1830a
WARNING:root:Found Start tag
WARNING:root:Received call type:applicationsharing, src:port is 10.10.10.205:23200 -> dst:port is 10.10.10.180:29074
Create policy "Lync:applicationsharing:10.10.205", src_port:23200, priority:18
Policy created, policyid is:aaea2792-2b2f-4666-b9b0-8ba7649f6497 Callid is:b66438a0a7624e9eb84dbf0d55c1830a
WARNING:root:Done StartOrUpdate
127.0.0.1 -- [07/Apr/2014 13:31:59] "POST / HTTP/1.1" 200 -
```
Automated IWAN Management (Path Optimization)
Performance Routing (PfR) Configuration and Compliance Assurance
DEMO APIC-EM QoS and ACL
SDN Lesson today

- Why SDN?
- What is SDN?
- How is Cisco implementing SDN?
- What is Cisco strategy on SDN?
- What can SDN do for my company?
- How do I start?
TOMORROW
Starts with Cisco SDN

Develop Apps:
https://developer.cisco.com/site/devnet/
home/index.gsp

Get APIC EM:
Contact local Cisco sales rep.