

What You Make Possible



Managing an Enterprise WLAN with Cisco Prime Infrastructure

BRKEWN - 2011



Intentionally left blank.

Agenda

1

Cisco Prime Infrastructure – Evolution, Feature Parity, Future

2

Cisco Prime Infrastructure Migration and Licensing

3

Unified Access – Lifecycle Management

4

Product Characteristics

5

Integration

6

Additional Resources

7

Best Practices

8

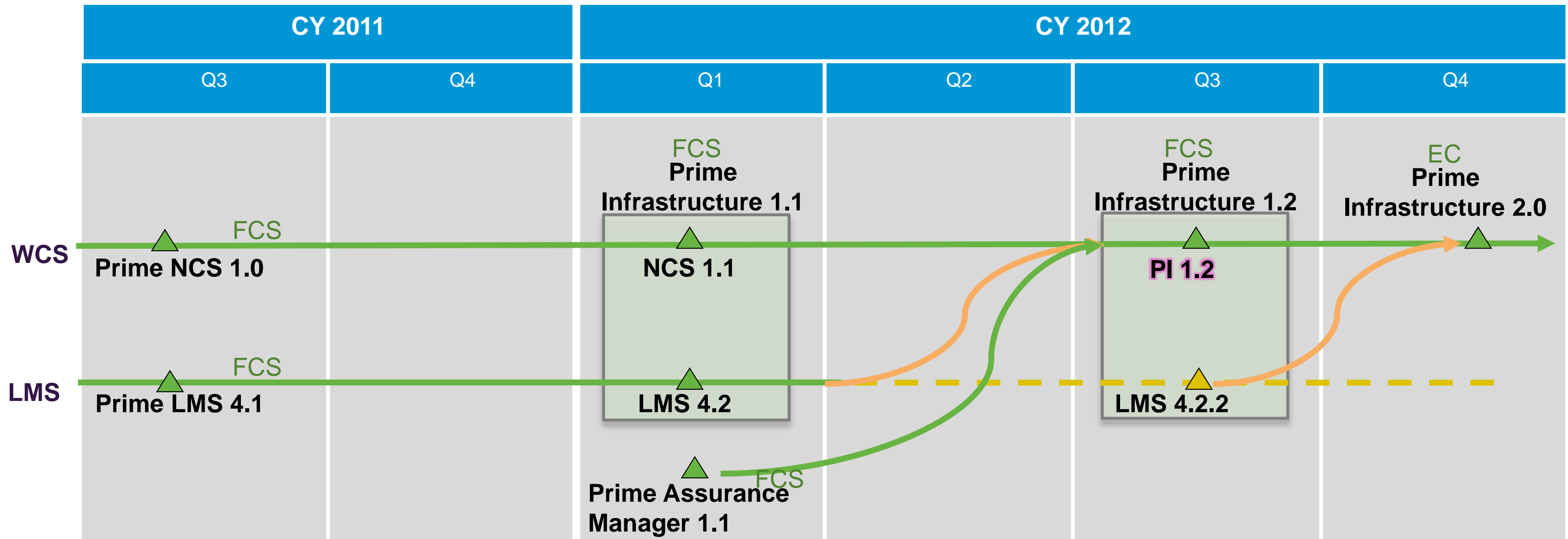
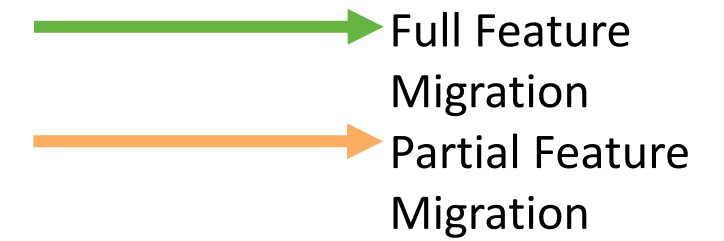
Q&A

Prime Infrastructure - Evolution, Feature Parity, Future



The Path to “One Management”

How We Got Here



The Evolution

Initial Alignment

- Aligned UX, deployment, licensing

Customer Consolidation

- Introduced bundle
- Single order, pricing, licensing, services
- **ISR / ASR / branch mgmt**
- **Assurance: App visibility**

Converged Platform

- Converged wired/wireless, routing lifecycle mgmt
- Integrated app assurance
- **Partial LMS migration**

Prime Infrastructure – Migration and Licensing



Cisco Prime for IT Portfolio

INTELLIGENT NETWORK ARCHITECTURE

Cisco Prime

Prime Infrastructure

Lifecycle

End-to-end lifecycle management
- Design, Deploy, Operate, Admin

Assurance

Application/ end-user visibility
- Monitor, Troubleshoot, Remediate

Compliance

Regulatory and best practices
- Monitor, Report, Remediate

Data Centre

Data Centre Network Mgr

Management of virtual resources
• Network, Compute, Storage

Network Analysis Module

Rich instrumentation for application
troubleshooting

NetFlow Generation Appliance

Visibility of Data Centre applications
and services

Prime Collaboration

Lifecycle

End-to-end lifecycle management
- Design, Deploy, Operate, Admin

Assurance

Voice/video/TelePresence visibility
- Monitor, Troubleshoot, Remediate

SP Integration

Smart Services

OS / ASICs

IPv6

SDN/API

Systems Test

Cisco Prime Infrastructure

Delivering on the Promise of One Management

Automated Best Practices

- Wired/wireless, Branch/WAN
- Integrated lifecycle
- Cisco best practices built-in
- PnP automated deployment
- Day 1 Device Support

**Operational
Productivity**

Lifecycle

**Borderless
Network**

Assurance

User, Site & App Experience

- App performance visibility
- User & site-level visibility
- Proactive monitoring
- Real-time troubleshooting
- Prime 360 Views

**User
Productivity**

Compliance

- Regulatory and best practice policies
- Automated audit and reporting
- Centralised remediation

**Regulatory and
Operational Compliance**

Cisco Prime Infrastructure 1.2

License Types Explained

License Type	Description	Dependencies/Requirements
Base	The Base license enables using a Prime Infrastructure management node (physical or virtual appliance).	One and only one base license is required for each management node.
Lifecycle	Enables the Prime Infrastructure device Lifecycle management feature set. This license type is based on the number of managed devices.	Requires a Base license.
Compliance	Enables access to the regulatory Compliance management policies and reports. This license type is based on the number of managed devices.	Requires a Lifecycle license. The number of devices you can run regulatory compliance reports on is limited based on the number of compliance licenses.
Assurance	Enables the Prime Infrastructure Assurance management feature set. This license type is based on the number of NetFlow enabled interfaces.	Requires a Base license.
PnP Gateway	This license supports the deployment of a separate Gateway for use with the plug-and-play feature where new devices can call in the gateway to receive their configuration and software image.	Requires a Lifecycle license.

Licensing

Simplified Licensing:

■ LIFECYCLE

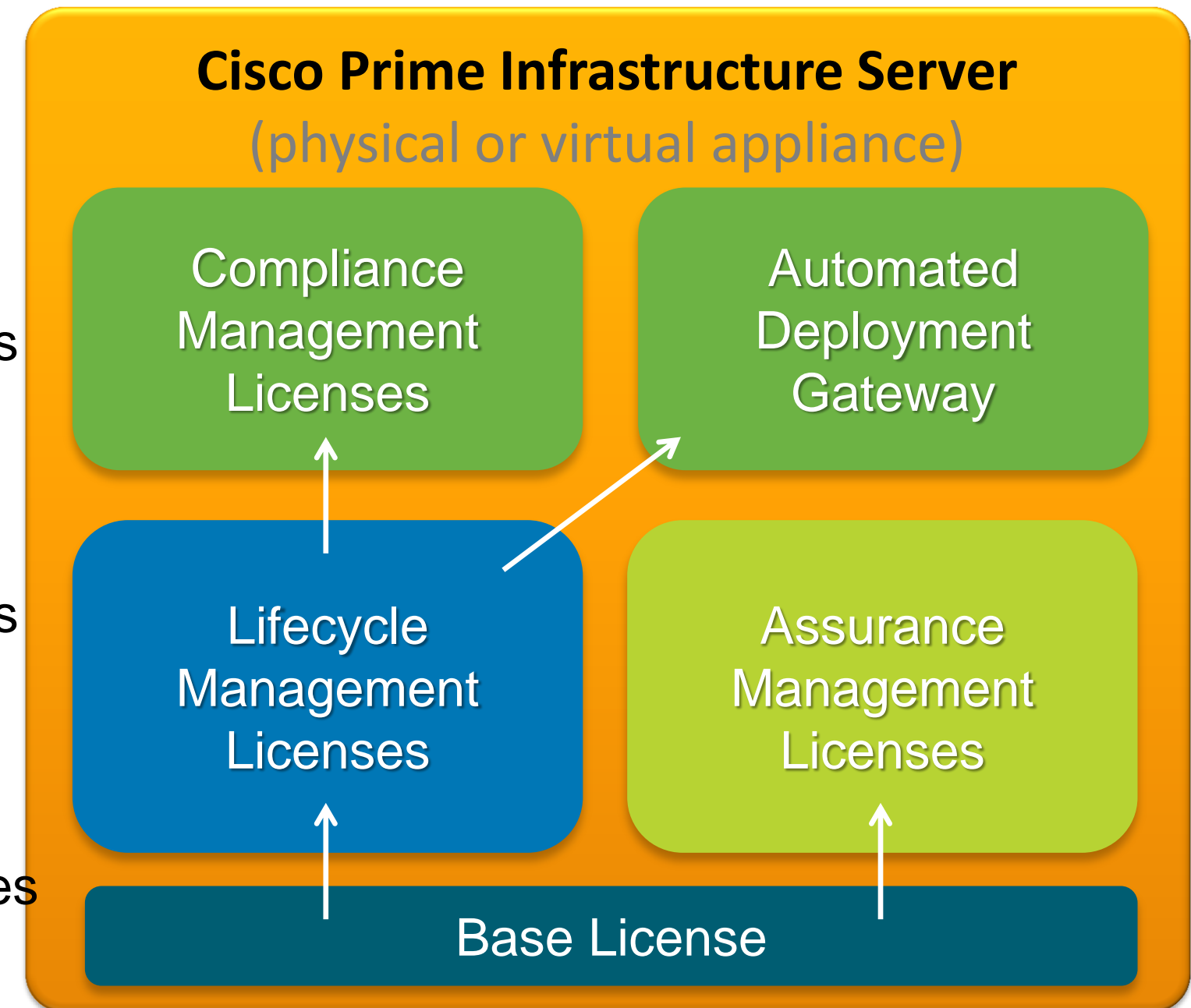
- Based on # of devices
- Additive Licensing from 25 to 10,000 devices

■ COMPLIANCE

- Based on # of LIFECYCLE devices
- Additive Licensing from 25 to 10,000 devices

■ ASSURANCE

- Based on # of interfaces
- Additive Licensing from 15 to 5,000 interfaces

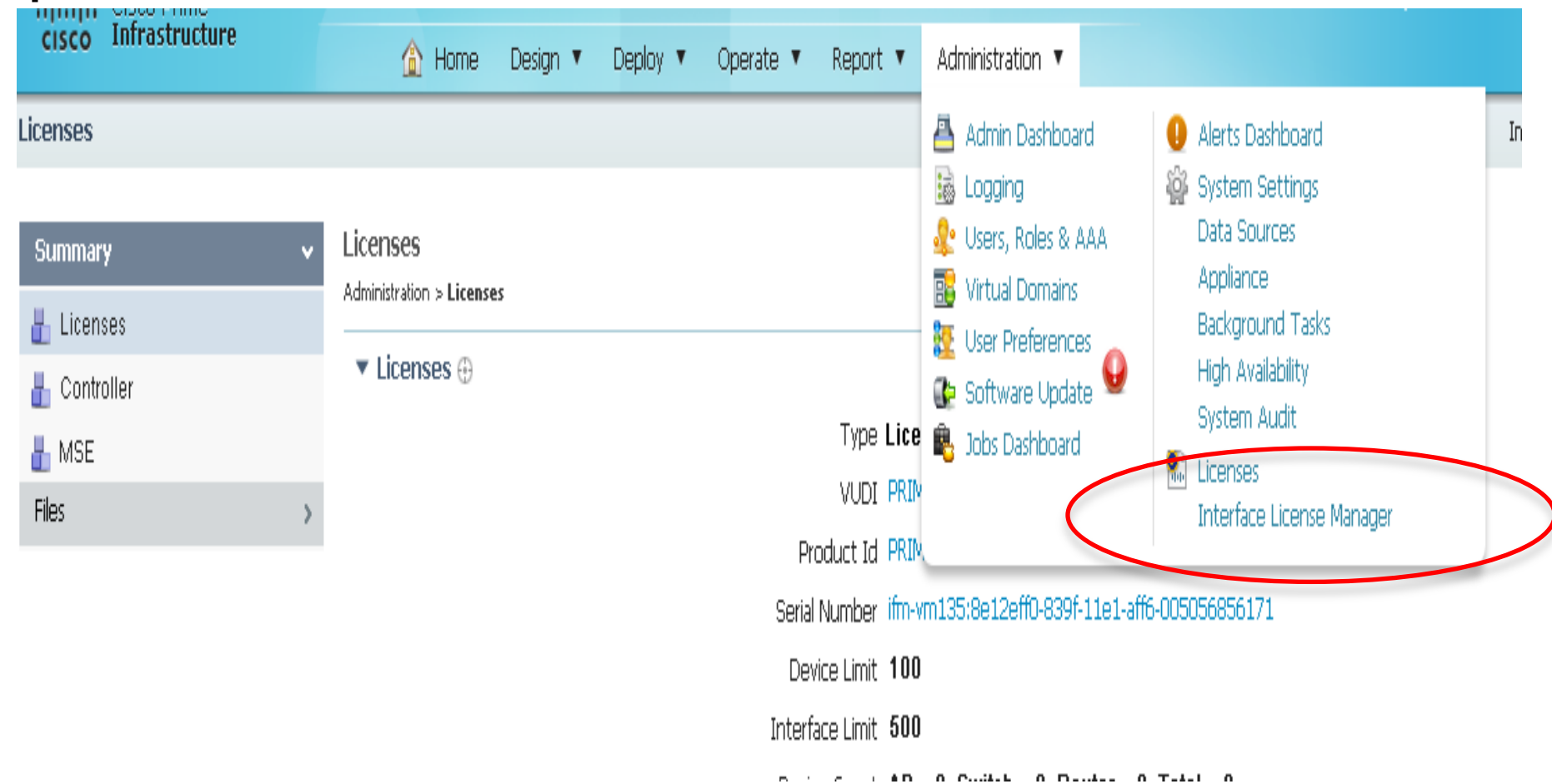


About License Node Locking

- Prime Infrastructure uses node locked licenses
- Two different types of node locking:
 - Physical Appliance: Unique Device Identifier (UDI)
 - Virtual Appliance: Virtual Unique Device Identifier (VUDI)
- UDI: Is made up of a PID and unique serial number
 - The PID for the physical appliance is “PI-APL”
 - Serial number is assigned by manufacturing and unique among all Cisco products
- VUDI: Is made up of a PID, Hostname, and UUID
 - The PID for the physical appliance is “PI-VAPL”
 - The hostname is assigned by the customer
 - The UUID is a generated 128 bit number (36 chars string representation) based on the current time and MAC address or random number
 - The combination of the hostname and UUID is the serial number
- LMS does not use node locked licenses

How to View the License Summary

- Navigate using Administration > Licenses then click on Licenses under Summary
 - Note: Administration > Interface License Manager will be seen also if valid Assurance licenses are present



License Summary

The screenshot shows the Cisco Prime Infrastructure interface for license management. The left sidebar contains a navigation menu with 'Licenses' selected. The main content area displays the details for a specific license instance.

Callouts and their corresponding fields:

- Type (License or Unlicensed):** Points to the 'Type' field, which is 'Licensed'.
- Count of devices added to the system:** Points to the 'Device Count' field, which shows 'AP = 0, Switch = 0, Router = 0, Total = 0'.
- Unique Serial Number of this instance:** Points to the 'Serial Number' field, which is 'ifm-vm135:8e12eff0-839f-11e1-aff6-005056856171'.
- Licensed Lifecycle device count limit:** Points to the 'Device Limit' field, which is '100'.
- Licensed Assurance interface count limit:** Points to the 'Interface Limit' field, which is '500'.
- Provides information about features, permanent vs. evaluation (number of remaining days), and limits:** Points to the 'Features' table.

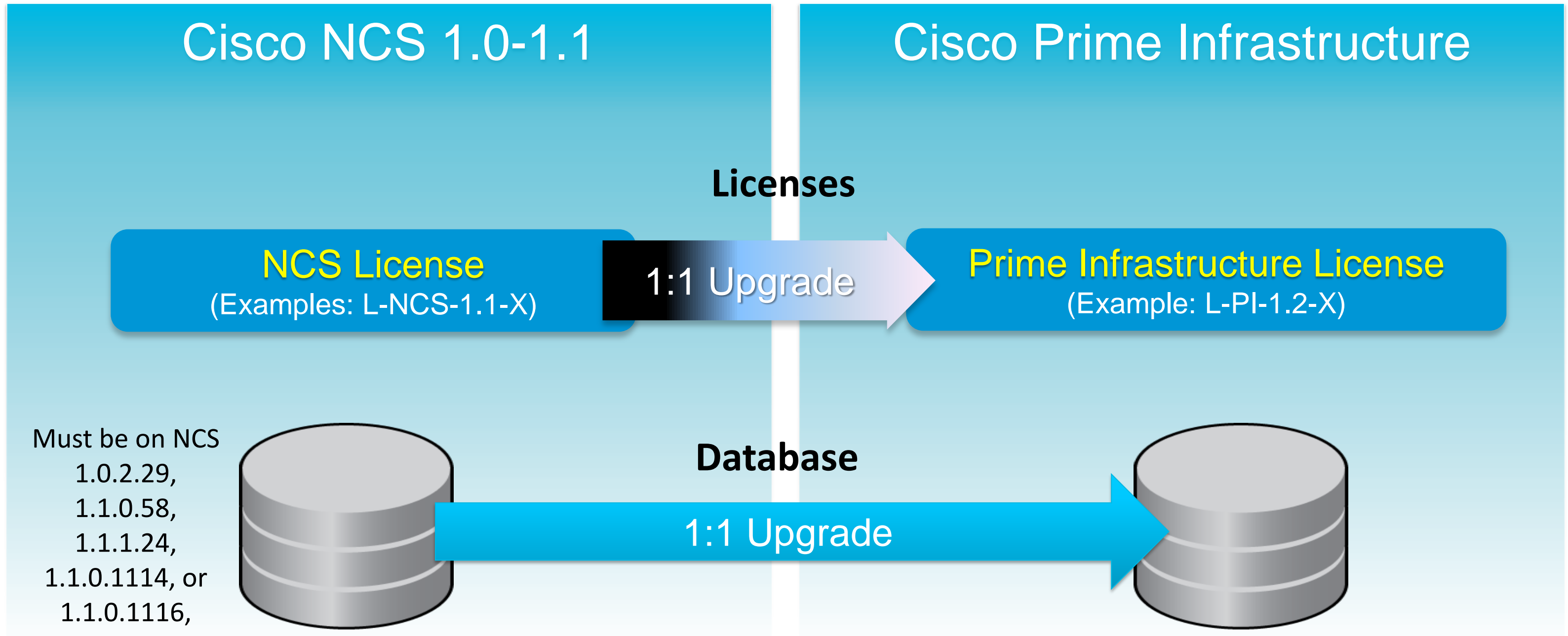
License Details:

- Type: **Licensed**
- VUDI: PRIME-NCS-VAPL:ifm-vm135:8e12eff0-839f-11e1-aff6-005056856171
- Product Id: PRIME-NCS-VAPL
- Serial Number: ifm-vm135:8e12eff0-839f-11e1-aff6-005056856171
- Device Limit: **100**
- Interface Limit: **500**
- Device Count: **AP = 0, Switch = 0, Router = 0, Total = 0**
- Interface Count: **0**
- % Used: **0%**
- % Used (PAM): **0%**
- NAM|WAAS Count: **0**
(Not counted towards License Limit except Special License)

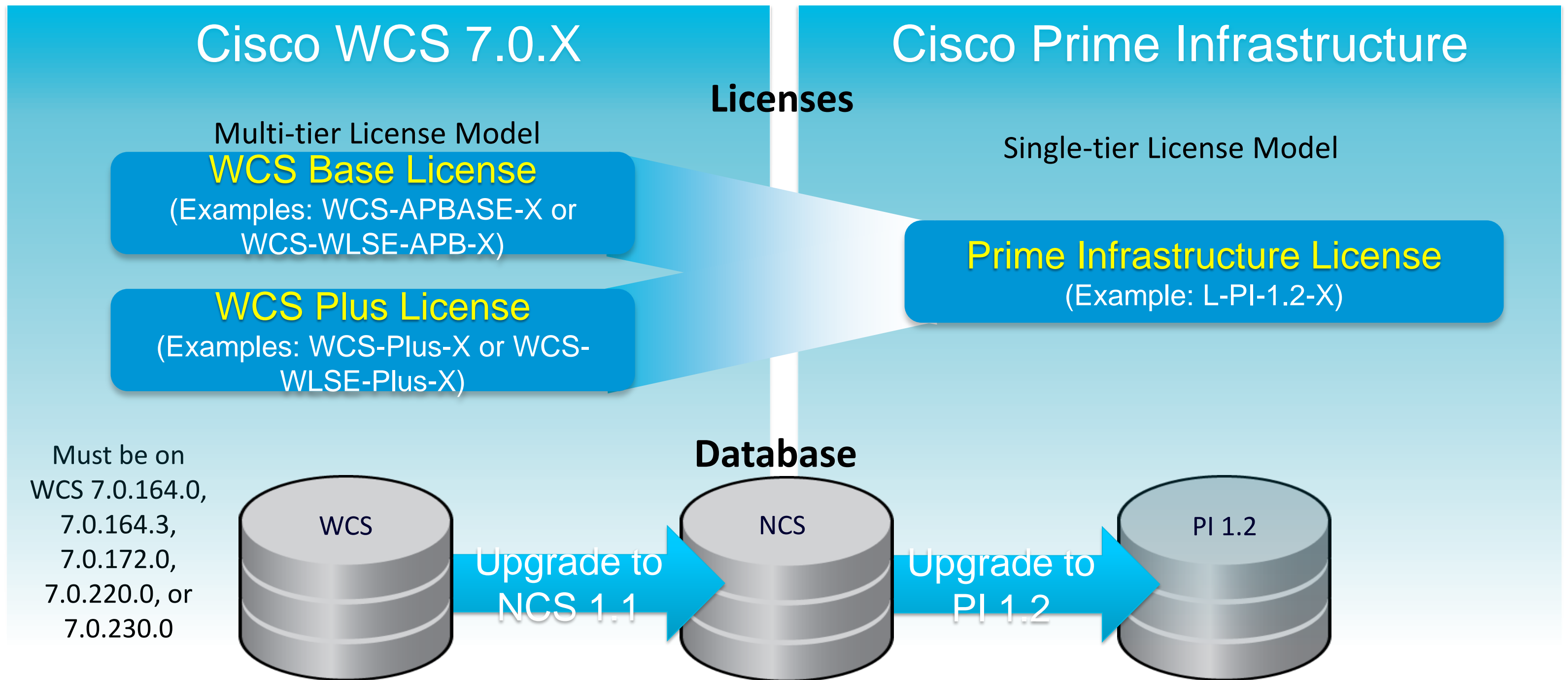
Features Table:

Feature	Type	Limit	Additional P...
Lifecycle	Evaluation (53d...	100	
Assura...	Permanent	500	

