TOMORROW
starts here.

Cisco Connect
Praha, Česká republika
24.–25. 3. 2015
Správa sítí LAN – jednoduše a přehledně

TECH-LAN-3

Zdeněk Roubal
Jaroslav Martan
Petr Mojžíšek (ANECT)
Industry Transformation Anchored in SDN
Abstractions and Intent Policies

Rapid IT Expansion

OPEX Reduction & LOB Agility Drivers

SDN Stack Model

- **Simplicity via Controllers**
  (one manageable source of truth to base network changes)

- **Automation via Apps**
  (rapid translation of intended business outcomes to required network behavior)

- **Flexibility via Loosely Coupled Abstractions**
  (harmonizes disparate network pieces to create a network as a “system”)

SDN Model Adds the Essential Ingredients that Makes Solutions Networking Possible for Complex Networks
Cisco Fast IT: Leading This Enterprise Transformation

SECURITY COLLABORATION SERVICES ORCHESTRATION WAN

PUBLISHED REST APIs

Application Centric Infrastructure (ACI) Compatible
Software Driven Enterprise Network Control and Management Platform

UNIVERSAL NETWORK ELEMENT PLUG AND PLAY LAYER

CATALYST NEXUS ISR ASR ASA WIRELESS

A New Software Driven Platform for Solutions Development
Network Control and Management Are Foundational…

…Components of the Platform for Building Applications
Common Policy Model from Branch to DC

Consistent Policy Across Cloud, DC, WAN and Access

Application Network Profile
SLA, Security, QoS, Load Balancing

User/Things Network Profile
QoS, Security, SLA, Device

Cloud
Data Center
WAN
Access

APIC
APIC
Changing Nature of IT Ops with SDN led Management

**Traditional Management**

Customer developed provisioning tools, manual CLI changes, and run book automation for IT Operations support

**Management (NMS)**

**SDN Led Management**

Customer input on business / service intent

Automation (Workflow / Orchestration)

Management (Provisioning and Assurance)

Controller (APIC-EM)
Changing Nature of IT Ops with SDN led Management

**Traditional Management**

- Feature Configuration

**SDN Led Management**

- Policy Automation

Customer developed provisioning tools, manual CLI changes, and run book automation for IT Operations support.

Customer input on business / service intent

Traditional Management

- Configuration
- Policy
- Automation

SDN Led Management

- Feature
- Policy
- Automation
Cisco Management Tool Portfolio for the Campus / Branch in 2014

Common Automation Layer
Common Monitoring / Assurance
Feature Configurable Provisioning
Common Controller Layer For Campus/Branch

System of Automation
Manual or Custom Scripted by Customers / Partners

System of Record
Prime Infrastructure

System of Change
Prime Infrastructure
No Controller Existed in 2014
Cisco APIC-EM: Campus / Branch Controller

Network Abstraction and Automation

Software or Appliance Based
NB RESTful APIs
Existing and New Device Support
Agile Integration Model

Masking Network Complexity, Exposing Network Intelligence
## Key Milestones to SDN Led Management Evolution in 2015

<table>
<thead>
<tr>
<th>Q1 2015</th>
<th>Mid-2015</th>
<th>Q4 2015</th>
</tr>
</thead>
</table>
| **APIC-EM CA**  
Path Visualization application for network path tracing | **APIC-EM GA**  
Scalable controller foundation supporting multiple use case / apps | **APIC-EM Updates**  
Expanded application support across multiple enterprise use cases |
| **Prime Infra 2.2 FCS (Dec 2014)**  
Cross domain monitoring across WAN, Access, DC | **Prime Infra Niihau**  
Integration with APIC-EM for core network service automation | **Prime Infra Lanai**  
Integration with APIC-EM and Automation as System of Record |
| **APIC-EM Apps**  
I WAN app EFT with policy based provisioning of Secure WAN | **APIC EM Apps**  
I WAN App GA with dynamic QoS changes; BSA app EFT | **APIC-EM Apps**  
Multiple apps across Wireless, Access, Collab, Security and Automation |
Cisco Controller and Management System Portfolio for the Campus/Branch in 12-24 Months

Common Automation Layer

Common Monitoring / Assurance

Feature Configurable Provisioning

Policy Prescriptive Provisioning

Common Controller Layer for Campus/Branch

System of Automation

System of Record

System of Change

Branch Service Automation

Prime Infrastructure

Prime Infrastructure

Multiple APIC-EM Apps

APIC-EM

NE

NE

NE

NE

NE
Two Deployment Modes for SDN led Provisioning with Distinct Network Scope

**Device Scope A**

**FEATURE CONFIGURABLE NMS with APIC-EM**
- Custom apps utilizing feature programmability via Prime NB APIs for configuration and data
- Prime Infra NMS integrated with APIC-EM providing full GUI based configuration and FCAPS management orchestrated by the System of Automation

**Customer, Partner or 3rd party developed Automation**

Prime Infrastructure

**Device Scope B**

**POLICY PRESCRIPTIVE APPS on APIC-EM**
- Cisco developed modular, policy automated management apps with common UI/UX framework with and embedded service automation
- Custom apps utilizing policy programmability via APIC-EM NB REST APIs

**Collab**, **Segmentation**, **Threat Defense**, **IWAN**, **Access**, **Wireless**

**Customer, Partner or 3rd party developed Apps**
APIC-EM
Policy Based Automation
Cisco Prime Infrastructure
The Path to One Management

Customer Consolidation
Wired / Wireless Bundle
  - Introduce PI as bundle
  - Unified purchase & entitlement

One Management
One wired/wireless/routing Product
  - New & NCS customers use PI
  - LMS Features migrate over time

Unified IT Operations
Integrated Management Stack
  - Network, DC, Security, Collab
  - EMS, assurance, orchestration...
  - Large Enterprise & SP Scale

Prime Infrastructure 1.x
  - PI Lifecycle
  - LMS 4.2
  - PI Assurance

Prime Infrastructure 2.0
  - PI Lifecycle
  - LMS 4.2.x
  - PI Assurance

Prime Infrastructure 2.1
  - PI Lifecycle
  - LMS 4.2.x
  - PI Assurance

Prime Infrastructure 2.2
  - PI Lifecycle
  - PI Assurance
  - PI DC/Cloud Assurance

Wired & Wireless
  - Wired/wireless endpoint visibility
  - ISE policy system integration

AVC for Branch & Edge
  - ISR / ASR / branch
  - Assurance & app visibility with Prime NAM integration
  - Prime Site & Device 360°

Unified Access
  - Converged Access Architecture
  - Unified wired / wireless / WAN
  - ISE policy system integration
  - Wired and wireless user application experience

Data Center
  - E2E assurance from user to DC
  - DCNM integration
Centralized lifecycle management - discovery, inventory, configuration, SWIM, and proactive/reactive monitoring

Advanced troubleshooting of wired and wireless infrastructure issues

Rapid device support through Device Packs for new Cisco® devices, routers, switches, controllers, access points, Nexus® technology, and more

Customizable configuration templates based on Cisco validated designs and guided workflows

Cisco Unified Access™ management and client tracking

- Seamless integration with Cisco Identity Services Engine (ISE) for simplified troubleshooting
- Seamless integration with Cisco Mobility Services Engine (MSE) for location-based services, rogue detection, etc.
End-to-end visibility for service-aware networking by applications, services, and end users

Out-of-the-box support for Cisco® advanced technologies, including AVC 2.0, NetFlow, Flexible NetFlow, NBAR2, Performance Agent, Medianet, and more

Service health dashboard allows quick health check on your business-critical applications

Simplified troubleshooting of applications and client access issues

Multi-NAM management
- Traffic analysis
- Application response time metrics
- Packet capture and decode
Extends One Management – Visibility of infrastructure and assurance from Branches all the way through campus and data center

Cisco UCS B and C series – Discovery, inventory of compute infrastructure and mapping that back to the network elements of the data center