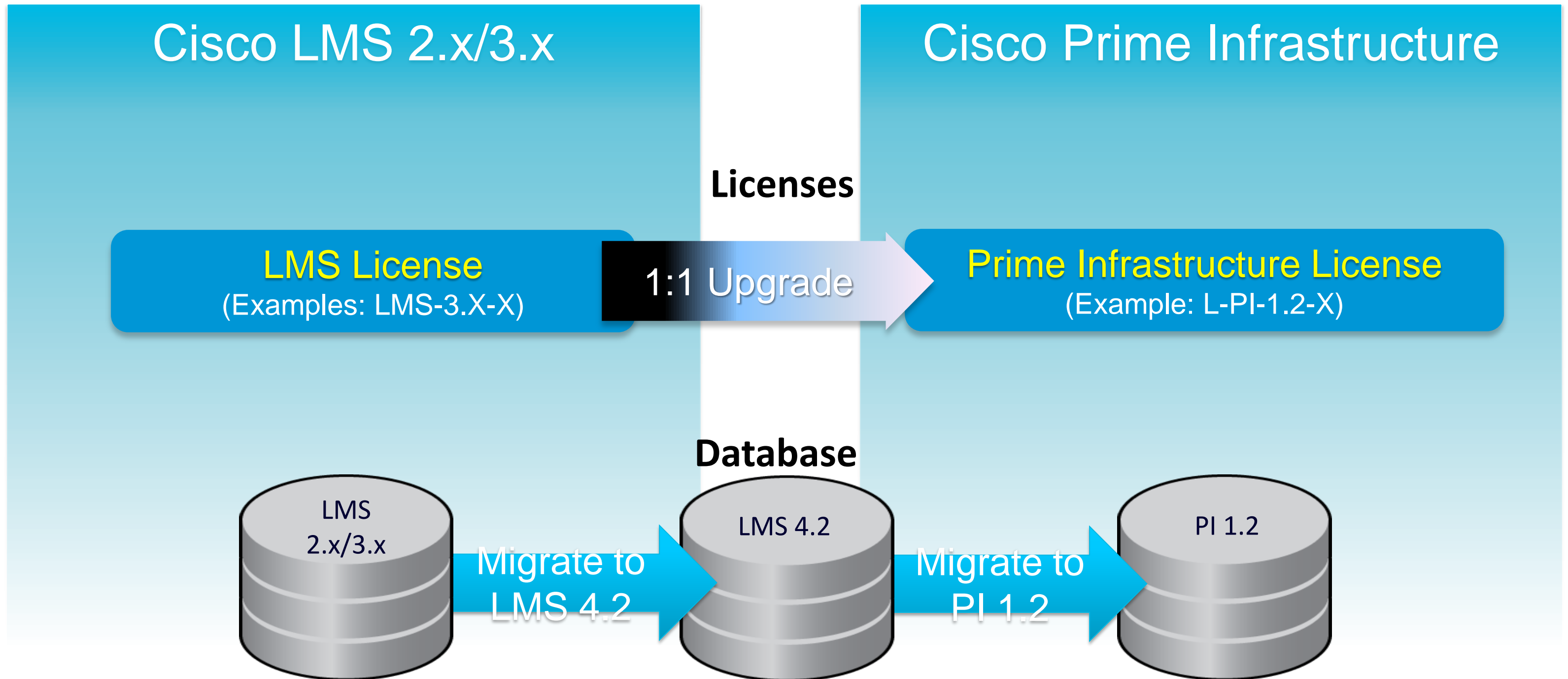
NCS to Prime Infrastructure Migration



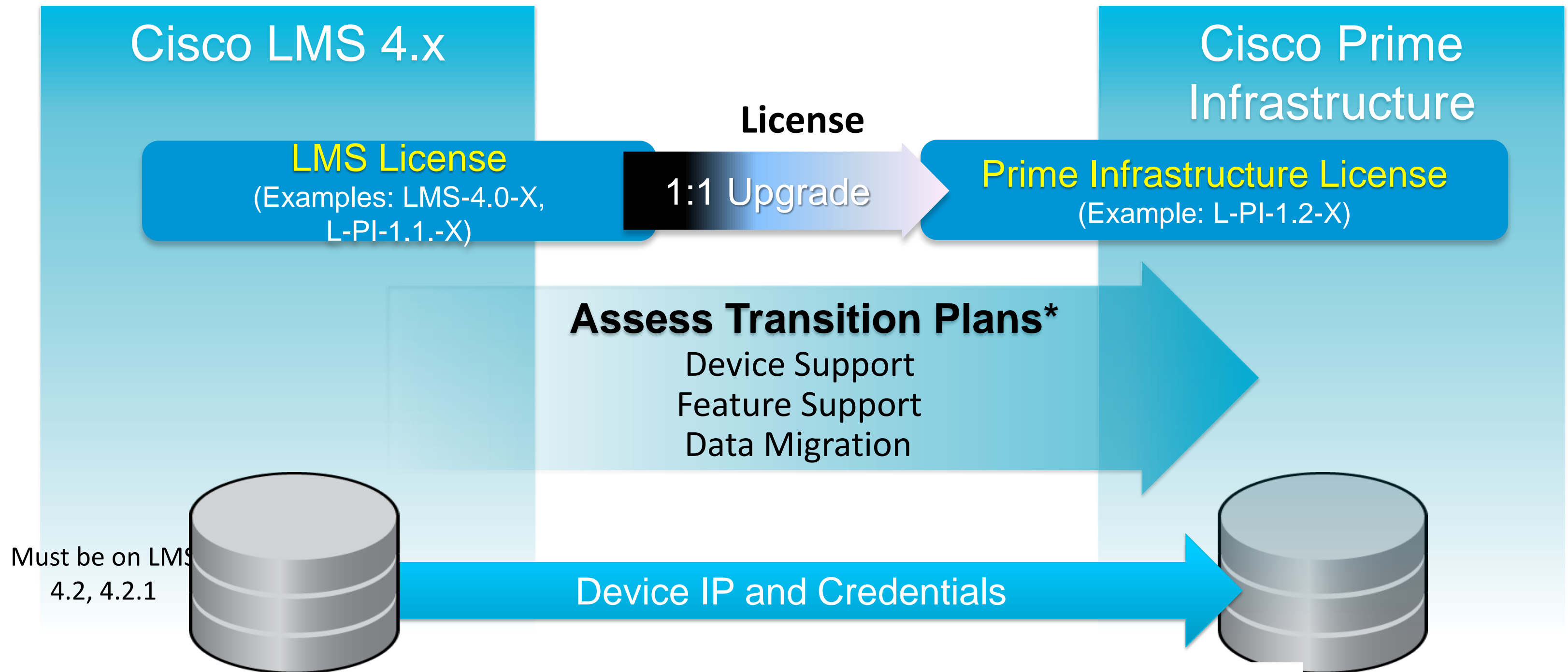
WCS to Prime Infrastructure Migration



LMS 2/3.x to Prime Infrastructure Migration



LMS 4.x to Prime Infrastructure Transition



*See cisco.com/go/primeinfrastructure for LMS transition guidance

LMS Migration to Prime Infrastructure

- [External](#) and [Internal](#) reference documents
- Recommend LMS customers deploy Prime Infrastructure in parallel with LMS transition as needed
- LMS will not be bundled with Prime Infrastructure 2.0
- Prime Infrastructure 1.2 will continue to be orderable through 2013

Prime Infrastructure 2.0 vs. LMS 4.2 Gaps

Functional Capability	LMS 4.2	PI 1.2	PI 2.0	Notes
System				
Solaris Server	●	x	x	Move to VM or appliance
Microsoft Windows Server	●	x	x	Move to VM or appliance
HPOV/NetView Integration	●	x	x	
Cisco Call Manager Integration	●	x	x	
API: DB Views	●	x	x	REST APIs in PI 1.2
API: CWCLI	●	x	x	REST APIs in PI 1.2
Monitor				
IP SLA Management	●	-	-	Requires Assurance license
N-hop Viewer	●	x	x	
UTLite	●	-	-	
UT Utility	●	x	x	
Inventory				
Inventory Change Notification	●	-	-	
Work Centers & Technologies				
EnergyWise Management	●	-	-	
Medianet Management	●	-	-	
Smart Install Management	●	x	x	PnP Automated Deployment in PI 1.2
Auto Smartports Mgmt	●	-	-	
Spanning Tree Mgmt	●	-	-	
VSS Management	●	-	-	
VRF/Lite Management	●	-	-	
POE Management	●	-	-	

Legend	
●	Equivalent Support
○	Partial Support
-	Pending Support
x	Not Supported
Red	Unique to Prime Infrastructure

Prime Infrastructure 2.0 LMS Coverage

Functional Capability	LMS 4.2	PI 1.2	PI 2.0	Notes
Work Centres & Technologies				
TrustSec Management	●	-	○	
VLAN Management	●	○	○	
IPv6 Support	●	○	●	
Automated Deploy (PnP)	X	●	●	
Zone-based Firewall Config	X	●	●	
Get/DM VPN Configuration	X	●	●	
ScanSafe Configuration	X	●	●	
Easy VPN Configuration	X	-	●	
Overlord / Container Management	X	-	●	
AVC Management	X	-	●	
Container Management	X	-	●	

Legend

- Equivalent Support
- Partial Support
- Pending Support
- X Not Supported
- Red Unique to Prime Infrastructure

Prime Infrastructure 2.0 LMS Coverage

Functional Capability	LMS 4.2	PI 1.2	PI 2.0	Notes
System				
VM soft appliance Server	●	●	●	
Physical appliance Server	○	●	●	
High Availability	○	●	●	Built-in active HA in PI 1.2
TAC Service Requests	●	●	●	
Support Communities Search	●	●	●	
API: REST	X	●	●	
ISE Integration	X	●	●	
Prime Infrastructure Cluster	X	-	○	
Prime Infrastructure Collector	X	-	○	
Instant Evaluation	X	-	●	
PI Mobile Application	X	●	●	
Prime Infrastructure ToolBar	X	●	●	
Monitor				
Event/Syslog Monitoring	●	●	●	
Device Health Monitoring	●	●	●	
Performance Monitoring	●	●	●	
Topology	●	-	○	
User Tracking	●	●	●	Supports both wired and wireless
RF Management and Tools	X	●	●	
Guided Troubleshooting	X	●	●	
360 Views	X	●	●	

Legend

- Equivalent Support
- Partial Support
- Pending Support
- X Not Supported
- Red Unique to Prime Infrastructure

Prime Infrastructure 2.0 LMS Coverage

Functional Capability	LMS 4.2	PI 1.2	PI 2.0	Notes
Inventory				
Day 1 Device Support	●	○	●	See LMS Device Support Reference
Cisco Unified Wireless support	x	●	●	
3rd Party Support	○	○	●	PI 1.2 support Aruba wireless mgmt
Discovery	●	●	●	
Inventory	●	●	●	
EoL/PSIRT Reporting	●	●	●	
Contract Connections	●	-	●	
Configuration				
Configuration Archive	●	●	●	
Configuration Templates	●	●	●	
Configuration Audit	●	○	○	
Configuration Discrepancy	●	○	○	
Best Practices Deviation	●	○	○	
Baseline Compliance	●	●	●	
Regulatory Compliance	●	-	○	Requires Compliance license
Software Image Management	●	●	●	
Cisco View	●	-	○	View only mode in Prime Infra

Legend

- Equivalent Support
- Partial Support
- Pending Support
- x Not Supported
- Red Unique to Prime Infrastructure

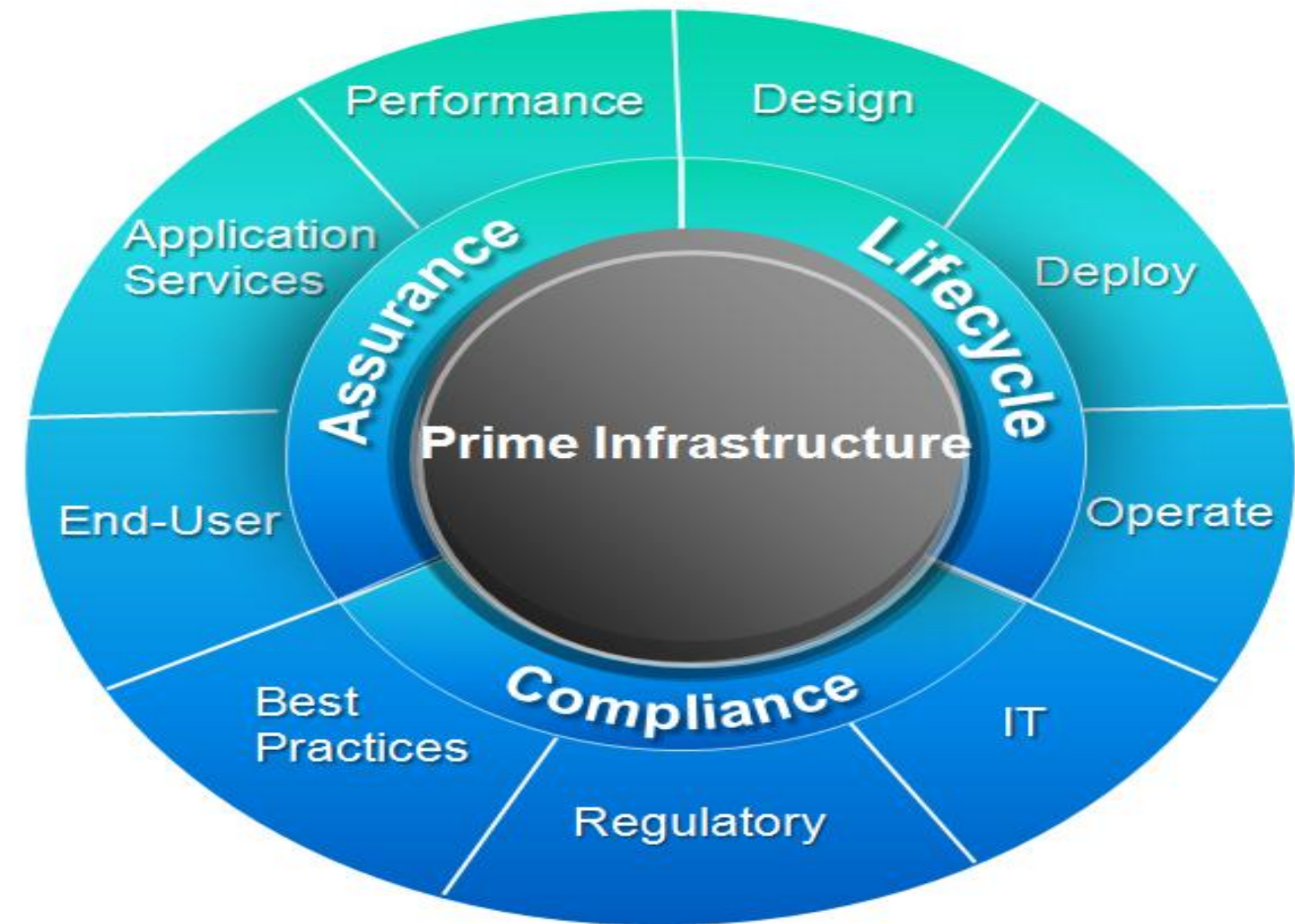


Unified Access – Lifecycle Management



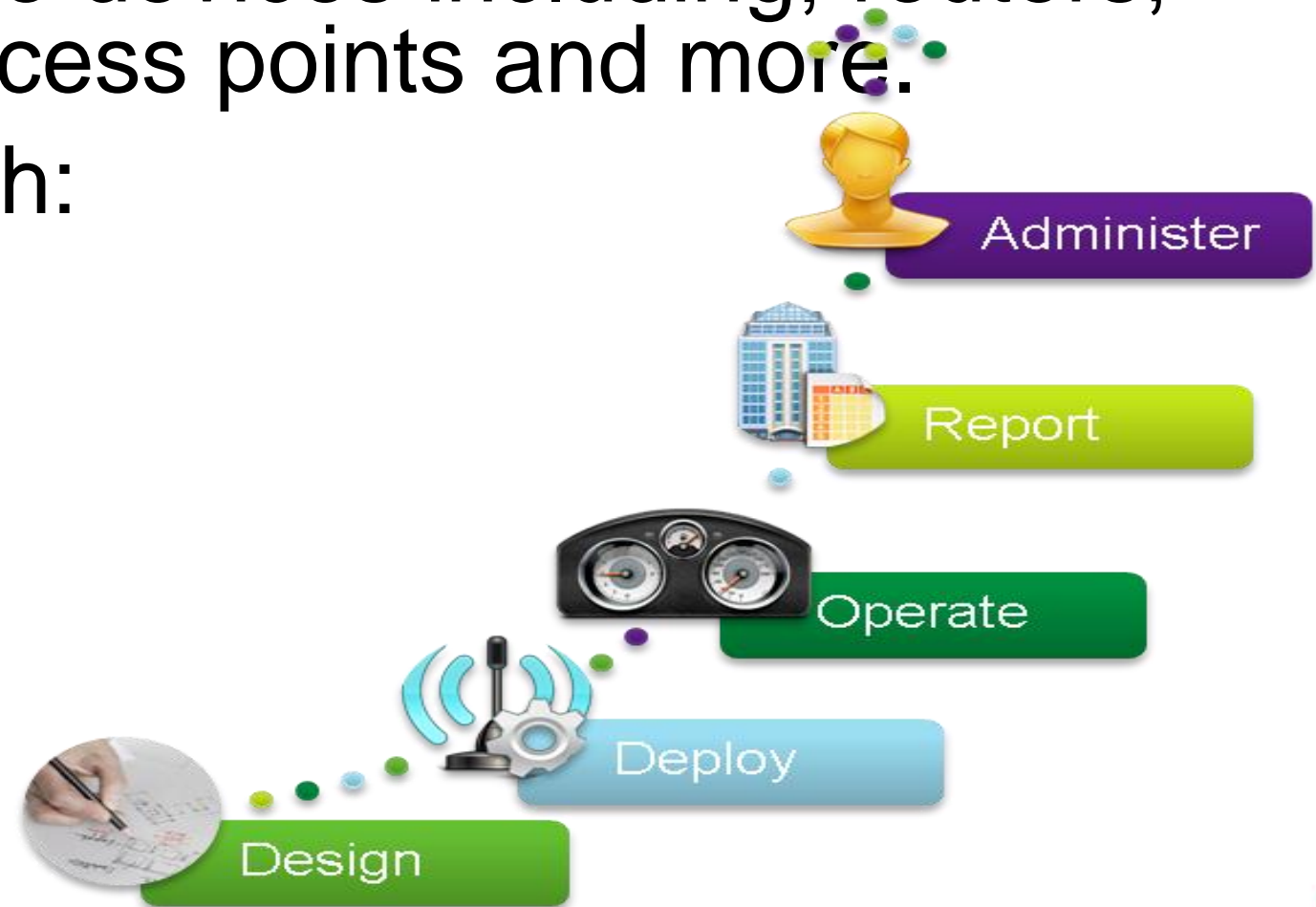
Prime Infrastructure 1.2 – Functional Overview

- ✓ A single integrated solution for comprehensive **lifecycle** management of wired/wireless access, campus, and branch networks
- ✓ Automates **compliance** with regulatory requirements, Cisco and IT best practices
- ✓ Utilises rich performance data for end-to-end network visibility to **assure** application delivery and optimal end-user experience

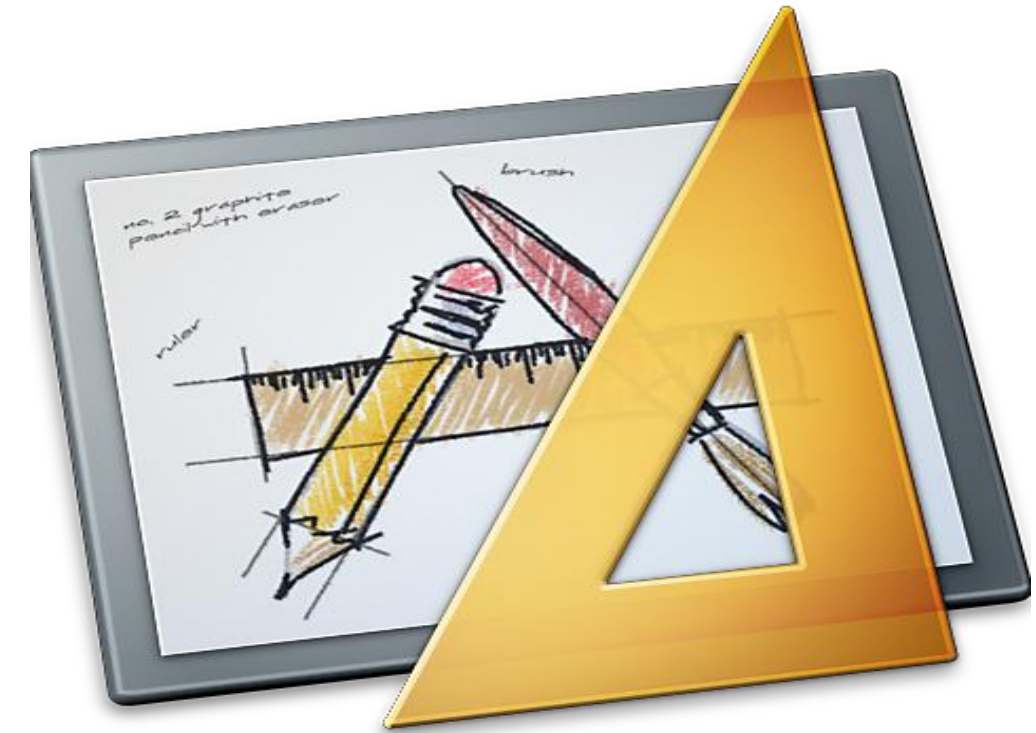


Lifecycle Management for Wired/Wireless

- Lifecycle approach provides an easy and efficient way to manage a complex wired and/or wireless network by simplifying the day-to-day operational tasks associated with managing the network infrastructure for all Cisco devices including; routers, switches, wireless controllers, access points and more.
- Stages in this Life Cycle approach:
 - Design
 - Deploy
 - Operate
 - Report
 - Administration



Design



Various Aspects of Design

- Configuration

- Designing Config Templates
 - CLI Templates
 - Composite Templates
 - Model based Templates
- Wireless Configuration

- Monitoring

- Design > Publish > Deploy workflow for controlled monitoring.
- Thresholds can now be designed proactively.

- Port, Sites and Maps

- Mobility



Mapping of Conventional Design Tasks

Conventional Tasks

- Organise Network into Sites
- Prepare for configuration
- Prepare for monitoring
- Prepare zero touch deployment
- Associate Companion Services for enhanced visibility

In Prime Infrastructure

- Design Sites and Maps
- Design Configuration Templates
- Design Monitoring and threshold Templates
- Design Automated Deployment Profiles
- Integrate Mobility and Identity Services

Design Your Own Configuration Template

- Model-based templates are provided for:
 - security (ACL, DMVPN, ScanSafe , GetVPN ...)
 - NAM
 - Wireless controller
- User can create his own CLI templates which can contains:
 - parameters (prompted during deploy)
 - scripting construction in Apache Velocity Template Language (VTL)
- User can define composite templates (template of templates)
- User can import existing Cisco Prime LMS templates

The screenshot displays the Cisco Prime Infrastructure Configuration Templates interface. The main window shows the configuration for a CLI template named "IP Phone DHCP Pool". The interface is divided into several sections:

- Template Basic:** Includes fields for Name (IP Phone DHCP Pool), Author (prime), Description, and Feature Category (CLI).
- Validation Criteria:** Includes fields for Device Type (Routers) and OS Version.
- Template Detail:** Includes a tab for CLI Content and a Form View. The CLI Content tab is active, showing the following configuration:

```
ip dhcp excluded-address 10.$Branch_ID.11.1 10.$Branch_ID.11.10
ip dhcp excluded-address 10.$Branch_ID.11.40 10.$Branch_ID.11.254

ip dhcp pool IP-Phones
network 10.$Branch_ID.11.0 255.255.255.0
default-router 10.$Branch_ID.11.254
option 150 ip $Call_Manager
```

A red box highlights the CLI Content tab, and a red arrow points to the "Add Variable" dialog box. The "Add Variable" dialog box is open, showing a table with the following columns: Name, Type, Description, Display Label, and Required. The table contains one row with the following values:

Name	Type	Description	Display Label	Required
Variable Name: Sortable Integer		Enter the Branch ID	Enter the Branch ID	<input checked="" type="checkbox"/>

The dialog box also includes fields for Range From (30), To (250), Default Value, and Validation Expression, along with Save and Cancel buttons.