Fault and Root cause analysis – Identify and isolate the source of the problem. Help pin point the issues to the right network or compute elements. Understand the impact of network problems onto the compute infrastructure. RemEDIATE the issues at its source

Availability and Performance – Monitor the availability status of the UCS physical servers. Provides visibility to the UCS ports health status and performance

Server 360 Degree view – Concise and easy to consume server details accessible from any where in the product. Allows for quick troubleshooting
Additional Platform Features

- ISE and MSE integration
- Virtual Domains
- Users, Roles, AAA, SSO
- Job Roles and Job Approvals
- System Audit (user initiated activities)
- High Availability
- Northbound Integration – REST API
- Technology and Device packs
- Physical / Virtual (Express, Standard, Pro) Appliance
- Custom MIBs and SNMP Polling Templates
- 3rd Party Device Support
Prime Infrastructure 2.2 Highlights

**Platform**
- Topology
- PI Operations Center
- R/W API's
- Technology Packs

**Wireless**
- CUWN - 8.0 and 8.1 Support with APs
- Converged Access – 3.6 and 3.7 with APs
- Maps Performance Improvements
- Meraki AP Support Tech Pack

**Wired**
- IPV6 Device Management
- QoS Monitoring Support
- IWAN Configuration Workflows
- CA Configuration Workflows Tech Pack

**Datacenter**
- UCS Server Assurance
- Nexus 9K Assurance
Prime Infrastructure 2.2 release has been optimized with **Single OVA file for all installation types.** (Express, Standard or Pro editions)

1. **Download**
   
   PI 2.2 virtual appliance ova from CCO onto your local machine

2. **Login** to Vmware vSphere client and deploy OVF template as shown
Simplified OVA Install ..2

3

Accept the install type from the option shown here

4

Resources like CPU and memory are automatically allocated based on the type
Simplified OVA Install ..3

5. Create PI instance and specify the VM location for template deployment

6. Select the configuration type and deploy
Converged Menu
Single Menu for All Operational Tasks

- Similar to Classic View
- Classic view is deprecated
- Maps and Topology at top level
- Device Work Center optimized
- Supports 3 deployment models based on best practice
- CVD based prescriptive templates that can be edited
- Full tested wireless configuration for converged access enabled in less than a minute
- Guided workflow for multi-site deployment
Credential Profiles
Update Device Credentials

An easy way to change credentials on a regular basis for compliance.
Network Discovery
Methods to discover existing Wired/Wireless Network

Discovery Settings:
- Allows multiple Protocols
- Filtering Capabilities

Manually add devices and use the Credentials Profiles
Bulk Device Edit & UDF Management

Bulk edit the device credentials
Hierarchical Location Groups for Inventory
Flexible Group Definitions

Multi Level Hierarchy for Location Groups

Devices can now belong to multiple groups based on Device Priority, Device Role etc.
Location Group Topology – Campus

Alarm Badge indicates highest alarm state of items inside the Container
Location Group Topology
Bldg SJC07

Launch the Device 360

Device Summary
Branch Offices connected to San Jose
Manually Create Elements
Network / Device / Link
N-Hop Topology (in Device 360)
Monitoring Policies
Improved OOTB Monitoring Setup

Automatically monitor the device health and WAN Interfaces with pre-defined thresholds
Out-of-the-box Assurance Templates
CLI Configuration for Data Sources – Simplified
AVC Configuration for Routers
CLI Configuration for AVC - Simplified

Enabling AVC on Multiple Devices

This Corresponds up to 700 Lines of CLI

1-Click Enablement per device
Visibility
Business Critical Applications Performance