At the bottom of the interface, there is a "Template Detail" section with a "Form View" tab. This tab is active, showing the following configuration:

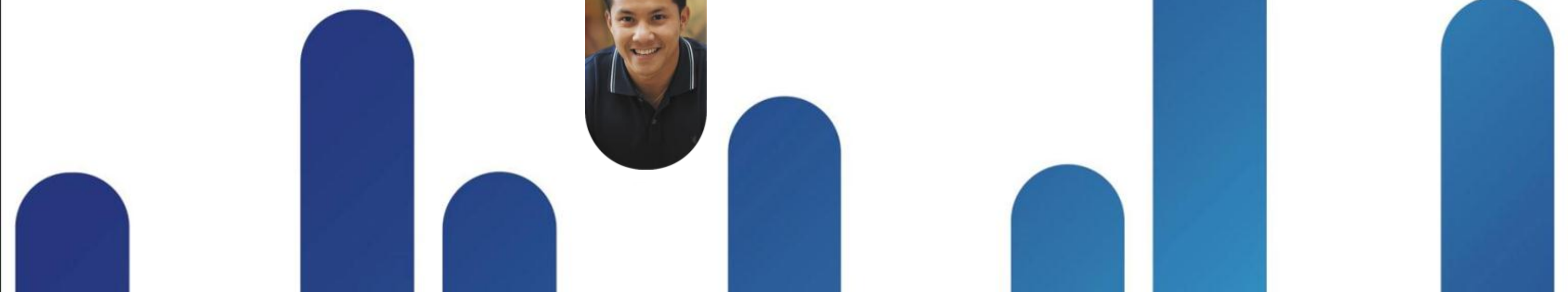
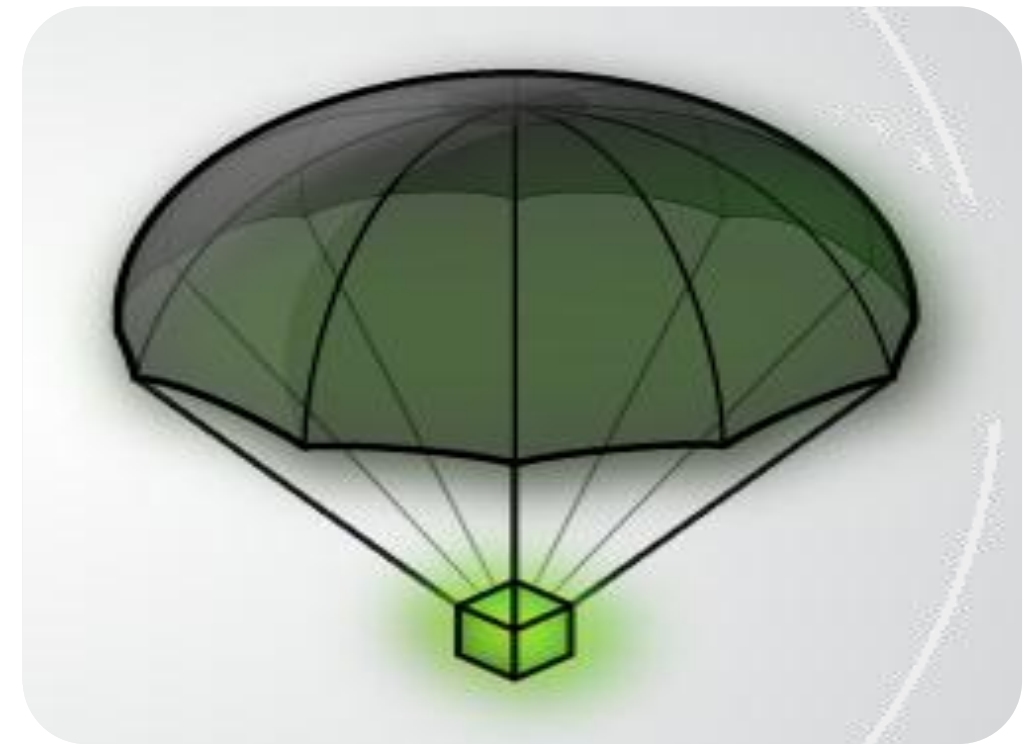
```
Enter the Branch ID: * [input field]
Call Manager: * 192.168.138.201
```

Design Site and Maps

Hierarchy of Campuses, Buildings and Floors

The screenshot displays the Cisco Prime Infrastructure interface. At the top, the navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The main content area is titled 'Maps' and shows a 'Floor View' for 'Cisco San Jose - Site 5 > BLD 14 > 3rd floor'. A signal strength legend at the top indicates a range from -35 dBm to -90 dBm. On the left, a 'Maps Tree View' and 'Floor Settings' panel are visible, with various options checked, including 'Access Points', 'AP Heatmaps', 'Clients', '802.11 Tags', 'Rogue APs', 'Adhoc Rogues', 'Rogue Clients', 'Coverage Areas', 'Location Regions', 'Obstacles', 'Rails', 'Markers', 'Chokepoints', 'Wifi TDOA Receivers', 'GPS Markers', 'Services', 'Interferers', and 'wIPS Attackers'. The main map area shows a detailed floor plan with various markers, including access points (e.g., 'SJC14-31B-AP8', 'SJC14-31B-AP6'), rogue APs (skull icons), and clients (e.g., 'jdelia', 'jepedraz', 'jacmathe'). A signal strength heatmap is overlaid on the floor plan. A 'Zoom & Pan Controls' callout points to navigation icons on the left. A '802.11u location specific service' callout points to the 'Services' checkbox in the settings. A 'Active Rogue APs' callout points to a skull icon on the map. A 'Next-Gen Maps' callout box on the right lists features: 'Reduced Clutter', 'Faster Loading', 'Better Navigation', 'Scalable Vector Graphics', and 'High quality images with zoom in/out'. The bottom left shows 'Load Status' with 'Loaded 2 out of 2 Adhoc Rogues'.

Deploy



Deploying Monitoring Templates

The screenshot shows the 'Monitoring Configuration' interface. On the left, there is a 'Templates' sidebar with a tree view. The tree is expanded to show 'Flexible NetFlow' templates, including 'Flexible_Netflow-25031097' through 'Flexible_Netflow-V7'. Below that, the 'Metrics' section is expanded to show 'Application', 'Class Based Quality of Service', 'Device Health', 'Interface Health', 'NAM Health', 'Traffic Analysis', 'Voice Video Data', 'Voice Video Signaling', and 'Threshold'.

Top N CPU Utilization

Device Name	Device IP	Average	Maximum	Minimum	Current
DEN-2911-RBR	10.0.109.2	75%	83%	69%	75%
DEN-2960S-S...	10.9.10.1	65%	65%	65%	65%
LON-3945-RBR	10.11.1.1	62%	72%	56%	58%
SF-2911-RBR	10.0.103.2	54%	85%	39%	39%
3945-East-1.cisco.com	192.168.152.1	51%	67%	43%	43%

- Device Health is automatically turned on once device is managed.
- Advanced Monitoring can be planned and designed before deploying Infrastructure
- Advanced monitoring leverage Cisco Networking Intelligence (Flexible Netflow, NBAR/NBAR2, NAM)
- Thresholds can be tied to packet capture profile for automatic captures.

Deploying Configurations on Devices

Enables simplified wireless and wired deployment of branch offices requiring common, standardised configurations

- Template based configuration to both wired and wireless devices from single GUI
- Editing and visualising configurations per device
- Enable instrumentation on routers and switches
- Create your own Golden templates and parameterise it for any device
- Provide the capability to group together discrete templates into a single composite template
- Zero Touch Device Deployments using Automated Branch Deployment

▼ Template Detail

▼ Ipssec Information

IKE Authentication Authentication Type

Encryption Policy Encryption Policy

▼ Topology and Routing Information

Select Topology Device

Create dynamic connection between spokes Sp Hu

▼ NHRP and Tunnel Parameters

*Network ID

*Hold Time 300 (secs)

*NHRP Authentication String

*Tunnel Key

*IP MTU 1400 (bytes)

TCP Maximum Segment Size 1360 (bytes)

Tunnel Source Interface

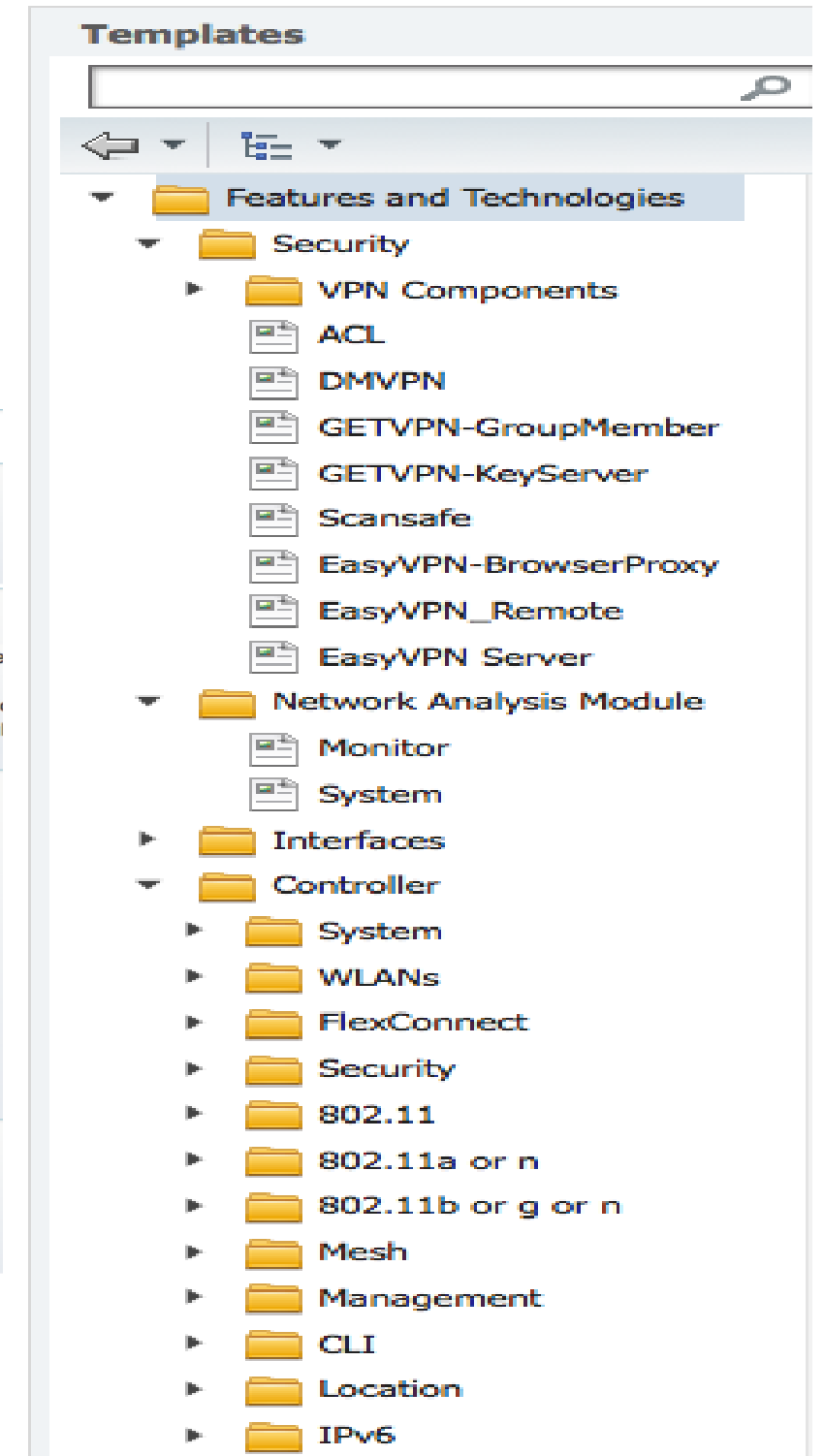
▼ NHS Information

Cluster Support

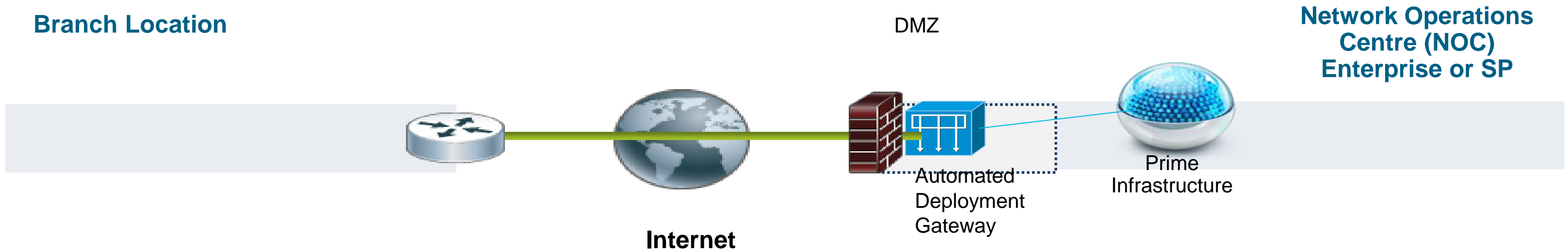
*IP Address of Hub's tunnel interface

*IP Address of Hub's physical interface

Save as New Template Cancel



Automated Deployment of New Devices



Two Deployment options:

- 1) Automated Deployment Gateway in a DMZ: devices connect to over the Internet without exposing Prime Infrastructure (*see picture above*)
- 2) Automated Deployment Gateway integrated into Prime Infrastructure (w/ release 1.2.1 Sep. 2012)



Prime Plug & Play simplifies the deployment of network

Cisco *live!*

Operate



Various Aspects of Operate

- Discovery Wired/Wireless Devices in your network using next gen discovery
- Instantly populates all of the dashboards out of the box for:
 - Site Dashboard
 - Application Dashboard
 - Incident Dashboard
 - Performance Dashboard
 - End User Experience
- Access to Operational Tools
 - Traditional – Ping, Traceroute, Packet Capture
 - Advanced – Wireless, Mediatrace, AP path



Mapping of Conventional Operational Tasks

Conventional Tasks

- Populate Device Inventory
- Managing configuration
- Upgrading devices
- Monitor Infrastructure
- Troubleshoot

In Prime Infrastructure

- Discover/Add/Import Devices
- Configuration archive operations (save, rollback, differences)
- Software image management
- Detailed Monitoring Dashboard
- Access to basic and advanced wired/wireless troubleshooting tools

Access Daily Tasks using Device Work Centre

Filter by device type, site groups, and user defined groups

1-Click Access to day-to-day operational tools !

High-Level view of managed devices

Detailed View for Selected Device

Device Work Center

Discovery Configuration Archives Software Image Management Image Dashboard Automated Deployment Status Network Audit

Device Group > Site Groups > LA Branch

LA Branch

Edit Delete Sync Groups & Sites Add Device Bulk Import

Device Name	Reachability	IP Address	Device Type	Collection Status	Collection Time	Software
<input checked="" type="checkbox"/> 3945-West-1	<input checked="" type="checkbox"/> Reachable	10.0.102.1	Cisco 3945 Integ...	Managed	August 20, 2012...	15.1(4)M1
<input type="checkbox"/> LA-3750-SBR	<input checked="" type="checkbox"/> Reachable	10.2.10.1	Cisco 3750 Stack...	Managed	August 20, 2012...	12.2(5)S
<input type="checkbox"/> WAE-574-LA-Bra...	<input checked="" type="checkbox"/> Reachable	192.168.136.66	Cisco WAE-574 ...	Managed with Warni...	August 20, 2012...	

Device Details Configuration Configuration Archive Image

System

Summary

10.0.102.1 > System > Summary

General

IP Address	10.0.102.1	Name	CISCO3945-CHASSIS
Device Name	3945-West-1	Description	CISCO3945-CHASSIS
Device Type	Cisco 3945 Integrated Services Router G2	Product ID	800-31577-02
Up Time	6 days 22 hrs 33 mins 45 secs	Version ID	A0
System Time	2012-Aug-20, 16:16:49 PDT	Serial Number	FTX1512AMQN
Reachability Status	Reachable	Inventory	
Location		Software Version	15.1(4)M1
Contact	nmtg	Model No.	CISCO3945-CHASSIS
Cisco Identity Capable	No	Port Summary	
Location Capable	No		

Populating Inventory

- Device Discovery using
 - ping sweep
 - CDP/LLDP
 - Routing Table, BGP and OSPF data
 - ARP table

Filtering capabilities

- Device can also be added
 - Manually – Individually
 - Bulk import

Discovery Settings

*Name

Protocol Settings

PingSweep Module

▼ **Layer 2 Protocols**

CDP Module

LLDP Module

▼ **Advanced Protocols**

Routing Table

Address Resolution Protocol

Border Gateway Protocol

OSPF

Filters

IP Filter

▼ **Advanced Filters**

System Location Filter

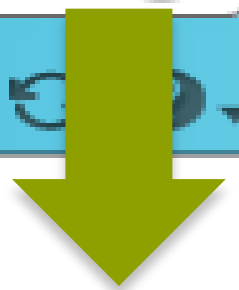
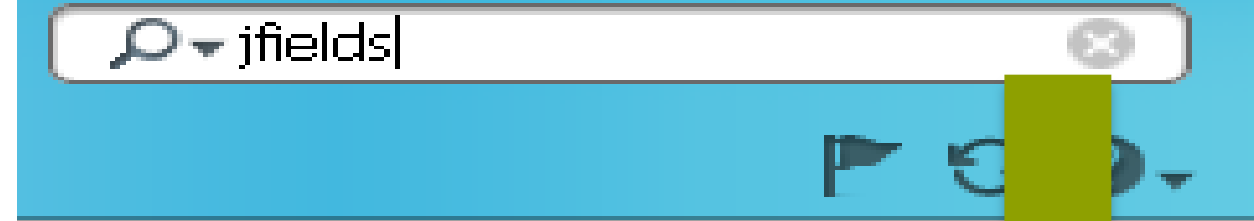
System Object ID Filter

DNS Filter

Current Discovery Settings

Save Run Now Cancel

Automated Wired/Wireless Client Discovery



Search Results

Your search 'jfields' matched following item(s). Please click on the 'View List'

Item Type	Item Count	Item List
Client	4	View List

Clients and Users

Clients Search Results - [Reset](#) Selected 0 | Total 4

Troubleshoot Test Disable Remove More Track Clients Identify Unknown Users

MAC Address	IP Address	IP Type	User Name	Type	Vendor	Device Name	Location	VLAN	Status	Interface	Protocol	Association Time
00:21:5c:01:b8:6f	192.168.152.38	Dual-Stack	jfields		Intel	AMS-2504-WLC	Root Area	13	Associated	vlan 13	802.11n(...)	2012-Aug-22, 1
00:26:b0:94:1b:6c	192.168.152.37	Dual-Stack	jfields		Apple	AMS-2504-WLC	Root Area	13	Associated	vlan 13	802.11g	2012-Aug-23, 0
dc:0e:a1:b9:22:58	192.168.152.27	IPv4	jfields		Compal	AMS-3750-SBR	Unknown	12	Disassociated	Fa1/0/6	802.3	2012-Aug-21, 1
cc:08:e0:2e:b6:32	192.168.152.36	IPv4	jfields		Apple	AMS-2504-WLC	Root Area	13	Disassociated	vlan 13	802.11n(...)	2012-Aug-21, 1



Get to the user association history in couple of clicks !!!



▼ Association History

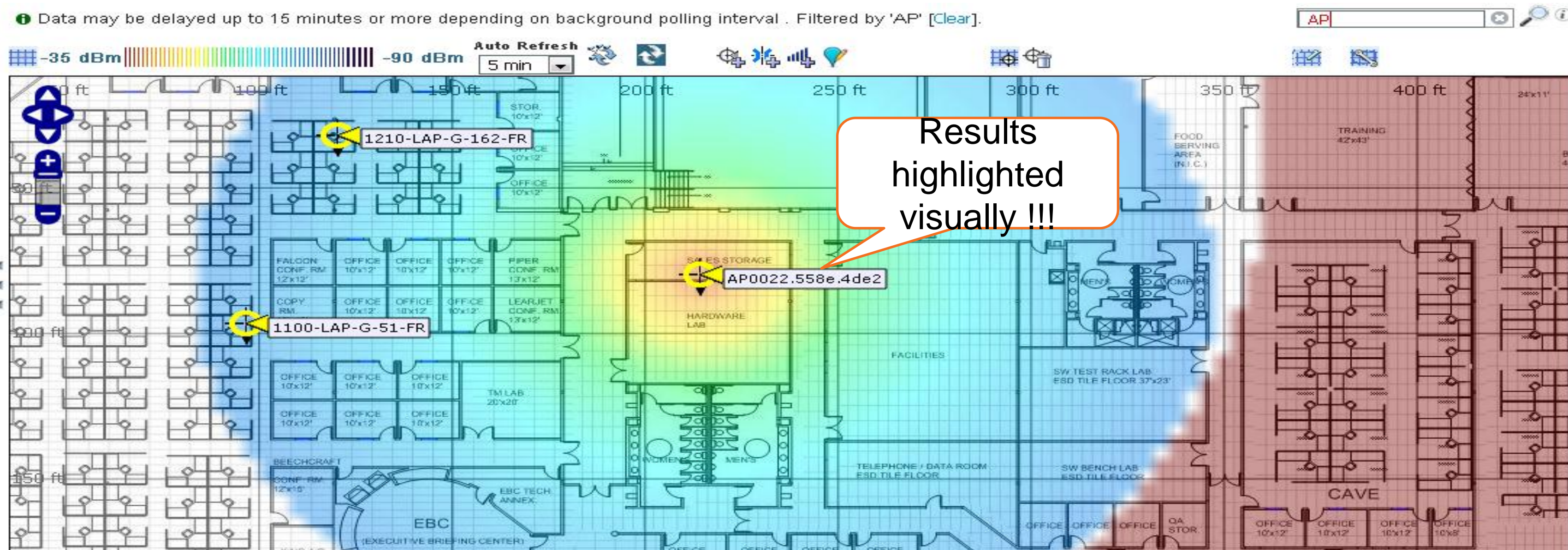
Association Time	Duration	User Name	IP Address	IP Address...	AP Name
2012-Aug-23, 09:37:45 PDT	3 hrs 8 min 4 sec	jfields	192.168.152.37	Dual-Stack	NMTG-AP3500-2
2012-Aug-22, 15:15:34 PDT	3 hrs 43 min 59 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2
2012-Aug-21, 14:38:21 PDT	17 hrs 21 min 22 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2
2012-Aug-20, 17:12:58 PDT	10 hrs 37 min 1 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2

IPv6 Visibility
Recognition of IPv6 Global and Link Local Addresses

AP are discovered and can be automatically associated to a map based on naming rule

Comprehensive search

Search by MAC, IP or Name for any map element



Results highlighted visually !!!

*note:association of AP on a map can be automatic but positioning of AP on the map is manual

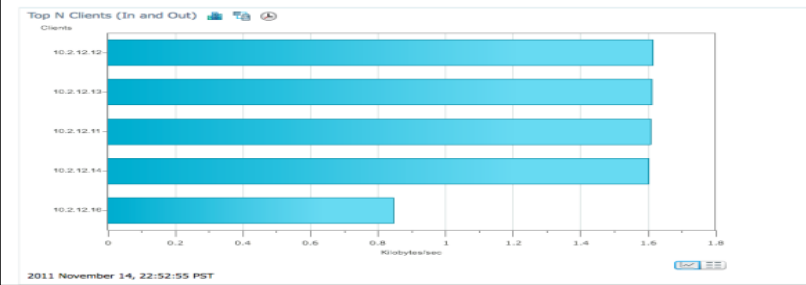
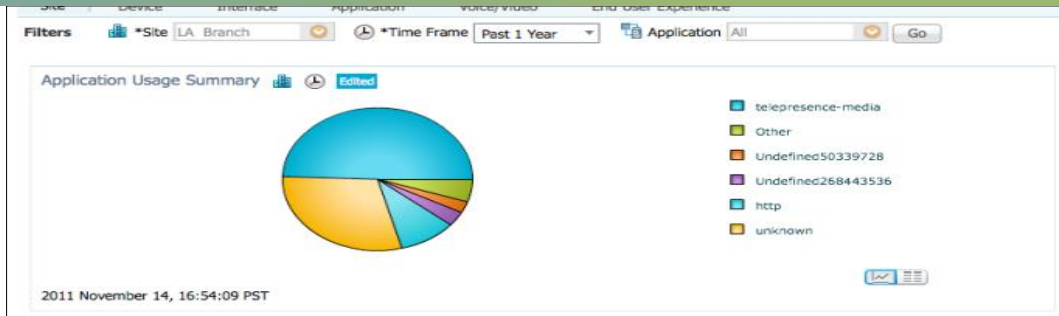
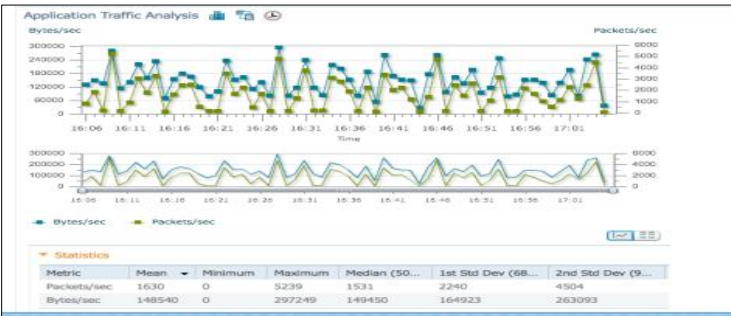
Multi-NAM Management

DISCOVER

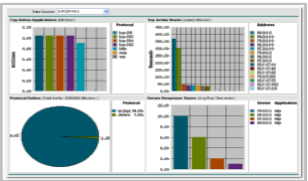
MANAGE

CONFIGURE

DATA-SOURCE



Cisco Prime NAM for WAAS VB



Cisco Prime NAM for Nexus 1010)



NAM 2200 Series Appliance



Cat65xx NAM3 Blade+



Cat65xx/C76xx NAM1, NAM2 Blades



Cisco Prime NAM for ISR G2 SRE



Cisco ISR/G2 NAM Blade

Multi-NAM Manager

Prime Infrastructure provides central discovery, reporting of data (ART/TA/RTP), packet capture, pcap file management, application definition, WAAS server config, image mgmt across multiple NAMs in an enterprise.

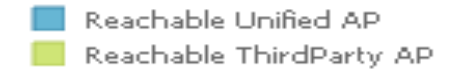
3rd Party Support

- ✓ 3rd Party Support for Wired and Wireless Devices
- ✓ Basic : MIB2 Monitoring, Inventory, and Availability

Network Device Summary

Total Managed Device Count: **79**

AP Availability: **3**



Device Group > Device Type > Third Party Wireless Controller > **Aruba 620 Series controller**

Aruba 620 Series controller

Selected 1 | Total 1

Edit Delete Sync Groups & Sites Add Device Bulk Import

Device N...	Reachability	IP Address	Device Type	Status	Software V...	Inventory Collection Ti...	AP Co...	Auto ...	Auto ...	Config...
<input checked="" type="checkbox"/> SFO-ARUBA...	<input checked="" type="checkbox"/> Reachable	10.3.10.2	Aruba 620 ...	Managed	6.1.1.0	2012-Aug-23, 03:02:50 PDT	2	false	false	true

Device Details

System > Ports > General

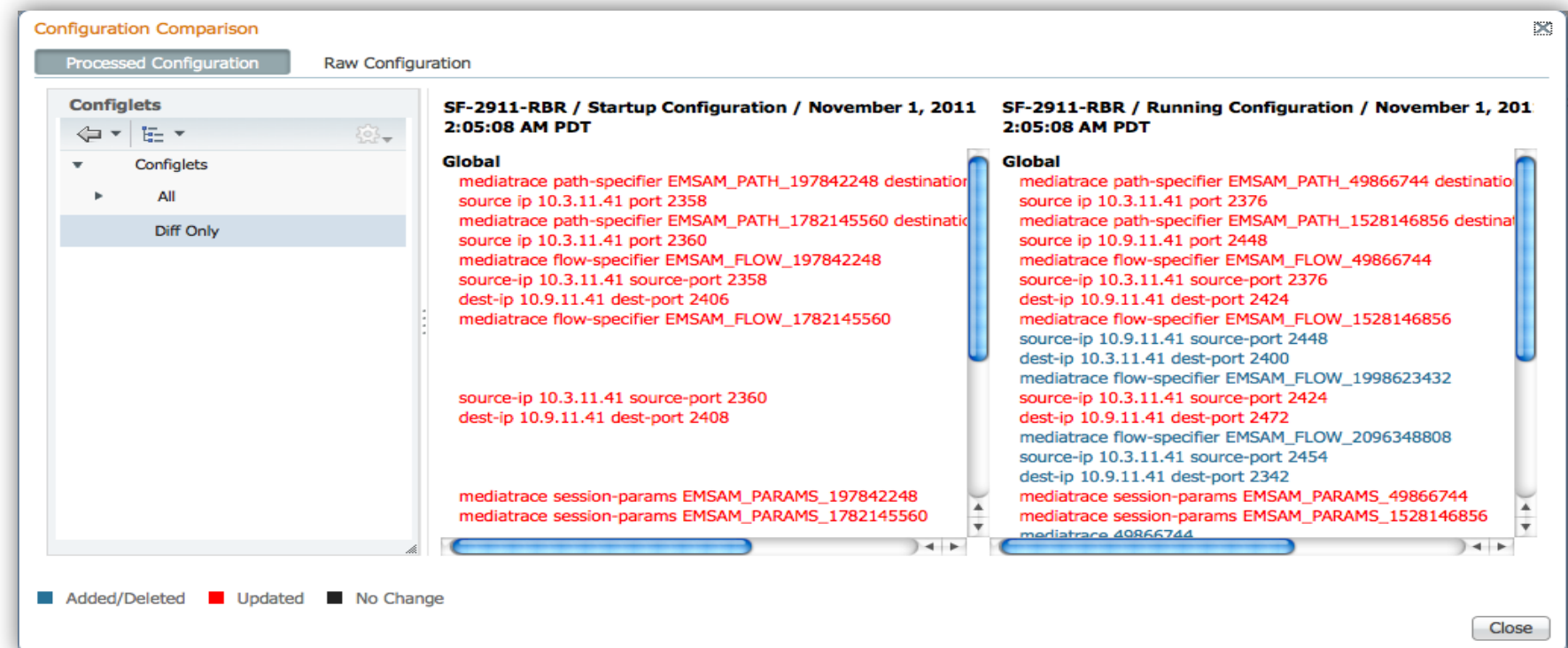
Monitor > Controllers > 10.3.10.2 > Ports > **General**

Port	Physical Mode	Admin Status	Port Type	Link Status
1	ACCESS	ENABLED	FASTER ETHERNET	●
2	ACCESS	ENABLED	FASTER ETHERNET	●
3	ACCESS	ENABLED	FASTER ETHERNET	●



Conventional Configuration Mgmt. Features

- 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.



Device Software Image Management

Import

Analyse

Distribute

Import Images

Source

- Device
- Cisco.com
- URL
- File

Collection Options

Select Device Platform

Select Image Version

Select Feature Package

Selected Image **c3750e-universal**

Upgrade Analysis

Image Source

- Local Repository
- Cisco.com

Device Selection

Devices

<input checked="" type="checkbox"/>	Name	Description
<input type="checkbox"/>	▶ ALL	All Members
<input type="checkbox"/>	▼ Device Type	Device Type
<input type="checkbox"/>	▶ Routers	Routers
<input checked="" type="checkbox"/>	▼ Switches and Hubs	Switches and Hubs
<input checked="" type="checkbox"/>	▼ Cisco Catalyst 3750 Series Swi	Cisco Catalyst 3750 Se
<input type="checkbox"/>	NY-3750-SBR.cisco.com	NY-3750-SBR.cisco.co
<input checked="" type="checkbox"/>	SF-3750-SBR	SF-3750-SBR
<input type="checkbox"/>	NY-3750-SBR	NY-3750-SBR

Image Selection

Distribute Images

Device Selection

- Show All Devices ⓘ

List of devices displayed are based on Images Selected ⊕

Devices

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	▼ Cisco Catalyst 3750 Series Swi	Cisco Catalyst 3750 Series Switches
<input type="checkbox"/>	NY-3750-SBR.cisco.com	NY-3750-SBR.cisco.com
<input type="checkbox"/>	SF-3750-SBR	SF-3750-SBR
<input type="checkbox"/>	BXB-3750-SBR	BXB-3750-SBR
<input type="checkbox"/>	SIN-3750-SBR	SIN-3750-SBR
<input type="checkbox"/>	LON-3750-SBR	LON-3750-SBR
<input type="checkbox"/>	RTP-3750-SBR	RTP-3750-SBR
<input type="checkbox"/>	LA-3750-SBR	LA-3750-SBR
<input type="checkbox"/>	FL4-3750-2	FL4-3750-2

Fault are Detected with Alarms and Events

- Alarms are generated from Events.
- Events can be trap, syslog or threshold violation
- Conventional actions are available :
 - Filter
 - Clear
 - Acknowledge
 - Annotate
- Troubleshooting tools are available :
 - ping, traceroute
 - show commands

The screenshot shows the 'Alarms & Events' interface. On the left is a 'Device Groups' tree with categories like 'ALL', 'Device Type', 'Cisco Interfaces and Modules', 'Wireless Controller', 'Unified AP', 'Switches and Hubs', 'Site Groups', and 'User Defined'. The main area displays a table of events with columns for Severity, Message, Status, Source, Timestamp, Owner, Category, and Condition. The table contains 15 rows of events, including security risks and interference threshold violations.

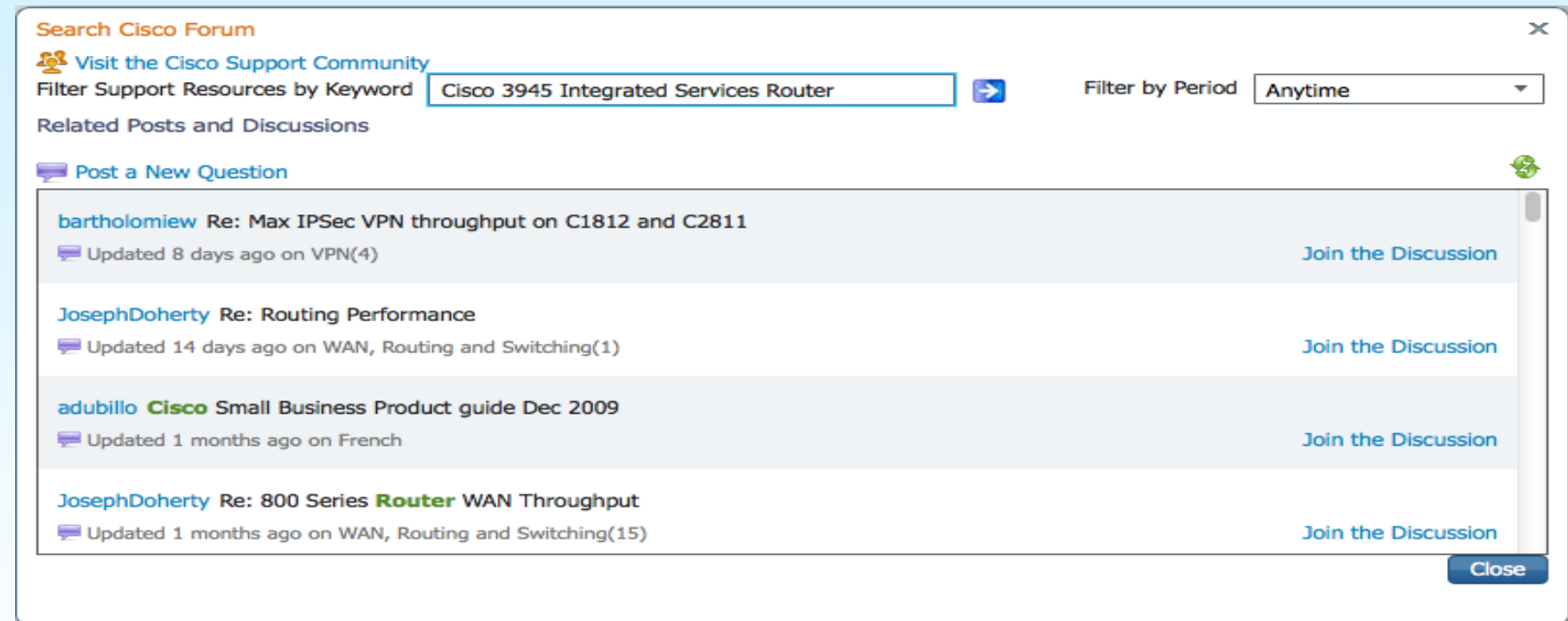
Severity	Message	Status	Source	Timestamp	Owner	Category	Condition
Critical	Security-risk Interferer 'Bluetoo...	Not Acknowle...	Lrad1f04:fe:7f:48:dc:9010	July 23, 2012 7:30:17 PM PDT		Security	Interferer Security Traps
Minor	Interference threshold violation...	Not Acknowle...	Lrad1f00:23:eb:ad:8c:f010	July 23, 2012 7:29:46 PM PDT		AP	
Critical	Security-risk Interferer 'DECT ...	Not Acknowle...	Lrad1f64:d9:89:47:66:a010	July 23, 2012 7:29:24 PM PDT		Security	Interferer Security Traps
Minor	Interference threshold violation...	Not Acknowle...	Lrad1f00:19:07:8d:5d:6010	July 23, 2012 7:29:19 PM PDT		AP	Interference
Critical	Security-risk Interferer 'WiFi In...	Not Acknowle...	Lrad1f04:fe:7f:48:dc:9010	July 23, 2012 7:29:14 PM PDT		Security	Interferer Security Traps
Minor	Noise threshold violation report...	Not Acknowle...	Lrad1f00:22:55:44:8e:e010	July 23, 2012 7:28:54 PM PDT		AP	Noise
Critical	Security-risk Interferer 'Bluetoo...	Not Acknowle...	Lrad1f04:fe:7f:49:27:0010	July 23, 2012 7:28:44 PM PDT		Security	Interferer Security Traps
Critical	Security-risk Interferer 'Bluetoo...	Not Acknowle...	Lrad1f04:7d:4f:53:35:9010	July 23, 2012 7:28:37 PM PDT		Security	Interferer Security Traps
Minor	Noise threshold violation report...	Not Acknowle...	Lrad1f00:22:55:12:7f:9010	July 23, 2012 7:28:20 PM PDT		AP	Noise
Critical	Security-risk Interferer 'WiFi In...	Not Acknowle...	Lrad1f04:7d:4f:53:28:2011	July 23, 2012 7:28:16 PM PDT		Security	Interferer Security Traps
Critical	Security-risk Interferer 'Bluetoo...	Not Acknowle...	Lrad1f04:7d:4f:53:35:9010	July 23, 2012 7:28:09 PM PDT		Security	Interferer Security Traps
Critical	Security-risk Interferer 'TDD Tr...	Not Acknowle...	Lrad1f04:7d:4f:53:12:9011	July 23, 2012 7:27:31 PM PDT		Security	Interferer Security Traps
Minor	Interference threshold violation...	Not Acknowle...	Lrad1f64:d9:89:42:23:5010	July 23, 2012 7:26:34 PM PDT		AP	Interference
Critical	Security-risk Interferer 'WiFi In...	Not Acknowle...	Lrad1f3c:ce:73:1a:26:9011	July 23, 2012 7:26:19 PM PDT		Security	Interferer Security Traps
Minor	Interference threshold violation...	Not Acknowle...	Lrad1f04:7d:4f:52:d5:6010	July 23, 2012 7:25:49 PM PDT		AP	Interference

The screenshot shows the details for a specific event. The event is 'Device '10.0.107.2'. Authentication failed.' with a severity of 'Minor'. The details are organized into several sections:

- General Information:** Source: 10.0.107.2, Owner: prime, Acknowledged: No, Category: Routers, Alarm Found At: July 18, 2012 10:29:23 PM PDT, Alarm Last Updated At: July 23, 2012 4:29:38 PM PDT, Alarm Detected Through: Wired Switch, Severity: Minor, Previous Severity: Minor.
- Device Details:** IP Address: 10.0.107.2, Device Name: IND-2951-RBR, Device Type: Cisco 2900 Series Integrated Services Routers G2, Up Time: 12 days 1 hrs 14 mins 57 secs, Reachability Status: Reachable, Collection Status: Managed, Software Version: 15.1(4)M2, Serial Number: 6517522, Location: INDIA 2900 Branch Router, Contact: (empty).
- Messages:** Device '10.0.107.2'. Authentication failed.
- Annotations:** A table with columns for Message, Posted By, and Timestamp. It shows 'Alarm assigned' and 'Device Updated with latest con...' both posted by 'prime' on July 23, 2012.
- Device Events:** A table with columns for Severity, Description, Source, and Timestamp. It shows 'Port {0} is up on device {1}' (Cleared) and 'Port {0} is down on device {1}' (Critical) events.

Smart Interactions – Allows to Communicate with Cisco Support Community

- ✓ Context Sensitive Device search
- ✓ Post to Cisco Support Community from the same interface
- ✓ One click access to support communities & Cisco knowledge base



- Less time needed to resolve problems
- Communicate with other Cisco experts

Smart Interactions – Allows to Open Ticket (Service Requests)

- ✓ Integrated Cisco service request management: Automates the service request process
- ✓ Create support cases with Cisco-TAC and partners
- ✓ Case status look-up
- ✓ Automatic attachment of problem context to the support cases

Create TAC Request

All fields required unless indicated as optional

Contact Information

Name: ABC Test CPR
Phone: 31-612349999x44-44
Email: srgthota@gmail.com
Preferred Contact Method: Phone Email

Problem Description

Problem Title: test_problem
Severity: S3 - Network or E
Description: Device 10.77.211.201 experienced an OperationallyDown at 27-Jun-2011 10:04:01
What were you doing when you experienced this problem? Operate

Technology Details

Technology: Router and IOS Architecture
Sub-Technology: IOS High CPU
Type of Problem: Software Failure

Supporting Documents (Optional)

Show technical info of the device
 Latest configuration difference
 Events for the last 24 hours
[Attach my own file](#)

Device and Contract Information

Device Name: 10.77.211.201
Device OS Type: -
Device Serial Number: SMT11100559
Contract Number: 3628249



- Less time needed to resolve problems
- Communicate with other Cisco experts

Lifecycle – GUI & Dashboards



Lifecycle versus Classic View



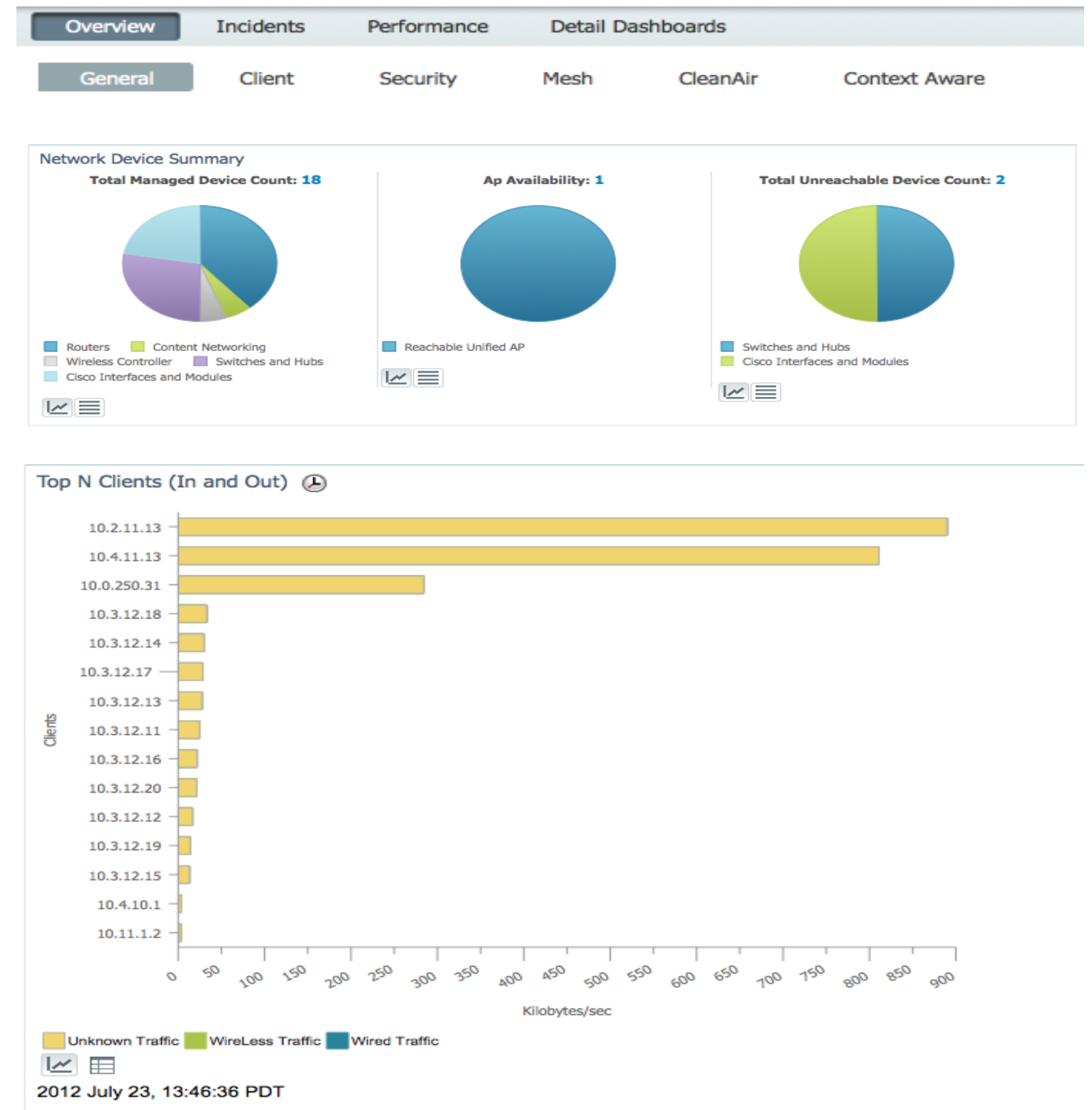
Lifecycle View : This is the default view for wired/wireless management using Design > Deploy > Operate > Report cycle