Application / Server Delay

Client & Network Delay

Application / Server Performance

Application ART Analysis

Experience

Analysis

Worst N Sites by ART Metrics

Selected Metric : Transaction Time

<table>
<thead>
<tr>
<th>Site</th>
<th>Application</th>
<th>Maximum Transaction Time (ms)</th>
<th>Average Transaction Time (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>India Branch</td>
<td>sap</td>
<td>16055</td>
<td>5665</td>
</tr>
<tr>
<td>Unassigned</td>
<td>sap</td>
<td>1491</td>
<td>564</td>
</tr>
<tr>
<td>San Francisco Branch</td>
<td>sap</td>
<td>2417</td>
<td>528</td>
</tr>
<tr>
<td>Los Angeles Branch</td>
<td>sap</td>
<td>1081</td>
<td>502</td>
</tr>
<tr>
<td>RTP Branch</td>
<td>sap</td>
<td>945</td>
<td>493</td>
</tr>
</tbody>
</table>
Interface Monitoring

Ability to “look” into the QoS Classes
Monitor the Service Health
Identify Sites and Applications that Needs Immediate Attention

Application Performance by site

Automated Baseline and Dynamic Threshold
Inventory Information

View Details for the Network Devices
Configuration Achieve
Wired Devices

Archive and Versioning of Configuration
- Fetch & store all the configurations on network devices
- Store multiple versions of configurations.
- Job based for periodic archival
- Detect changes done outside the PI server and archive the change

Compare Configuration
- View configurations
- Compare configurations between versions of same or different devices
- Reporting configuration mismatches

Rollback Configuration Rollback
- Update the configuration on a device in the network
- Ability to specify which configurations to download.
- Ability to specify options like reboot, write mem etc.
- Job based
Network Overview

- Asset Information for the Converged Network
- Editable Dashlets for Context Aware Information
- Quick Peek into Devices that are Network and SNMP Unreachable
- User Defined Dashboard Customization

Network Device Summary:
- Total Reachable Device Count: 77
- Total Unreachable Device Count: 11
- Operational AP: 20

Device Unavailability Summary:
- Site Name: Unassigned
  - AP: 0
  - Routers: 6
  - Switches: 1
- Site Name: Asia Pacific
  - AP: 0
  - Routers: 0
  - Switches: 0
- Site Name: Europe
  - AP: 0
  - Routers: 0
  - Switches: 0
- Site Name: Management Apps
  - AP: 0
  - Routers: 0
  - Switches: 0
- Site Name: North America
  - AP: 0
  - Routers: 0
  - Switches: 0
- Site Name: San Jose Data Center
  - AP: 0
  - Routers: 0
  - Switches: 0
- Site Name: System Campus
  - AP: 0
  - Routers: 0
  - Switches: 0

Device Reachability Status:
- Device Name: Router.cisco.com
  - Device IP: 10.155.12.153
  - Location: Unreachable
- Device Name: PAR-3750-88R
  - Device IP: 10.12.10.1
  - Location: Unreachable
- Device Name: D10-damo-892W.cisco.com
  - Device IP: 128.107.150.77
  - Location: Unreachable
- Device Name: C406K-Dev-1
  - Device IP: 10.0.255.41
  - Location: Unreachable
- Device Name: COM-PUBL.cisco.com
  - Device IP: 192.168.138.201
  - Location: Reachable
- Device Name: CORF-2
  - Device IP: 10.0.255.32
  - Location: Reachable
- Device Name: BRN-nm5-88F.cisco.com
  - Device IP: 192.168.138.131
  - Location: Reachable
Clients Monitoring & Troubleshooting
Single pane of glass to view wired and wireless clients

All the “Associated” wired and wireless clients
Wired Client Troubleshooting

Client status with recommended troubleshooting steps

1. Verify that the DHCP server is reachable.
2. Verify that the DHCP server is configured to serve the WLAN.
3. If DHCP bridging mode is enabled and the client is configured to get an address from the DHCP server, verify that the local DHCP server is present.
4. Verify that the client has a static IP address configured and is generating IP traffic.
5. Ensure that the DHCP scope is not exhausted.
6. If there are multiple DHCP servers, ensure they are not configured with overlapping scopes.