Classis View : Eases migration for existing NCS 1.x customers



Network Overview

- Hierarchical dash boards that reflect the converged network status in real time
- Drill down capabilities to troubleshoot and arrive at rich set of information in one click
- User defined dashboards that allows to create your own view
- Contextual Site, Device, Interface Application, End User experience dashboards to display dynamic network health status
- Service/Domain specific contents grouped in one view



Site Dashboard

Voice/Application/End User Site Experience

- Contextual site based information from one view
 - What services and users will be affected in my site – *Assessed by looking at Devices that are down in a site*
 - My Applications are down, who are the users that are affected by that – *Obtained by looking at Applications accessed by end users in a site*
 - What are the devices that needs to be replaced or requires maintenance in my site - *Top N worst devices that are underperforming in a site*
 - Are other users in the site affected by latency in transaction time - *Users having the most issues in the site*

Device Reachability Status

Device Name	Device IP	Location	SNMP Reachability
sjc24-wnbu11a-sw1.Cisco...	10.33.21.153		✓ Reachable
Cisco_d6:f6:e4	10.34.138.11	SJC14 13 NOCa	✓ Reachable
oeap-talwar-2	171.70.35.133	SJC-14 BDF 2.2	✓ Reachable
Cisco_69:51:e0	10.32.36.10	SJC14 22 BDF	✓ Reachable
Cisco_ea:00:63	10.32.36.4	SJC14 2nd Floor BDF	✓ Reachable
Cisco_7d:88:00	171.70.35.131	SJC-14 BDF 2.2	✓ Reachable
Cisco_d5:02:4f	10.32.34.2	SJC-14 IDF-2.1	✓ Reachable
Cisco_fe:56:00	10.32.37.6	SJC14 22 BDF	✓ Reachable
Cisco_32:1b:23	10.32.37.4	SJC14 2.2 BDF	✓ Reachable
Cisco_fe:54:20	171.70.35.135	SJC-14 BDF 2.2	✓ Reachable

2012 July 23, 20:39:30 PDT

Worst N Clients by Transaction Time

Client	Type	User	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Art Analysis	Past 24 Hour Trend (ms)
10.7.12.12	unclassified	204	65		53
10.7.12.13	unclassified	131	63		54
10.7.12.11	unclassified	58	53		54
10.7.11.17	unclassified	3	1		1
10.7.11.12	unclassified	2	1		1

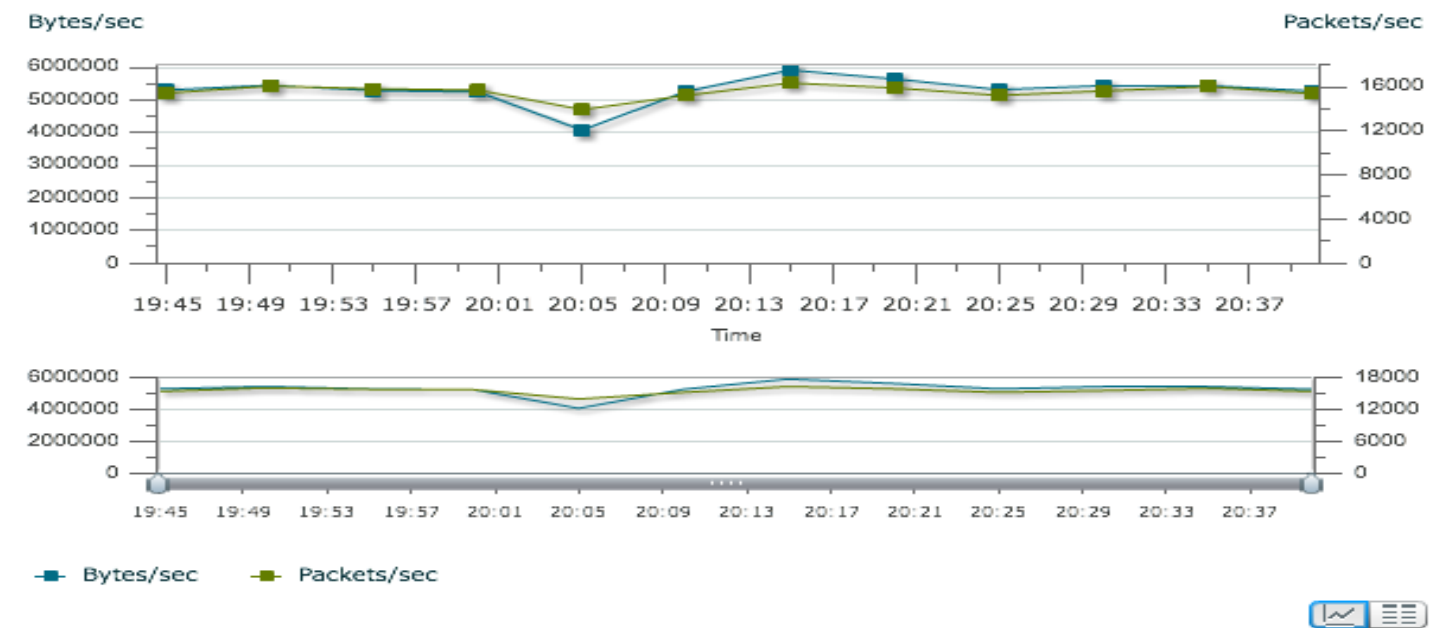
2012 July 23, 20:40:54 PDT

Application Dashboard

Application Performance and End User Experience

- Contextual Application based information from one view
 - What are the Top Server and Top Clients in my network that are having worst transaction time – *Assessed by looking at the Worst Clients by transaction time and Application Server Performance*
 - Which of my Sites are experiencing worst transaction time for any given application – *Obtained by looking at Worst Sites by transaction time*
 - Which of my Clients are using the most bandwidth- *Top N Clients (In and Out)*
 - How is my Application Traffic statistics over time- *Application Traffic Analysis dashlet*

Application Traffic Analysis 📊



Worst N Sites by Transaction Time 📊

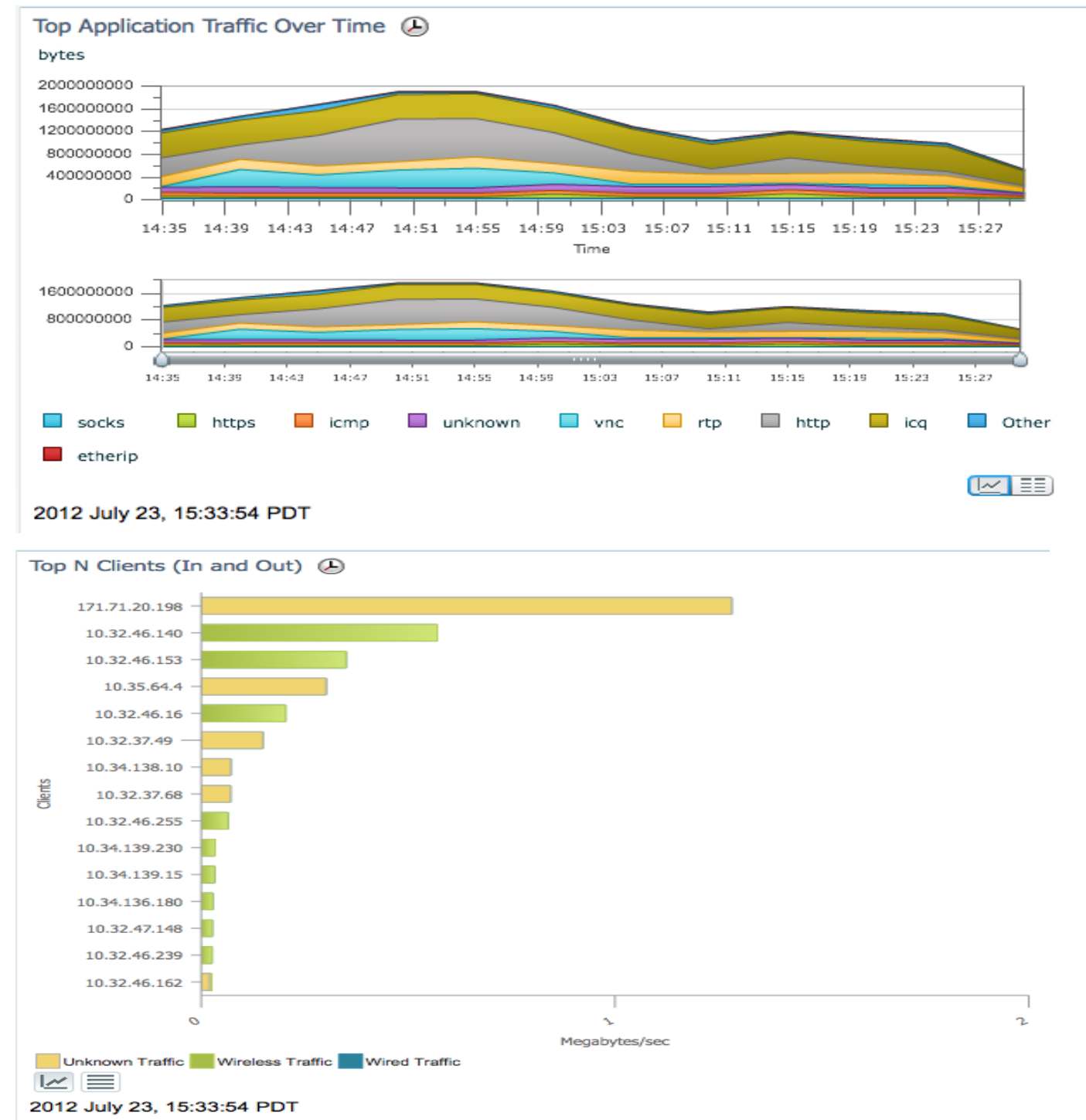
Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Past 24 Hour Trend (ms)	
Unassigned	cisco-callmanager	60028	36773		15005
Unassigned	pip	30583	30245		30367
Unassigned	rmiregistry	31613	29035		30220
Unassigned	mapi	255850	25043		35774
Unassigned	cisco-sccp	30907	16361		15537

2012 July 23, 20:45:01 PDT

Interface Dashboard

■ Interface Centric View

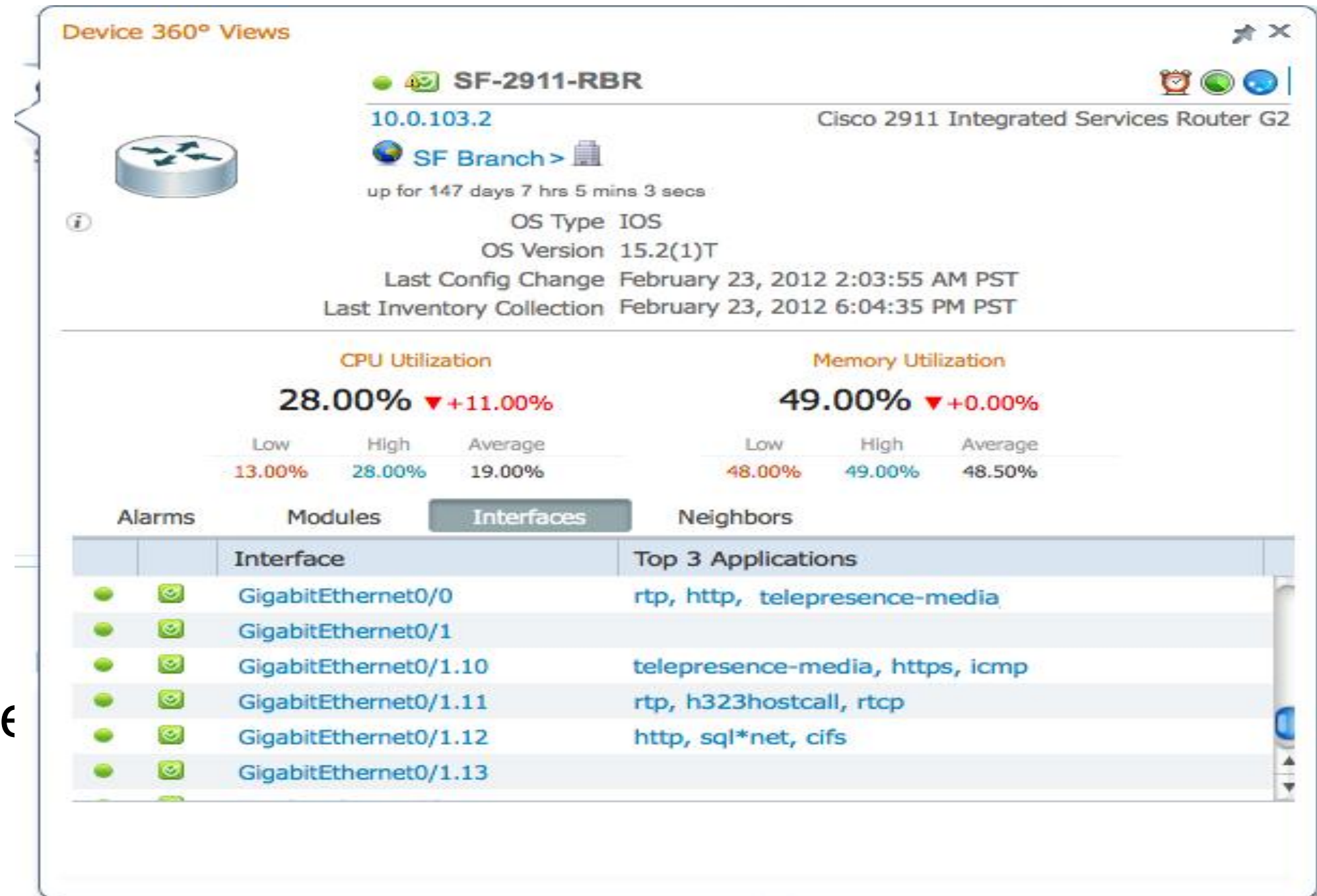
- What is my total over all In and Out bandwidth through my WAN interface? – *Interface Tx and Rx Utilisation trend*
- What application traffic occupies most bandwidth on a given interface–
Assessed by looking at Top N Application
- Are most traffic through an interface Wireless or Wired - *Obtained by looking at Top N Application traffic over time*
- What is bandwidth savings on account of applying Class based Qos, how many packets got dropped-
Obtained by looking at Class Map statistics



Device 360 View

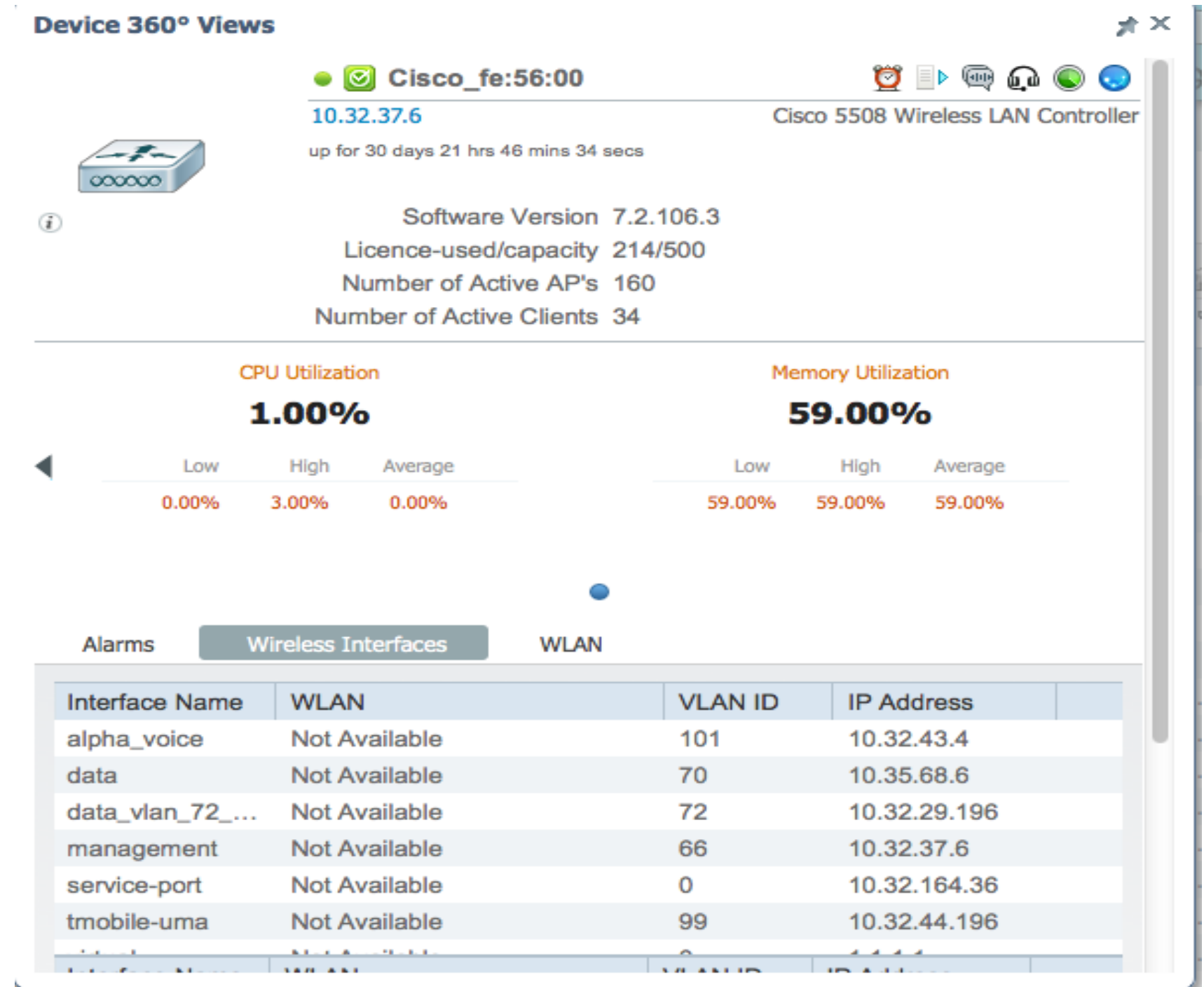
Contextual drill down for device troubleshooting

- Realtime contextual device details from “device” perspective
 - Device name, location and type with system uptime
 - OS version and status
 - CPU and Mem utilisation
 - Interface status type and visibility of application traffic
- Provides quick snapshot to isolate and troubleshoot device related issues



Wireless Device 360 View

- Concise wireless information about devices from anywhere within the product
- 360 views available for wireless Controller & APs
- On click shows the following
 - OS version and status
 - License used/Capacity
 - Number of Active Aps
 - Number of Active Clients
 - CPU and Mem utilisation
- Provides snapshot of wireless interfaces, alarms and WLAN



Assurance



Assurance

Improve Application visibility and end user experience

End User Experience

- ✓ **Wired/Wireless user experience - Top applications based on end point type, BW Utilisation, etc.**
- ✓ Voice quality experience
- ✓ Path Trace (for Voice/Medianet Applications)

Visibility

- ✓ Traffic Analysis & Reporting
- ✓ **End-to-end application performance**
- ✓ **Multi-NAM: Packet level debugging and troubleshooting**
- ✓ **WAN optimisation visibility**

Network Performance

- ✓ Availability and Performance polling with Event/Alarm generation
- ✓ Custom MIB poller
- ✓ **Configuration of devices for data and flow collection: NetFlow, Medianet, PA, NBAR**

How is Assurance Achieved ?

By normalising and correlating data across multiple sources – leverage the power of embedded Cisco instrumentation



NAM module/Appliance

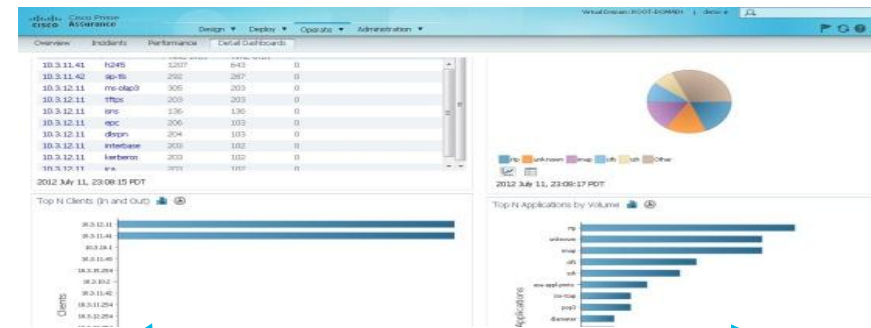


Cisco ISR
NBAR2, PA, Medianet



Cisco ASR
NBAR2, AVC, Medianet

Prime Infrastructure



NetFlow Generation Appliance (NGA) 3140

Wireless Controller
NBAR2



Cisco Catalyst 3750-X w/ 3K-X 10G
Netflow, Medianet



Cisco 6509
Netflow, Medianet



SNMP/CLI
Polling



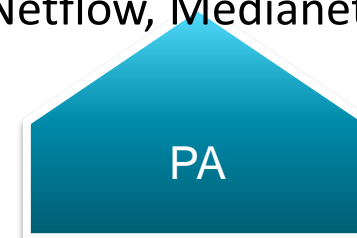
SPAN/
ERSPAN



Netflow



WAAS



PA



MEDIANET



NBAR



NBAR2



Rich Application Visibility and Analysis

Site Device Interface **Application** Voice/Video End User Experience

Filters *Application citriximaclient *Time Frame Past 1 Hour Site Go

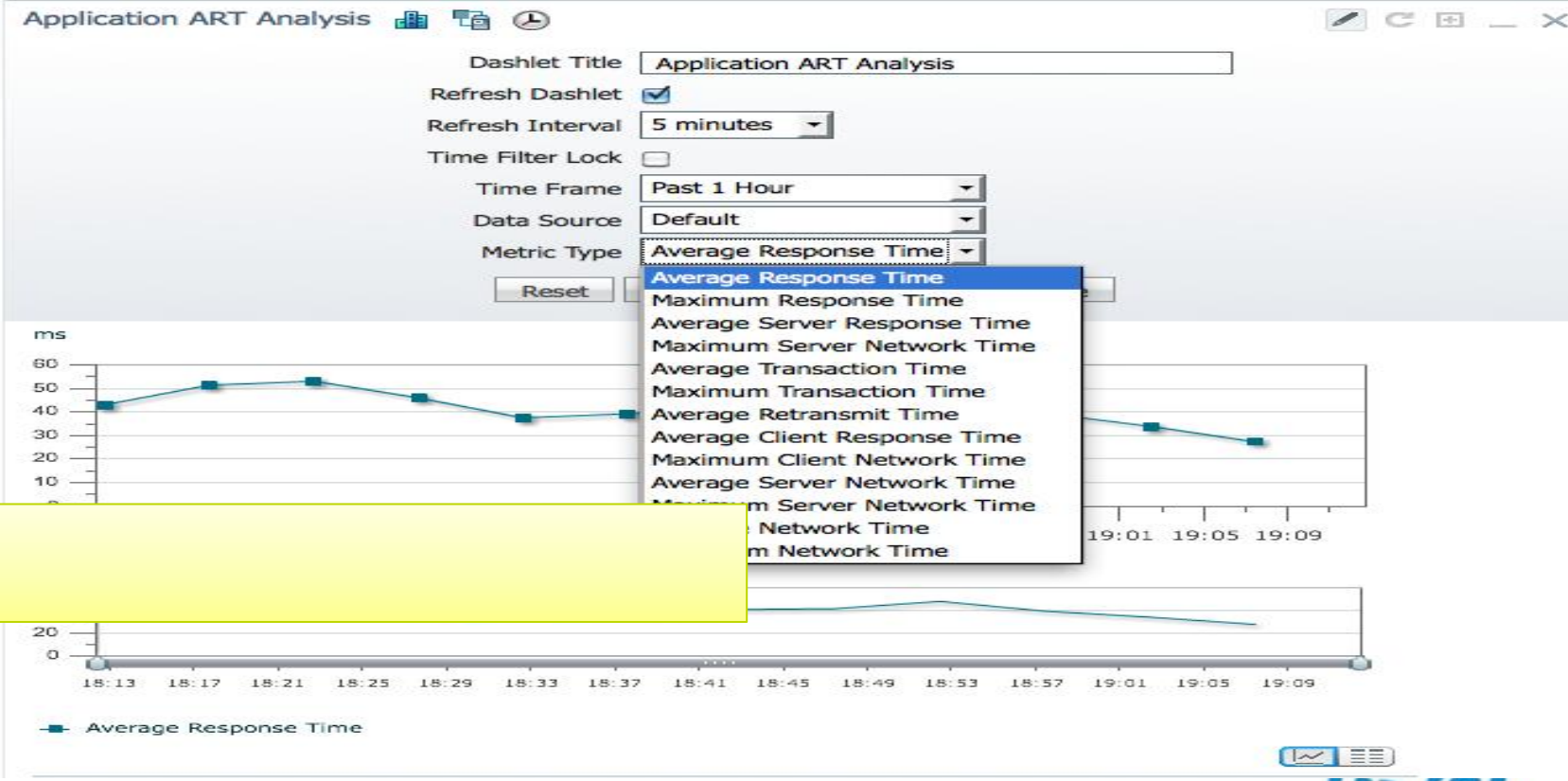
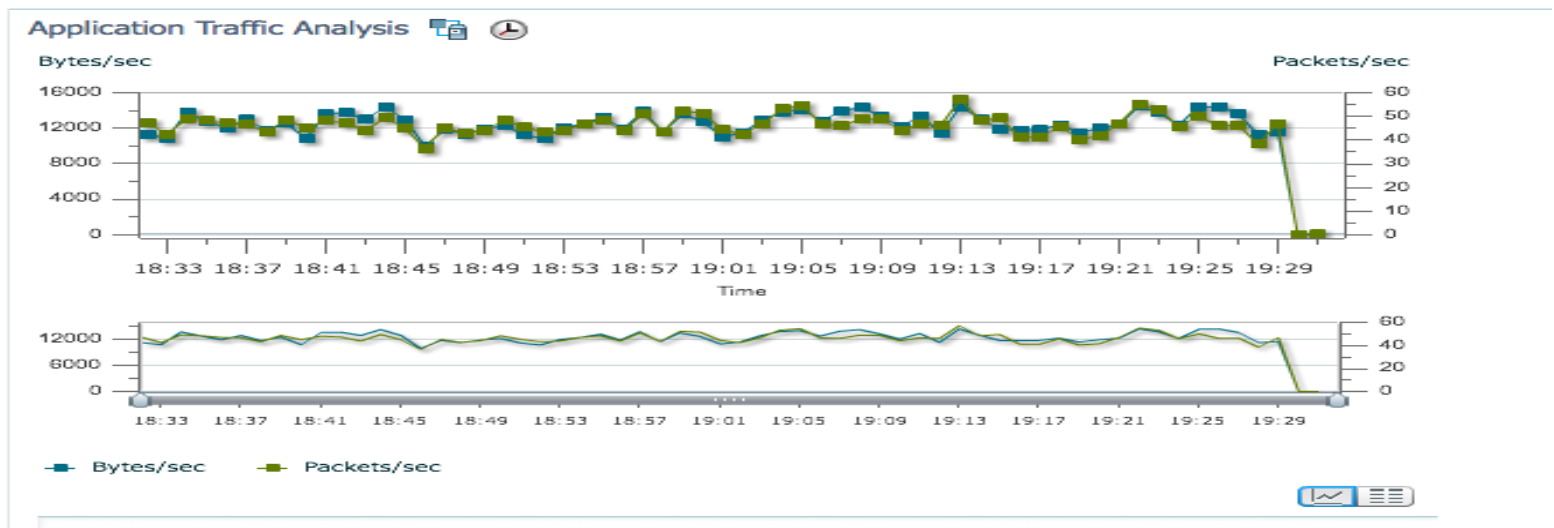
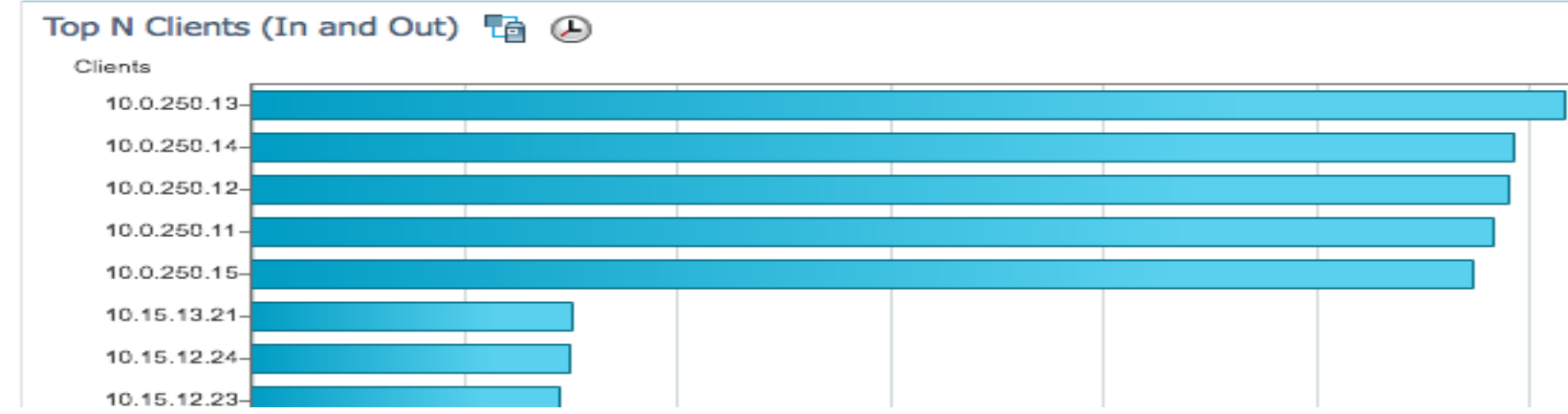
Experience

Analysis

Server

Worst N Sites by Transaction Time

Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Past 24 Hour Trend (ms)
IND Branch	citriximaclient	5015	1585	
SJ Data Center	citriximaclient	5015	604	
San Jose Campus	citriximaclient	1036	594	
LON Branch	citriximaclient	975	514	
RTP Branch	citriximaclient	892	241	



App Server Performance

App Server	Site	Application	Maximum Transaction Time (ms)	Average Transaction Time (ms)	Past 24 Hour Trend (ms)
10.0.250.13	SJ Data Center	citriximaclient	415	798	
10.0.250.12	SJ Data Center	citriximaclient	413	884	
10.0.250.11	SJ Data Center	citriximaclient	360	932	
10.0.250.14	SJ Data Center	citriximaclient	333	580	
10.0.250.15	SJ Data Center	citriximaclient	333	580	

See the right information from the right source

The screenshot shows the Cisco NAM configuration interface. At the top, there are tabs for 'Site', 'Device', 'Interface', 'Application', and 'Vc'. Below these, there are filter sections for '*Site' (set to 'LON Branch') and '*Time Frame'. The main area is titled 'Top N Applications' and contains a configuration table:

Dashlet Title	Top N Applications
Refresh Dashlet	<input checked="" type="checkbox"/>
Refresh Interval	5 minutes
Sort Order	Descending
No. of Rows	15 (Default)
Traffic Type	All Traffic
Data Type	Rate
Override Dashboard Time Filter	<input type="checkbox"/>
Time Frame	Past 1 Hour
DSCP	All
Filter By	Datasource
Datasource	All

At the bottom of the configuration area are buttons for 'Reset', 'Save', 'Save And Close', and 'Close'. A 'Datasource' dropdown menu is open, showing a list of data sources:

- 192.168.152.2-2691360
- ACC-NAM2204.cisco.com-DATA POR...
- ACC-NAM2204.cisco.com-DATA POR...
- ACC-NAM2204.cisco.com-DATA POR...
- ACC-NAM2204.cisco.com-DATA POR...
- Campus-NAM3.eset-cisco.com-DATA ...
- Campus-NAM3.eset-cisco.com-DATA ...
- DC-NAM2220.cisco.com-DATA PORT 1
- DC-NAM2220.cisco.com-DATA PORT 2
- NAM-External
- NAM-Internal
- RTP-NAM-SRE.cisco.com-External
- RTP-NAM-SRE.cisco.com-Internal

Select from one of the data sources:

- Netflow
- Flexible Netflow
- NAM NDE
- NAM Data Port

Obtain Voice and Video Stats Out of the Box

Worst N RTP Streams by MOS

RTP Streams	Max. MOS	Avg. MOS	Min. MOS	Past 24 Hour Trend	
Management to San Jose Campus	4.34	4.15	3.45		4.2
SJ Data Center to Management	4.38	4.26	3.81		4.3
San Jose Campus to RTP Branch	4.3	4.29	4.28		4.3
Management to SJ Data Center	4.38	4.38	4.38		4.4
San Jose Campus to Management	4.38	4.38	4.38		4.4

Site to Site
Voice
Statistics

Worst N Sites by MOS

Site	Max. MOS	Avg. MOS	Min. MOS	Past 24 Hour Trend	
SJ Data Center	4.38	4.33	2.19		4.38
RTP Branch	4.38	4.34	4.16		4.35
San Jose Campus	4.37	4.37	0		4.37
Management	4.38	4.38	0		4.38

Worst Site
by MOS
Scores

Several additional portlets are available out of the box for Dashboards

Realtime Voice Troubleshooting

Identify the root cause of a bad voice call

Troubleshoot the RTP conversations thanks to key metrics like jitter, loss or MOS score

Leverage Medianet instrumentation to obtain and analyse the service path for a conversation

The screenshot displays the Cisco Prime Assurance interface for RTP troubleshooting. The top section, titled "RTP Conversations Details", shows a table of conversation metrics. The second row is selected, showing a jitter of 73.1 ms and a packet loss of 7. Below this, the "RTP Stream details" section provides specific metrics: Start Time 01-May-12 09:44:00, Reported Jitter (ms) .03, and Reported Packet Loss 36. The source and destination IP addresses and ports are also listed. The bottom section, "Medianet Path View", shows a network diagram with four routers (sam-r4, sam-r3, sam-r2, sam-r1) and their respective IP addresses. The path from sam-r4 to sam-r1 is highlighted, indicating the service path for the conversation.

	Jitter (ms)	Packet	Source...	Destinat...	Type	Source U
Trace Service Path						
Analyze on Multiple Data Sources	196.4	8	19268	18252		
10.4.11.13	175.4	8	19268	18252		
10.4.11.111	73.1	7	2432	2400		
10.4.11.111	76.5	7	2432	2400		
10.4.11.111	73.3	6	2432	2400		
10.4.11.111	77.2	6	2432	2400		

RTP Stream details

Start Time 01-May-12 09:44:00
Reported Jitter (ms) .03
Reported Packet Loss 36

Source IP Address 10.64.92.176
Source Port 23796
Source Site Unassigned

Destination IP Address 10.64.92.201
Destination Port 22818
Destination Site Unassigned

Med...	Router	Dist...	Status	Action
10.64.92.30	10.64.92.30	0	Completed	Restart Mediatrace

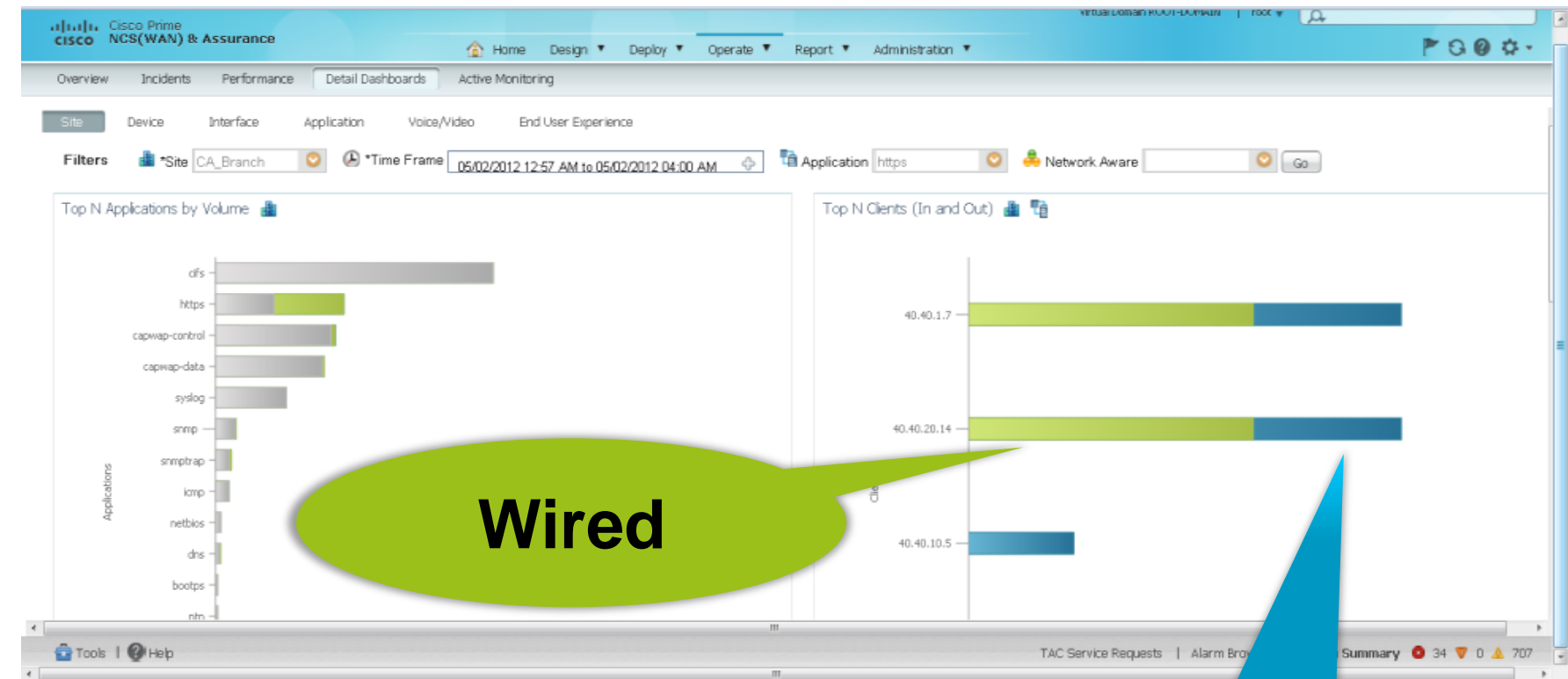
Medianet Path View

Step 5 of 5 : Mediatrace completed

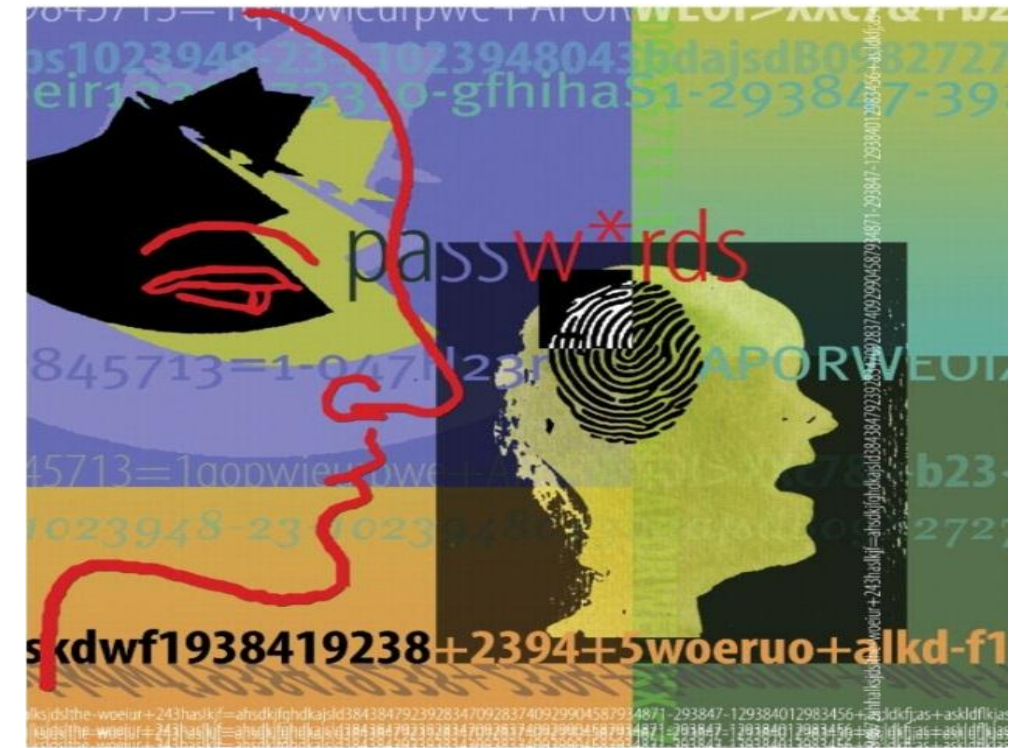
Assurance is Wired/Wireless Convergence!

■ End user experience

- Top applications accessed by end users based on the end point type
- Applications where the end user is having performance issues
- Bandwidth utilised by end users for applications
- Comparison of end user to users site experience to isolate issues



Compliance



Best Practices

Ensure Corporate and Regulatory Compliance

- Enables IT organisations assess their network and devices for out-of-policy configurations, security and risk vulnerabilities
- Robust out-of-the-box compliance rules engine for customisable compliance auditing based on Cisco and industry best practice rules
 - Analysis against EOL and PSIRT notifications
- Optional - regulatory compliance reporting against specific industry initiatives such as:
 - PCI/DSS**
 - HIPAA
 - STIGS
 - NERC



Compliance Reports in Prime Infrastructure

Home Design Deploy Operate Report Administration

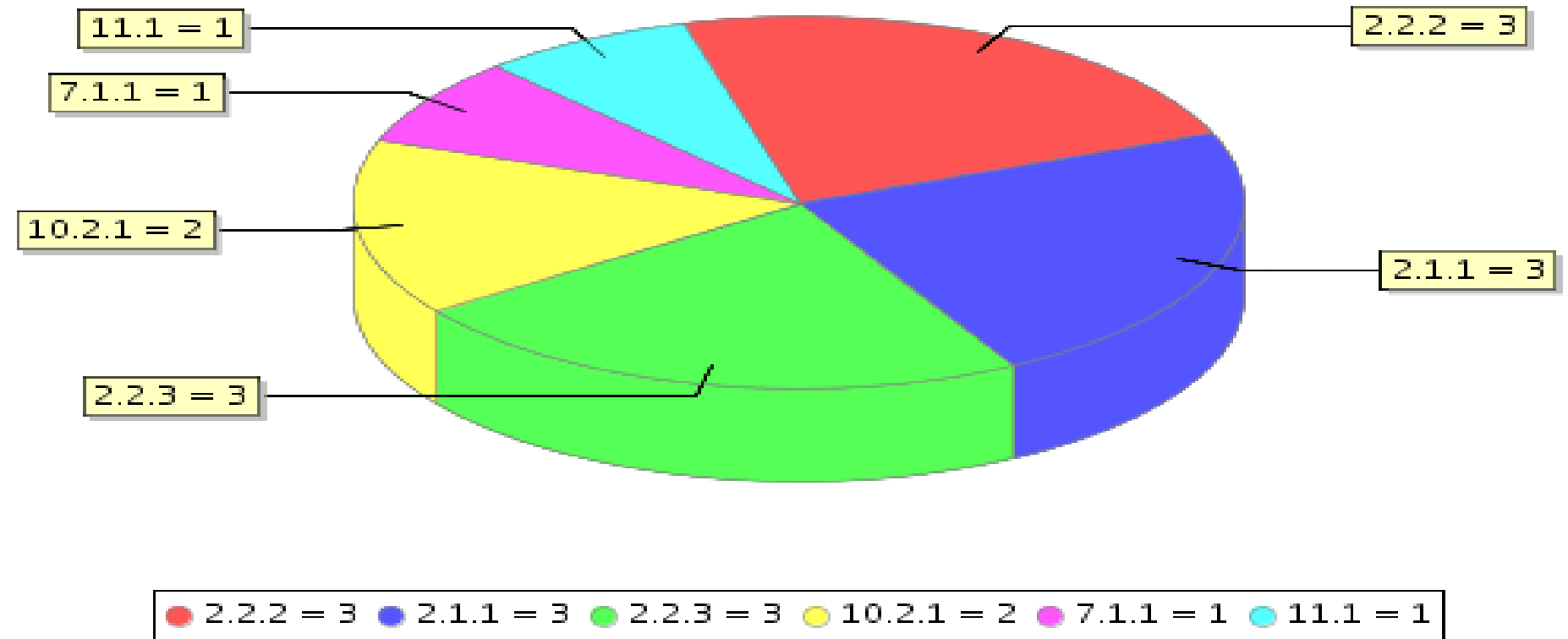
Report Launch Pad
Reports > Report Launch Pad

- Report Launch Pad
- Scheduled Run Results
- Saved Report Templates

- Autonomous AP
- CleanAir
- Client
- Compliance**
 - Configuration Audit
 - PCI DSS Detailed
 - PCI DSS Summary
- Device
- Guest
- MSE Analytics
- Mesh
- Network Summary
- Performance
- Raw NetFlow
- Security


Number of Devices Violated By PCI DSS Requirement






of Devices Violated By PCI DSS Requirement



Quick Launch-point for Smart Interactions

Device 360° Views


3945-East-1.cisco.com
10.0.104.1
NY Branch
up for 2 days 8 hrs 31 mins 24 secs
OS Type IOS
OS Version 15.1(4)M1
Last Config Change August 14, 2012 3:22:17 PM PDT
Last Inventory Collection August 21, 2012 3:02:16 AM PDT

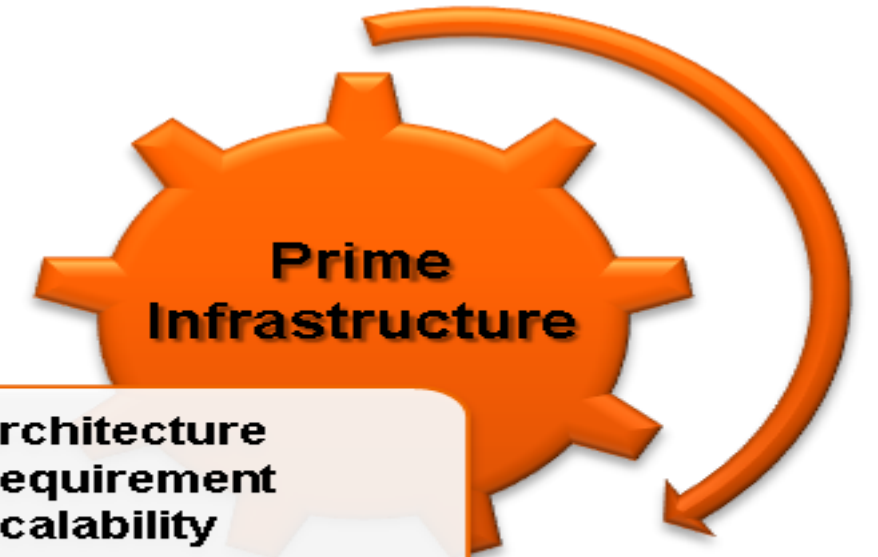






Cisco 3945E Integrated Services Router G2

Smart Interactions like Support Forums and TAC Service Request Creation can be accessed in just one click from any Device 360° popup