System Detail

802.1x Status: Authz Success
Client don’t have IP Address assigned
Session State is: Authz Success
Analyzing User Experience
Gather 360 Perspective to Quickly Isolate Performance Issues

Global Search
Or, Search by Username/IP Address
Jack Fields has 2 Wireless and 1 Wired Client

User 360 view: Client details, Applications and Alarms
Drill-down for details analysis
# Alarm Management

## Incidents Dashboard

### SNMP Reachability check and the ability to launch Device 360

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device IP</th>
<th>Location</th>
<th>SNMP Reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router.cisco.com</td>
<td>128.107.150.66</td>
<td></td>
<td>Unreachable</td>
</tr>
<tr>
<td>LA-2504-WLC</td>
<td>192.168.3.13</td>
<td>LA Branch</td>
<td>Unreachable</td>
</tr>
<tr>
<td>eset-lmr-42-1</td>
<td>192.168.138.138</td>
<td>Unknown</td>
<td>Unreachable</td>
</tr>
<tr>
<td>Router.cisco.com</td>
<td>10.155.12.153</td>
<td></td>
<td>Unreachable</td>
</tr>
<tr>
<td>PAIR-3750-5KB</td>
<td>10.12.10.1</td>
<td>Paris 3750 switch</td>
<td>Unreachable</td>
</tr>
<tr>
<td>DG-damo-892W.cisco.com</td>
<td>128.107.150.77</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C4ink-Dist-1</td>
<td>10.0.255.41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCM-PUBL1.cisco.com</td>
<td>192.168.138.201</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CORE-2</td>
<td>10.0.255.32</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTP-NAM-SRE.cisco.com</td>
<td>192.168.136.131</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Network Reachability Check

**Top N Sites with Most Alarms**

- North America: 20
- San Francisco Branch: 30
- Paris Branch: 10
- Europe: 5
- RTP Branch: 0

### Device Unavailability Summary

<table>
<thead>
<tr>
<th>Site Name</th>
<th>AP</th>
<th>Routers</th>
<th>Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassigned</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Europe</td>
<td>0</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Management Ops</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>North America</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>San Jose Data Center</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>India Campus</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
### Alarm Browser

#### Alarm Summary
- Category: Critical - 1,800, Major - 2, Minor - 1,777

#### Clients
- Context-Aware Notifications: 7
- Controller: 70
- Coverage Hole: 0
- Mesh Links: 0
- Mobility Service: 0
- Performance: 0
- Rogue AP: 0
- Routes: 0
- RRM: 0
- SE Detected Interferers: 0
- Security: 32
- Switches and Hubs: 25
- System: 0
- Third Party AP: 0
- Third Party Controller: 0
- Wireless Controller: 0