Alarms	Modules	Interfaces	Neighbors	
Device Name	Index	Port	Duplex	Sysname
7206-Core-2	1	GigabitEthernet0/2	fullduplex	Not Available
NY-2911-RBR	2	GigabitEthernet0/0	halfduplex	Not Available
DEN-2911-RBR	3	GigabitEthernet0/0	fullduplex	Not Available
AMS-2921-RBR	4	GigabitEthernet0/0	fullduplex	Not Available

Product Characteristics



- **Architecture**
- **Requirement**
- **Scalability**
- **Performance**
- **Supported Devices**
- **Deployment**



Product Deployment Considerations

■ Virtual Appliance

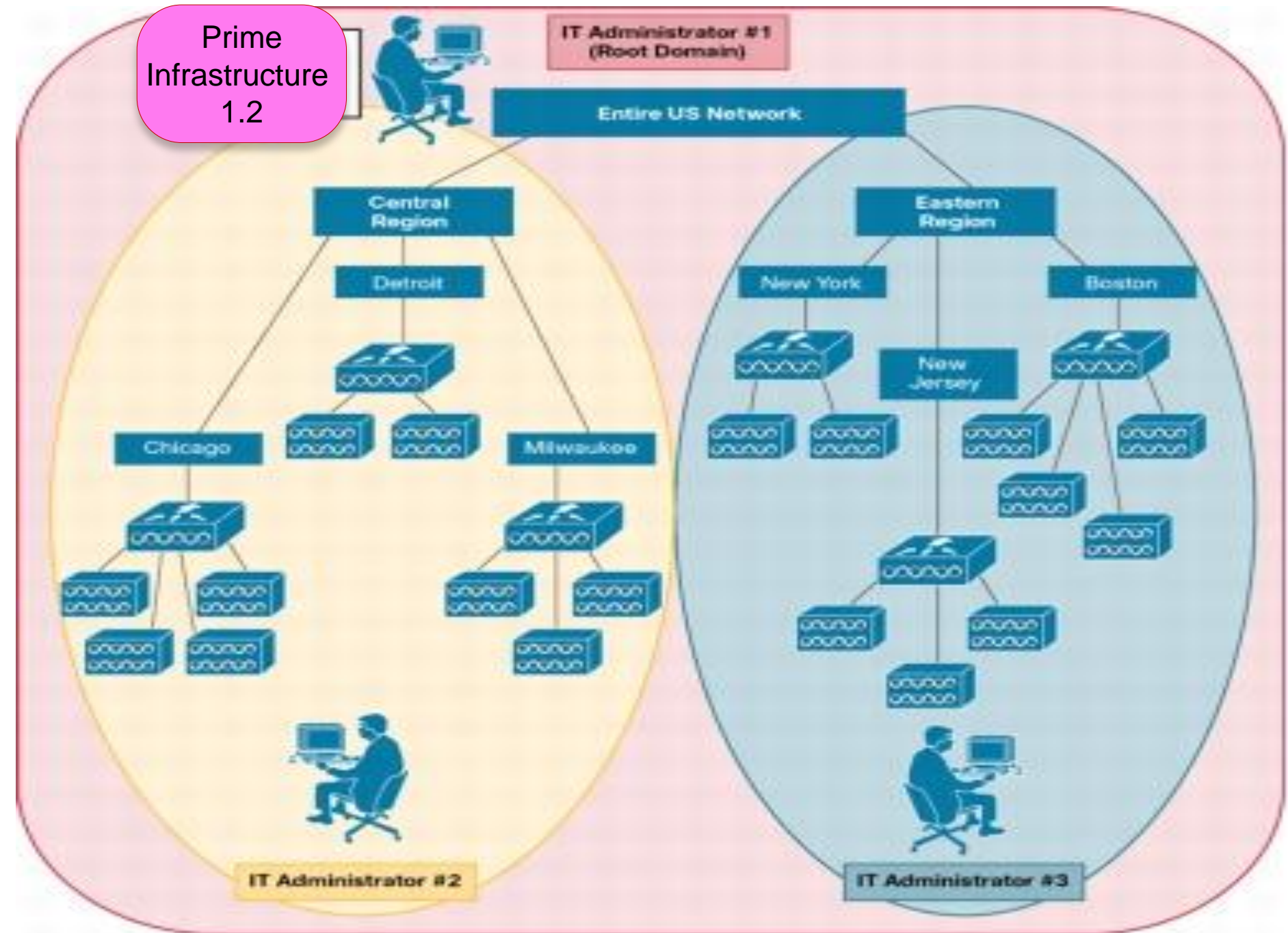
- Virtual Appliances are supported on ESXi 4.1 and 5.0 with VMFS 3.1 and 5.0 resp.
- There are block size requirements if using ESX 4.x. They don't apply to ESX 5.0 and higher.
- UCS B-Series with external storage is recommended way to deploy Prime Infrastructure

■ Physical Appliance

- Prime Infrastructure Appliance comes pre-installed with Prime Infrastructure 1.2
- Deploying Cisco Prime NCS Virtual Appliance on CiscoWorks Wireless LAN Solution Engine (WLSE) models 1130-19 or 1133 is not supported.
- Physical Appliances are field upgradable

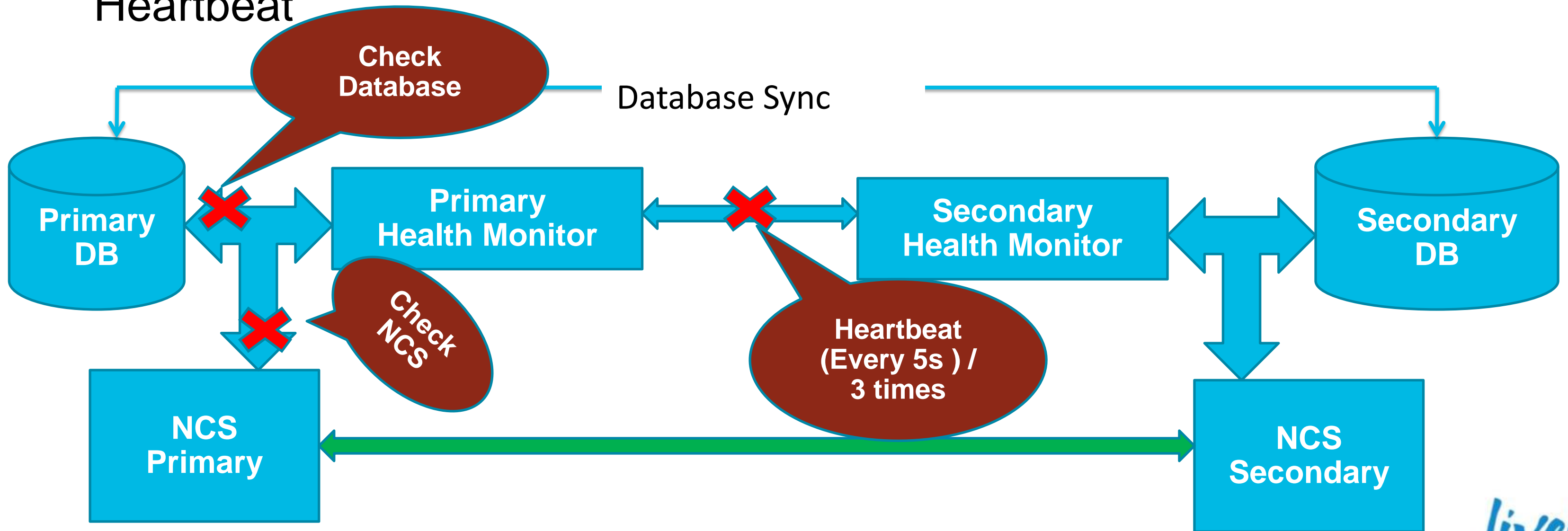
Virtual Domains – Multi-domain Management

- Virtual domains allows to control who has access to specific sites and devices
- Virtual domains can be based on physical sites, device types, user communities or any combinations
- By default one single Virtual domain exist called root-domain



High Availability Deployment

- PI supports High Availability in Active/Standby mode
- Failover can be automatic or manual
- Automatic failover is triggered by database check, Server check , Heartbeat



Product Requirement

Virtual Appliance Size	VMware ESX/ESXi	Processor	DRAM	Hard Disk
Small Virtual Appliance	Version 4.1 or 5.0	4 virtual CPUs (vCPUs)	8 GB	200 GB
Medium Virtual Appliance	Version 4.1 or 5.0	4 virtual CPUs (vCPUs)	12 GB	300 GB
Large Virtual Appliance	Version 5.0	16 virtual CPUs (vCPUs)	16 GB	400 GB
Extra Large Virtual Appliance	Version 5.0	16 virtual CPUs (vCPUs)	24 GB	1200 GB

- *Cisco UCS can be used as a virtual infrastructure deployment. i.e ESX/ESXi running on UCS should be okay if the VM requirements are met.*

Physical Appliance	Processor Speed	DRAM	Hard Disk
Prime Appliance	16 CPUs	16 GB	4 x 300 GB (RAID 5)

- *Physical Appliances are field upgradable*
- *Prime Infrastructure Appliance that comes pre-installed with Prime Infrastructure 1.2*
- *Deploying Cisco Prime NCS Virtual Appliance on CiscoWorks Wireless LAN Solution Engine (WLSE) models 1130-19 or 1133 is not supported.*

Prime Infrastructure Bundle Sizing Matrix

Bundle	Component	Small VA	Medium VA	Large VA	X-Large VA	Prime Appliance
Life Cycle	Devices	2500	6,000	11,000	18,000	11,000
Life Cycle	CPU Cores	4	4	16	16	16
Life Cycle	Memory (GB)	8	12	16	24	16
Life Cycle	HD Size (GB)	200	300	400	1,200	400
Life Cycle	LWAPs	3000	7,500	15,000	15,000	15,000
Life Cycle	Wired/Wireless Clients	10K/33K	20K/75K	50K/200K	50K/200K	50K/200K
Life Cycle	Events Per Second	100	300	300	1,000	300
Bundle	Component	Small VA	Medium VA	Large VA	X-Large VA	Prime Appliance
Assurance	Devices	NA	NA	5,000	18,000	5,000
Assurance	CPU Cores	NA	NA	16	16	16
Assurance	Memory (GB)	NA	NA	16	24	16
Assurance	HD Size (GB)	NA	NA	400	1,200	400
Assurance	Events Per Second	NA	NA	1000	1000	1000
Assurance	Flows Per Second	NA	NA	16,000	80,000	16,000
Assurance	NME-NAM polling	NA	NA	40	40	40
Assurance	NAM3 polling	NA	NA	40	40	40
Bundle	Component	Small VA	Medium VA	Large VA	X-Large VA	Prime Appliance
LC + Assurance	Devices	NA	NA	5,000	18,000	5,000
LC + Assurance	LWAPs	NA	NA	5,000	15,000	5,000
LC + Assurance	Wired/Wireless Clients	10K/33K	20K/75K	25K/75K	50K/200K	25K/75K
LC + Assurance	Memory (GB)	8	12	16	24	16
LC + Assurance	HD Size (GB)	200	300	400	1,200	400
LC + Assurance	Events Per Second	100	300	300	1,000	300
LC + Assurance	Flows Per Second	NA	NA	16,000	80,000	16,000
LC + Assurance	NME-NAM polling	NA	NA	40	40	40
LC + Assurance	NAM3 polling	NA	NA	40	40	40

Device Scalability

Managed Device Category	Device Type	Max. Count (18,000)
Wireless Infrastructure Devices	Controllers	1200
	Autonomous APs	5,000
	Lightweight Aps	15000 (40K transient clients per 5 min)
	MSE's	25
Wired Infrastructure Devices	Routers/Switches	12,000
	NME-NAMs	2,000
	NAM-1	400
	NAM-2	100
	NAM 2204 Appliance	50
	NAM 2220 Appliance	40

Device Scalability

Managed Device Category	Device Type	Max. Count (18,000)
Wireless Infrastructure Devices	Controllers	1200
	Autonomous APs Lightweight Aps	5,000 15000 (40K transient clients per 5 min)
	MSE's	25
Wired Infrastructure Devices	Routers/Switches	12,000
	NME-NAMs	2,000
	NAM-1	400
	NAM-2	100
	NAM 2204 Appliance	50
	NAM 2220 Appliance	40

- **Similar scalability exists for 3rd party APs/Controllers**
- **Up to 18,000 devices can be mix-n-matched from the table with their own limits above.**

End-Point and Flow Scalability

Managed Device Category	Device Type	Max. Count
Clients	Wired	50,000
	Wireless	200,000
Polling	Device	5 Min.
	Interface	5 Min.
Events	Events per second	1,000
Assurance Flows (Netflow)	Simultaneous NAM Polling per Collector	40
	Flows per second with distribution (Beta only)	80,000
	Netflow interfaces	20,000
Users	Concurrent UI operators	10
Scripts	Northbound API Scripts	25

Supported Devices – Wired

Device Types	Device Families
Cisco® Integrated Services Routers (ISRs)	8x0 Series, 1800 and 1900 Series, 2800 and 2900 Series, 3800 and 3900 Series
Cisco Aggregation Services Routers (ASR)	1000 Series
Cisco Catalyst® Switches	2900, 2975, 3750, 3560, 4500, 4900, and 6500 Series
Cisco® Network Analysis Module (NAM)	Catalyst 6500 Series Analysis Module-1, Module-2, Module-3, NAM2204 Series Appliances
Cisco Wide Area Application Services (WAAS)	WAE-512, WAE-522, WAE-612, WAE-674, WAE-7341
Data Centre Devices	Nexus 1K, 2K, 3K, 4K, 5K, 7K Series, Cisco MDS 9000 Series Multilayer Fabric Switches, Cisco MDS 9000 Series Multilayer Switches, UCS 5108 and UCS 6140XP

Supported Devices – Wireless

Device Types	Device Families
Cisco Mobility Service Engine (MSE)	2700 Series Wireless Location Appliance 3300 Series
Cisco Wireless Controllers (WLC)	2100, 2500, 4400, 5500 Series, Flex 7500 Series, Catalyst 3750G Series Integrated WLC, Catalyst 6500 Series (WiSM,WiSM2), WLC Module on SRE, WLC Module (WLCM and WLCM-E) for ISR, Wireless Controller on Service Ready Engine (WLCM2 on SRE)
Cisco® Lightweight Access Points (LWAP)	600 Series, 1040, 1524, 1552, 3500i, 3500e, 3600i, 3600e, 801A_, 802A_
Cisco Autonomous Access Points (AAP)	1130AP, 1200AP, 1240AP, 1250AP, 1260AP, 1141AP, 1142AP, 1800 and 800 ISR Series, Aironet 1310 and 1410 Bridges
Other Device Types	ME2400, ME3400E, ME3600, ME3800, R7200, R7300, R7400, R7500, R7600/S, CBS, IE/Rockwell

Integration



PI - ISE Integration

- PI leverages ISE API for posture assessment and report generation
- client-level view: security details
- Ability to troubleshoot client connectivity issues

PI + ISE: Client Posture and Profiling

ISE determines client to be Microsoft Workstation based on device fingerprinting

Client **00:06:1b:dd:8c:aa**
Refreshed 2012-Feb-09, 14:33:51 PST Note: None

Client Attributes

General

User Name **lysander**
IP Address **172.20.224.217**
MAC Address **00:06:1b:dd:8c:aa**
Vendor **Notebook**
Endpoint Type **Microsoft-Workstation**
Media Type **Wired**
Hostname **Data Not Available**
CDP Device ID **Data Not Available**
Software Version **Data Not Available**
Model **Data Not Available**
UDI **Data Not Available**

Session

Switch Name **ncs-demo_switch**
Switch IP Address **172.20.224.54**
Interface **GigabitEthernet1/0/13**
Wired Speed **100Mbps**
VLAN ID **50**
VLAN Name **VLAN0050**
Status **Associated**
On Network **Yes**

Traffic

Last Accounting Time **2012-Apr-14, 08:36:03 PDT**
Packets Tx/Rx **22937357/213454**
Bytes Tx/Rx **2030648253/27884661**

Security

Authenticating ISE **wnbu-ise1**
Authentication Method **802.1X**
Auth Status **Authorization Succeeded**
Authorization Profile Name **PermitAccess**
Posture Status **Not Applicable**
TrustSec Security Group **Data Not Available**
Audit Session ID **AC14E036000043CACC726FE7**
Windows AD Domain **cisco.com**
EAP Type **PEAP**

Client authenticated using 802.1x via ISE

Client session history

Session History

Association Time	Duration	User Name	IP Address	IP Address...	Switch Name	Interface	VLAN ID	Traffic (MB)
2012-Feb-09, 14:33:51 PST	64 days 17 hrs 2 min 41 sec	lysander	172.20.224.217	IPv4	ncs-demo_switch	GigabitEthernet1/0/13	50	1,963.0

Client Visibility – PI and ISE Integration

Client 00:26:b0:94:1b:6c (Refreshed :2012-Dec-20, 15:19:12 PST)

Client Attributes

General

User Name **jfields** ⊕
IP Address **192.168.152.44**
MAC Address **00:26:b0:94:1b:6c**
Vendor **Apple**
Endpoint Type **Apple-Device**
Client Type **Regular**
Media Type **Lightweight**
Mobility Status **Local**
Hostname **Data Not Available**
E2E **Not Supported**
802.11u Capable **No**
Power Save **ON**
CCX **Not Supported**

Device Identity Details via
ISE Integration

Session

Controller Name **AMS-2504-WLC**
AP Name **NMTG-AP3500-2**
AP IP Address **192.168.152.14**
AP Type **Cisco AP**
AP Base Radio MAC **04:c5:a4:f2:3f:60**
Anchor Controller **Data Not Available**
802.11 State **Associated**
Association ID **2**
Port **1**
Interface **vlan 13**
SSID **AMS-DOT1X**
Profile Name **AMS-dot1x**
Protocol **802.11g**
VLAN ID **13**
AP Mode **local**
Data Switching **Unknown**
Authentication **Unknown**

Device Session Details

Security

Security Policy Type **WPA2**
EAP Type **PEAP**
On Network **Yes**
802.11 Authentication **Open System**
Encryption Cipher **CCMP (AES)**
SNMP NAC State **Access**
Radius NAC State **RUN**
AAA Override ACL Name **none**
AAA Override ACL Applied Status **N/A**
Redirect URL **none**
ACL Name **none**
ACL Applied Status **N/A**
FlexConnect Local Authentication **No**
Policy Manager State **RUN**
Authenticating ISE **eset-ise-1**
Authorization Profile Name **Default-Corporate-Policy**
Posture Status **Not Applicable**
TrustSec Security Group **Data Not Available**
Windows AD Domain **eset.cisco.com**

Security policy + Windows
AD domain

Client Troubleshooting: Wireless Client

Client Troubleshooting [Go back](#)

▼ Properties

General

User Name **CISCO\janaraya** ⓘ
IP Address **0.0.0.0**
MAC Address **00:21:6a:91:9b:88**
Vendor **Intel**
Endpoint Type **Unknown**
Client Type **Regular**
Media Type **Lightweight**
Mobility Role **Unassociated**
Hostname **Data Not Available**
E2E **V1**

Session

Controller Name **SJC 14 LWAPP1**
AP Name **SJC14-12B-AP6**
AP IP Address **171.71.123.16**
AP Type **Cisco AP**
AP Base Radio MAC **58:bc:27:12:e0:10**
Anchor Address **Data Not Available**
802.11 State **Associated**
Association ID **50**
Port **1**
Interface **corp1**
SSID **blizzard**
Profile Name **blizzard**
Protocol **802.11n(5GHz)**

Security

Security Policy Type **WPA2**
EAP Type **EAP-FAST**
On Network **No**
802.11 Authentication **Open System**
Encryption Cipher **CCMP (AES)**
SNMP NAC State **Access**
Radius NAC State **8021X_REQD**
AAA Override ACL Name **none**
AAA Override ACL Applied Status **N/A**
Redirect URL **none**
ACL Name **none**
ACL Applied Status **N/A**
H-REAP Local Authentication **No**
Policy Manager State **8021X_REQD**
Authenticating ISE **Data Not Available**
Authorization Profile Name **Data Not Available**
Posture Status **Unknown**
TrustSec Security Group **Data Not Available**
Windows AD Domain **Data Not Available**

Status of client connectivity

Troubleshoot

✔ 802.11 Association ⚠ 802.1X Authentication ? IP Address Assignment ? Successful Association

Problem
802.1X Authentication Failure

Recommendation
Check whether Radius server(s) is reachable
Check whether client's choice of EAP method is supported by radius server
Check Clients username/password/cert is valid
Check to see if the certificates used by the Authentication server are accepted by the client.

Client Status: Wired

Clients and Users

Client **00:19:56:28:3c:b5** (Refreshed :2012-Nov-14, 18:25:23 PST)



Client Attributes

General

User Name **Unknown**
IP Address **10.15.11.109**
MAC Address **00:19:56:28:3c:b5**
Vendor **Cisco**
Endpoint Type **Cisco-IP-Phone-7961**
Media Type **Wired**
Hostname **Data Not Available**
CDP Device ID **SEP001956283CB5**
Software Version **SCCP41.8-0-1-0S**
Model **Data Not Available**
UDI **Data Not Available**

Session

Switch Name **FL4-3750S-1**
Switch IP Address **10.15.10.1**
Interface **FastEthernet2/0/4**
Wired Speed **100Mbps**
VLAN ID **11**
VLAN Name **Campus_Phns**
Status **Disassociated**
On Network **No**

Client Attributes
– clients details
including
endpoint type
and software
version

Session History



Association Time	Duration	User Name	IP Address	IP Address...	Switch Name	Interface	VLAN ID	Traffic (MB)
2012-Nov-14, 18:25:23 PST	27 days 22 hrs 27 min 40 sec	Unknown	10.15.11.109	IPv4	FL4-3750S-1	FastEthernet2/0/4	11	0.0
2012-Nov-13, 16:08:43 PST	1 days 2 hrs 10 min 13 sec	Unknown	10.15.11.109	IPv4	FL4-3750S-1	FastEthernet2/0/4	11	0.0

Wired Client Troubleshooting

Properties

General

User Name	Jane
IP Address	0.0.0.0
MAC Address	00:24:e8:e7:7c:87
Vendor	Dell
Device Type	Data Not Available
Media Type	Wired
Hostname	Data Not Available
Posture Status	Unknown
Serial Number	Data Not Available
Software Version	Data Not Available

Session

Device	CoreSwitch.wlan.local
Switch	
Port / Interface Name	GigabitEthernet1/0/40
Wired Speed	10Mbps
VLAN ID	10
VLAN Name	Management

Traffic

No statistics information available for this client.