#### Investigate the High Severity Events

**Alarm Summary for Category Critical**

<table>
<thead>
<tr>
<th>Port</th>
<th>Message</th>
<th>Status</th>
<th>Failure Source</th>
<th>Time Stamp</th>
<th>Owner</th>
<th>Category</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1960/102</td>
<td>Port is down on devr 102...</td>
<td>Not Acknowledged</td>
<td>RPT-1960-102</td>
<td>November 5, 2013 00:53 AM PST</td>
<td>Routers</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>2/2</td>
<td>Port GigabitEthernet/2/2 is down on devr 2</td>
<td>Not Acknowledged</td>
<td>SF-2/2</td>
<td>November 5, 2013 00:53 AM PST</td>
<td>Routers</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>10/16</td>
<td>Port GigabitEthernet/10/16 is down on devr 10</td>
<td>Not Acknowledged</td>
<td>SF-2/2</td>
<td>October 28, 2013 12:28 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>10/16</td>
<td>Port GigabitEthernet/10/16 is down on devr 10</td>
<td>Not Acknowledged</td>
<td>SF-2/2</td>
<td>October 28, 2013 11:58 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1/14</td>
<td>Port GigabitEthernet/1/14 is down on devr 1/14</td>
<td>Not Acknowledged</td>
<td>SF-2/2</td>
<td>September 10, 2013 04:55 PM PDT</td>
<td>Encashia</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1/10</td>
<td>Port GigabitEthernet/1/10 is down on devr 1/10</td>
<td>Not Acknowledged</td>
<td>SF-2/2</td>
<td>September 10, 2013 04:55 PM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1/10</td>
<td>Port Serial/1/10: Booze Channel is down.</td>
<td>Not Acknowledged</td>
<td>RPT-1960-102</td>
<td>September 10, 2013 04:55 PM PDT</td>
<td>Routers</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1/10</td>
<td>Port Security-Interferer With Invalid Ch...</td>
<td>Not Acknowledged</td>
<td>AP Low-Ap-3</td>
<td>November 28, 2013 3:56 AM PDT</td>
<td>Routers</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1/10</td>
<td>Port Security-Interferer With Invalid Ch...</td>
<td>Not Acknowledged</td>
<td>AP Low-Ap-3</td>
<td>September 9, 2013 7:00 PM PDT</td>
<td>Security</td>
<td>Interferer Security Traps</td>
<td></td>
</tr>
<tr>
<td>1/10</td>
<td>Port FastEthernet/1/10 is down on devr 1/10</td>
<td>Not Acknowledged</td>
<td>AP Low-Ap-3</td>
<td>August 29, 2013 11:40 AM PDT</td>
<td>Security</td>
<td>Interferer Security Traps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The Controller Hardware Mod has...</td>
<td>Not Acknowledged</td>
<td>AMS-3750-18/2</td>
<td>August 29, 2013 4:39 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Failed to authorize AP 1005568-4r2/2</td>
<td>Not Acknowledged</td>
<td>AP000-5568-4r2</td>
<td>October 8, 2013 11:44 AM PDT</td>
<td>AP</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>2/2</td>
<td>Port Gigabitethernet/2/2 is down on devr 2</td>
<td>Not Acknowledged</td>
<td>LON-4556-2/2</td>
<td>November 5, 2013 10:37 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td>1960/152</td>
<td>Port is down on devr 1960/152...</td>
<td>Not Acknowledged</td>
<td>Port 1960/152</td>
<td>November 28, 2013 4:50 AM PDT</td>
<td>Controller</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Gigabitethernet/110/14 is down on devr 110</td>
<td>Not Acknowledged</td>
<td>BGN-3750-110/cisco.com/110/GigabitEth...</td>
<td>November 28, 2013 12:47 AM PDT</td>
<td>Switches and Hubs</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Element limit for Context Aware Service is...</td>
<td>Not Acknowledged</td>
<td>Location Server service 2</td>
<td>November 28, 2013 4:52 AM PDT</td>
<td>Mobility Service</td>
<td>Link down</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Element limit for Context Aware Service is...</td>
<td>Not Acknowledged</td>
<td>Location Server service 2</td>
<td>November 28, 2013 4:52 AM PDT</td>
<td>Mobility Service</td>
<td>Link down</td>
<td></td>
</tr>
</tbody>
</table>
Cisco Prime Infrastructure – Operations Center
Centralized Visualization Across Multiple PI Instances

Prime Infrastructure Console

Single Pane Monitoring
- Unified Assets View
- Unified Alarms View
- Unified Clients views
- Consolidated Reports
- Consolidated Dashlets
- Consolidated Search

Fan Out Queries
Device Affinity

Prime Infrastructure Instances

Network Data

Static Data

Aggregation

Networking and/or its affiliates. All rights reserved.
Network Management
System of Record vs. System of Change

**Prime Infrastructure**
- Policy definition
- Historical reporting on events & performance
- Configuration archive
- Troubleshooting workflows
- Capacity Trending
- Predictive Analytics

**APIC - EM**
- Policy enforcement
- Discovery (for change)
- Topology (for change)
- PnP
- Network state monitoring
- Device abstraction
- Network Control
Links and Resources
Links and Resource

- **Weekly Prime Demo Series**

- **Prime Infrastructure Evaluation**
  - [http://www.cisco.com/go/nmsevals](http://www.cisco.com/go/nmsevals)

- **APIC-EM – Developer Community**