Security

Authorization Policy	
Auth Status	Running
Audit Session ID	AC14E20100000066174E128:
Security Policy Status	No
Security Policy	802.1X
EAP Type	Unknown
State	Disassociated

Troubleshoot

Link Connectivity ✓ 802.1x Authentication ✓ Authorization ✓ IP Connectivity ⚠

Problem

Client could not complete DHCP

Recommendation

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

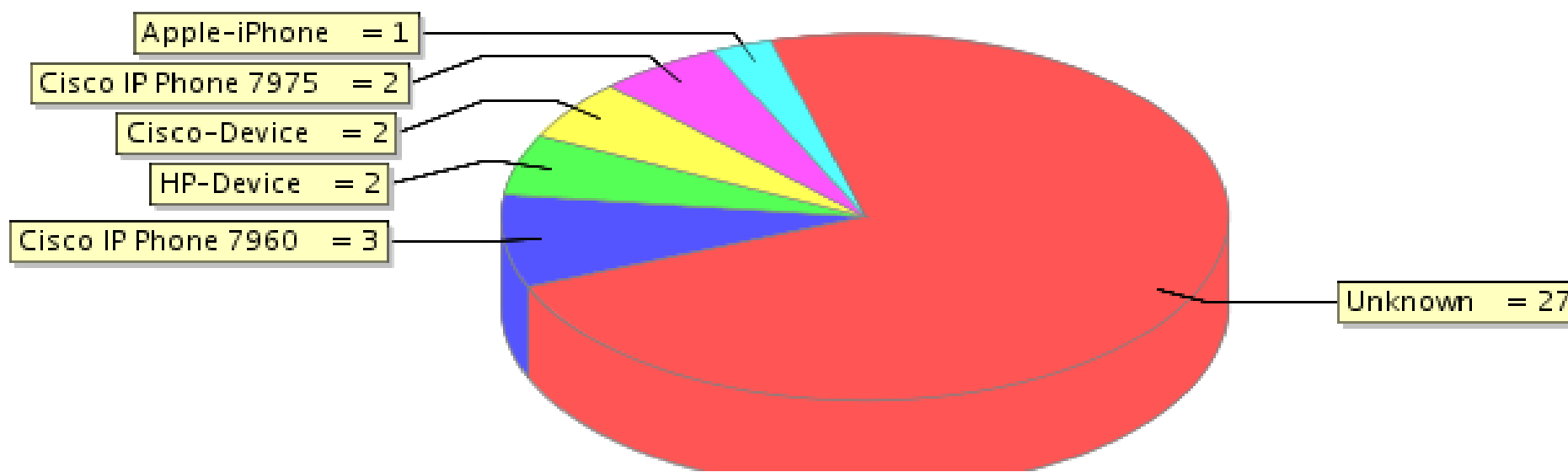
802.1x Status: Authc Success
Client don't have IP Address
Session State is : Authz Success

Client status with recommended troubleshooting steps

Client Summary Report - Endpoint Type

Endpoint Type	Number of Sessions	Number of Clients	Session Time (Hours)	Traffic (MB)	% of Sessions	% of Clients	% of Session Time	% of Traffic
Unknown	29	27	3.0	5107.8	74.36	72.97	74.07	66.98
Cisco IP Phone 7960	3	3	0.05	861.3	7.69	8.11	1.23	11.29
HP-Device	2	2	0.45	1647.05	5.13	5.41	11.11	21.6
Cisco-Device	2	2	0.38	9.72	5.13	5.41	9.47	0.13
Cisco IP Phone 7975	2	2	0.0	0.0	5.13	5.41	0.0	0.0
Apple-iPhone	1	1	0.17	0.0	2.56	2.7	4.12	0.0

Clients by Endpoint Type



ISE Reports in PI

ISE reports cross-launched from within PI (single sign-on)

Report Launch Pad	
Reports > Report Launch Pad	
Autonomous AP	
Autonomous AP Cpu/Memory Utilization ⓘ	New
Autonomous AP Summary ⓘ	New
Autonomous AP Tx Power and Channel ⓘ	New
Autonomous AP Up Time ⓘ	New
Autonomous AP Utilization ⓘ	New
Busiest Autonomous APs ⓘ	New
CleanAir	
Air Quality vs Time ⓘ	New
Security Risk Interferers ⓘ	New
Worst Air Quality APs ⓘ	New
Worst Interferers ⓘ	New
Client	
Busiest Clients ⓘ	New
Client Count ⓘ	New
Client Sessions ⓘ	New
Client Summary ⓘ	New
Client Traffic ⓘ	New
Client Traffic Stream Metrics ⓘ	New
Posture Status Count ⓘ	New
Guest	
Guest Accounts Status ⓘ	New
Guest Association ⓘ	New
Guest Count ⓘ	New
Guest User Sessions ⓘ	New
WCS Guest Operations ⓘ	New
Identity Service Engine (open in a new window)	
Endpoint Authentication Summary ⓘ	New
Endpoint Profiler Summary ⓘ	New
Posture Detail Assessment ⓘ	New
Top N Endpoint Authentications ⓘ	New
Top N User Authentications ⓘ	New
User Authentication Summary ⓘ	New
Mesh	
Alternate Parent ⓘ	New
Link Stats ⓘ	New
Nodes ⓘ	New
Packet Stats ⓘ	New
Stranded APs ⓘ	New
Worst Node Hops ⓘ	New

PI + ISE Reports

Subset of ISE reports cross-launched from within PI (single sign-on).

Identity Service Engine (open in a new window)

- Endpoint Authentication Summary
- Endpoint Profiler Summary
- Posture Detail Assessment
- Top N Endpoint Authentications
- Top N User Authentications
- User A

Endpoint > Query and Run > Top N Authentications By Endpoint Calling Station ID

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Endpoint > Top 10 Authentications By Endpoint Calling Station ID

Date : April 11, 2012

Generated on April 11, 2012 2:35:39 PM PDT

[Reload](#)

Calling Station ID	Pass	Fail	Total	Fail %	Status
00:06:1B:DD:8C:AA	3	0	3	0.00	<div style="width: 100%; height: 10px; background-color: green;"></div>

Integration with Mobility Service Engine (MSE)

MSE supports a suite of mobility services programs.

- **Context-Aware Services:** capture detailed contextual information about such things as location, temperature, availability, and applications used
 - **Context Aware Engine for Clients:** The Cisco location engine (RSSI) is used to track Wi-Fi clients, rogue clients, rogue APs, and wired clients.
 - **Context Aware Engine for Tags:** The AeroScout location engine (both RSSI and TDOA) is used to track Wi-Fi active RFID tag.
- **Adaptive Wireless Intrusion Prevention System (wIPS):** wIPS software provides visibility and comprehensive threat prevention for the mobility network through monitoring, alerts, classifying, and remediation of wireless and wired network vulnerabilities.

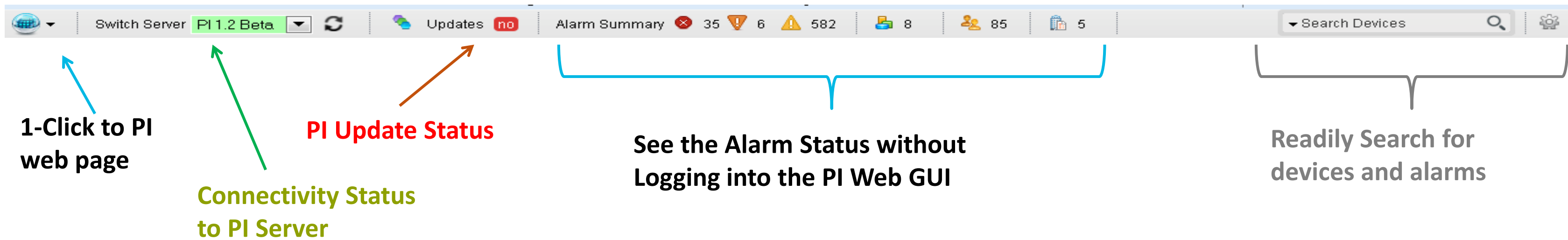
Additional Resources



Additional Resources

- ❑ **Cisco Prime Infrastructure 1.2 Documentation**
<http://www.cisco.com/go/primeinfrastructure>
- ❑ **Ordering Guide, Release Notes**
http://www.cisco.com/en/US/prod/collateral/netmgts/ps6504/ps6528/ps12239/guide_c07-714720.html
http://www.cisco.com/en/US/partner/docs/net_mgmt/prime/infrastructure/1.2/release/notes/cpi_rn.html
- ❑ **Evaluation / Demo : Software Download and License Registration**
<https://cisco.mediuscorp.com/market/networkers/productView.se.work?/nxt/rcrs/proieidentity/=19888>
<https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet?FormId=3999>
- ❑ **Quick Start Guide**
http://www.cisco.com/en/US/docs/net_mgmt/prime/infrastructure/1.2/quickstart/guide/cpi_qsg.pdf
- ❑ **Email**
ask-prime-infrastructure@cisco.com
- ❑ **Request license or re-host a license**
Email licensing@cisco.com
- ❑ **Cisco Prime Infrastructure iPhone App**
<http://appfinder.lissoft.com/app/cisco-prime.html>

Prime Infrastructure Toolbar

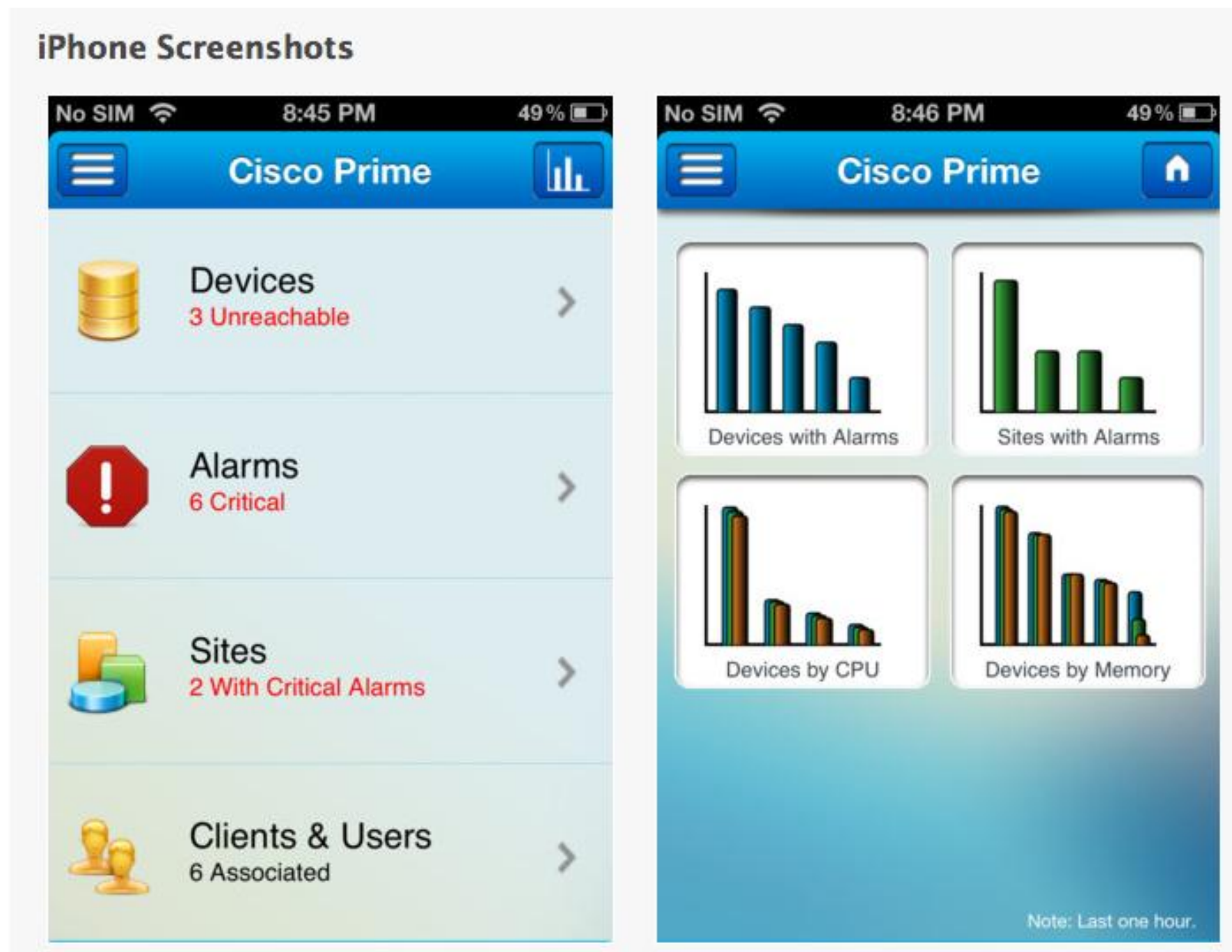


- At-a-glance, exception-based status – Devices unreachable, clients and sites with issues, active alarms
- Instant search for devices or alarms
- Contextual quick launch directly into Prime Infrastructure
- Live software update notifications – new device support, configuration templates, compliance rules, upgrades, etc.

iPhone App: Cisco Prime Infrastructure

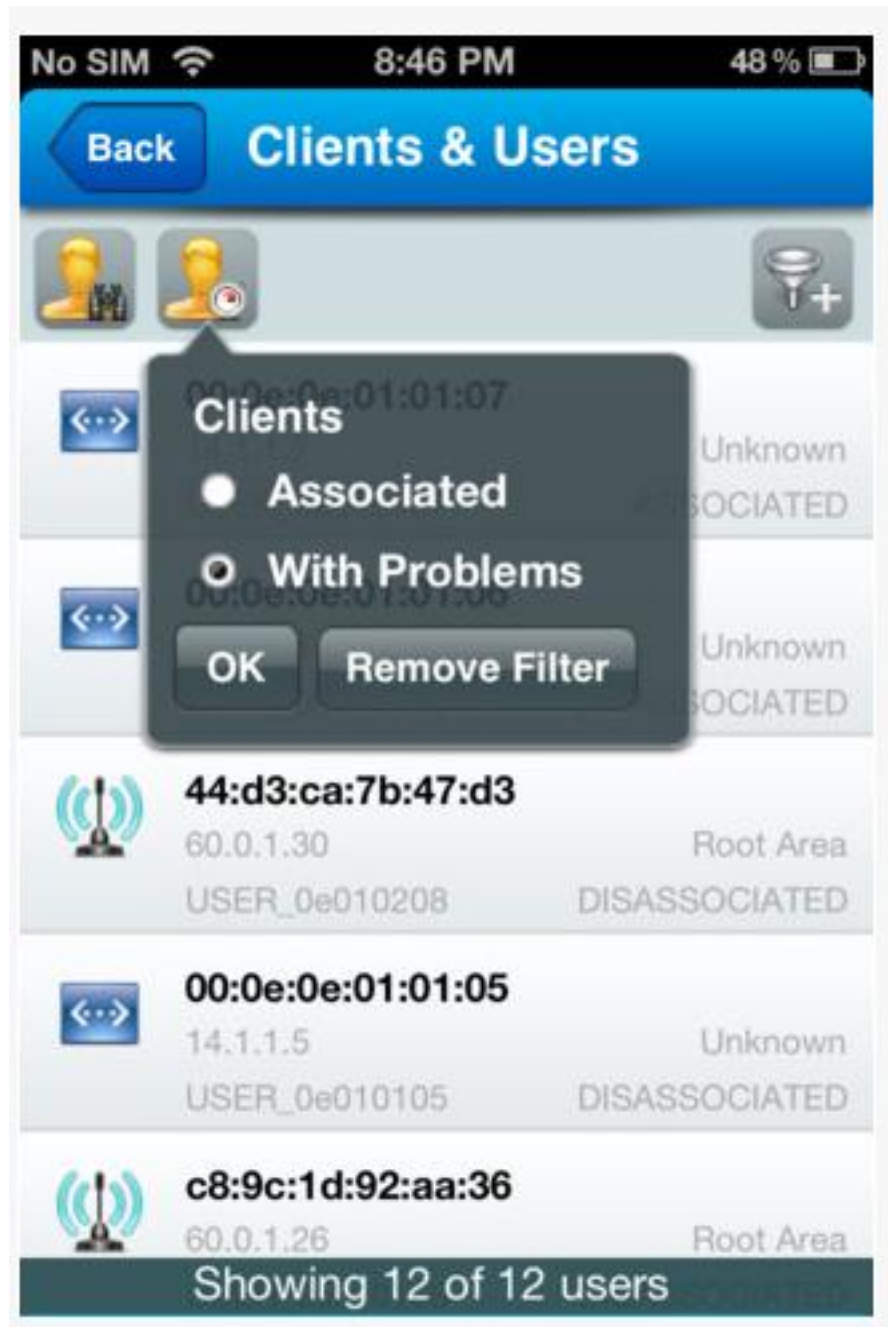


Cisco PI – iPhone App



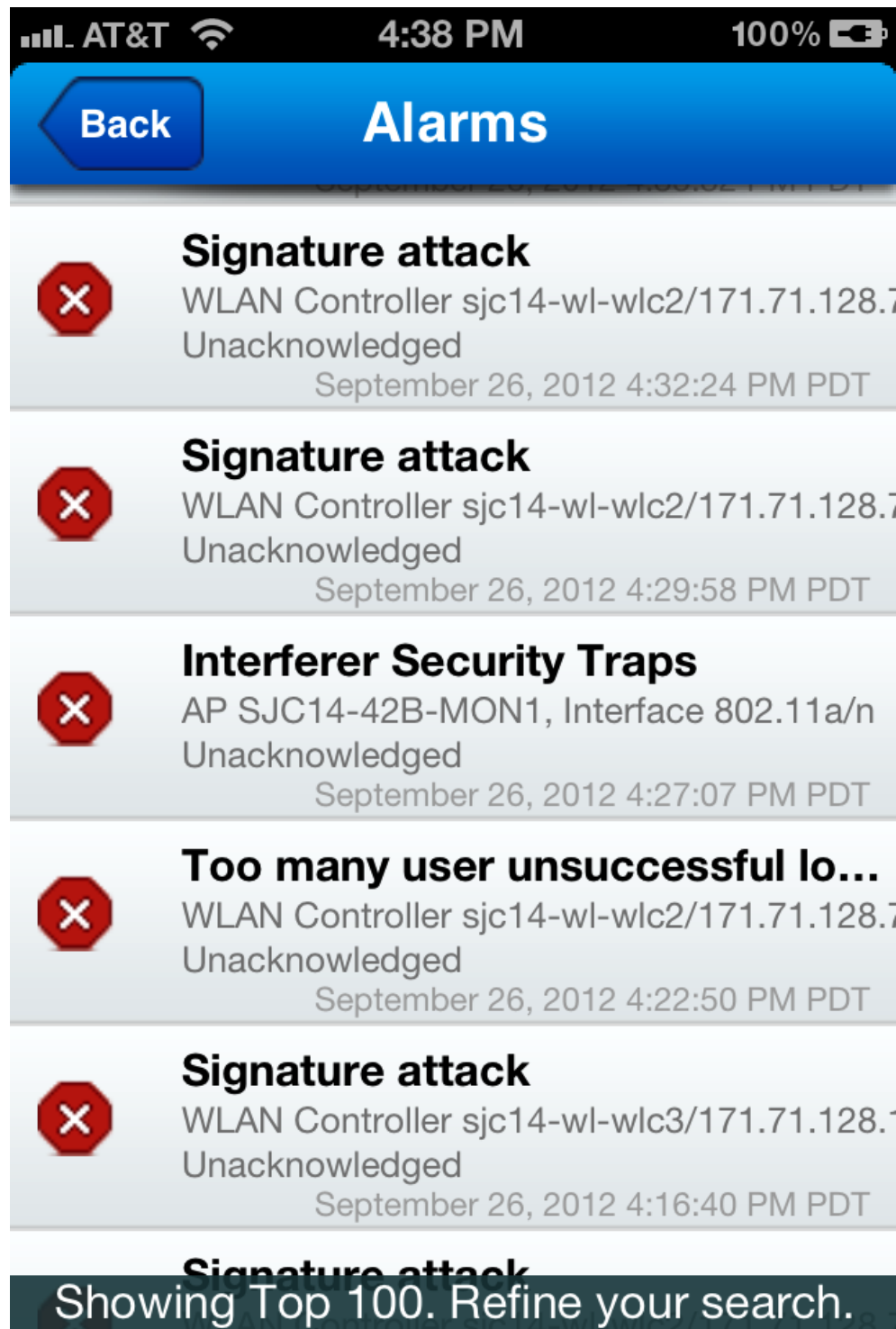
- Free application on Apple iTunes
- Provides network management summary
- Home screen displays top-level view including alarms

iPhone App



- Can view list of clients on the network
- Client list filtering capability

iPhone App – Alarm Information



- View alarm summary information in list format
- Filter based on user-defined criteria

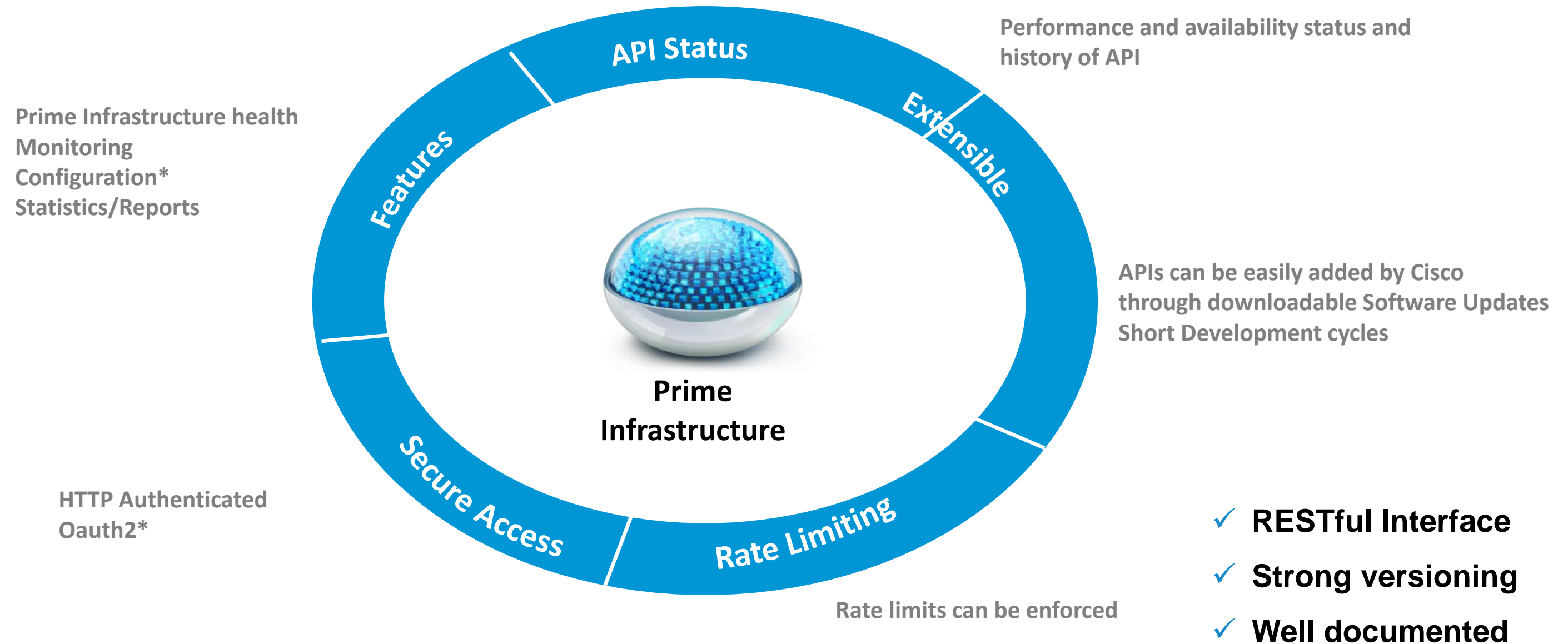
iPhone App – Device Summary



- List view of device inventory
- Device list filtering capability

Overview - Northbound API

Just point browser to “https://<pi-hostname>/webacs/api/v1” to get started.



* Not in Phase 1

Best Practices

- Database upgrade issues – There is a Field Notice for this:
<http://www.cisco.com/en/US/ts/fn/635/fn63595.html>

Q & A



Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2013 Polo Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site www.ciscoliveaustralia.com/mobile
- Visit any Cisco Live Internet Station located throughout the venue

Polo Shirts can be collected in the World of Solutions on Friday 8 March 12:00pm-2:00pm



Cisco *live!* 365

Don't forget to activate your Cisco Live 365 account for access to all session material,

communities, and on-demand and live activities throughout the year. Log into your Cisco Live portal and click the "Enter Cisco Live 365" button.

www.ciscoliveaustralia.com/portal/login.wv

Cisco *live!*

