

TOMORROW starts here.



Cisco *live!*

Managing an Enterprise WLAN with Cisco Prime Infrastructure

BRKEWN-2011

Brett Acton
Consulting Systems Engineer

Session Agenda

- Introducing Cisco Prime Infrastructure
- Installation and Initial Setup
- Planning and Deploying a Wireless Network
- Configuration Templates
- Maps
- Monitoring the Network
- Tools and Troubleshooting
- Reporting
- Advanced Topics

Session Objective

This session focuses on Cisco Prime Infrastructure (PI) as a deployment, management, and troubleshooting tool for Cisco Unified Wireless and wired (access) networks.

Attendees are required to have familiarity with basics of PI installation; topics covered in this session are, but not limited to: deployment options with PI (templates, auto-provisioning); operational insights, system dashboards, trends, alarms; drill-downs, cross-linked intuitive workflows to monitor client related information; enhanced reporting interface design and customisation abilities.

This session should be complemented with BRKEWN-2010 to get a complete overview of the advanced management and mobility services offered for a Cisco Wireless LAN.



Introducing Cisco Prime Infrastructure

Cisco Prime Infrastructure Overview

- Cisco Prime Infrastructure provides a single integrated solution for complete lifecycle management of Cisco routers, switches, and wireless devices, along with deep visibility into end-user experience and application performance
- Extends the functionality of Cisco WCS/NCS, provides complete lifecycle management of wired and wireless access networks
- Provides monitoring of endpoint security policy integration with Cisco Identity Services Engine (ISE)
- Upgrades/Migrations are available for existing customers of:
 - Prime Infrastructure 1.x [free upgrade to PI 2.0 with SASU contract]
 - Cisco Prime NCS 1.0 [free upgrade to PI 2.0 with SASU contract]
 - Cisco WCS*
 - CiscoWorks LMS 2.x/3.x
 - Cisco Prime LMS 4.x [free upgrade to PI 2.0 with SAS contract]
- Cisco Prime Infrastructure 2.0 also includes the software and licenses to use Cisco Prime LMS 4.2

* For data migration requires doing an intermediate upgrade to NCS 1.1

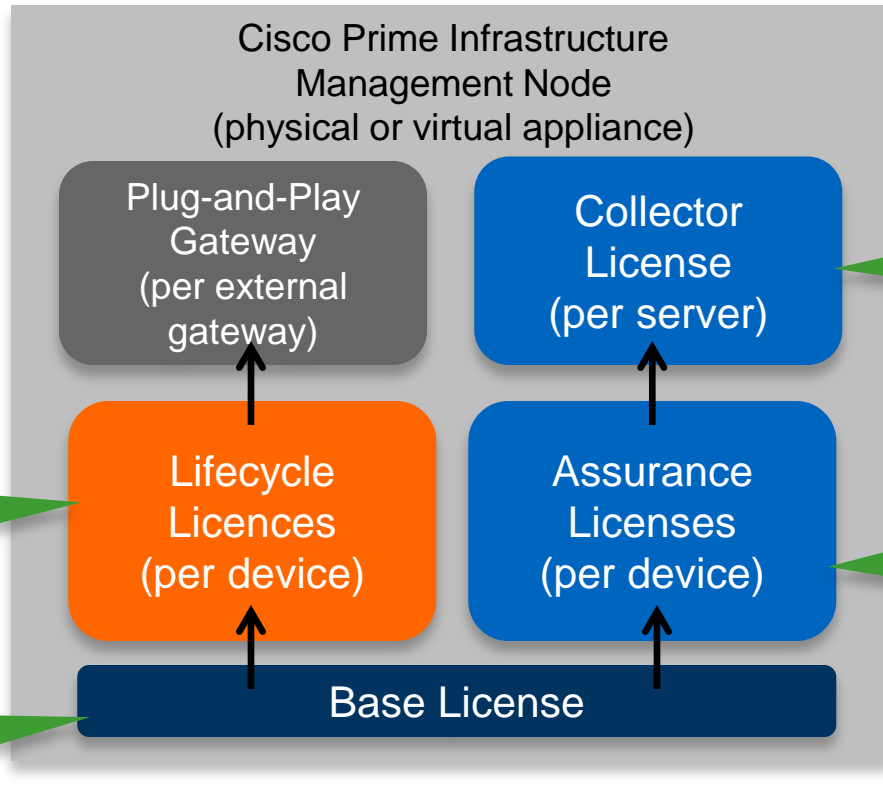
Device Name	Reachability	IP Address	Device Type	Collection Status	Collection Time	Software Version
IPM3550-1	Reachable	172.20.110.66	Cisco Catalyst 35	Managed	August 29, 2012	12.0(5)110P
IPM3550-1	Reachable	172.20.110.71	Cisco Catalyst 35	Managed	August 29, 2012	12.0(5)625
IPM3550-2-test	Unreachable	172.20.110.72	Cisco Catalyst 35	Managed with Warn	June 30, 2012	12.0(5)6E
IPM3550-E	Reachable	172.20.110.73	Cisco Catalyst 65	Managed	August 29, 2012	12.0(3)39302
IPM-CONTROLLER2	Reachable	171.69.217.69		Managed with Warn	August 29, 2012	7.0.114.33
IPM-CONTROLLER3	Reachable	171.69.217.71		Managed with Warn	August 29, 2012	7.0.114.33
IPM-Controller1	Reachable	171.69.217.65		Managed with Warn	August 29, 2012	7.0.94.157
IPM_2021_yourds	Reachable	171.69.217.76	Cisco 2021 Integ.	Managed with Warn	August 21, 2012	15.0(1)394

System	Summary
IP Address	172.20.110.71
Device Name	IPM-3550-1
Device Type	Cisco Catalyst 3550-24PS Switch
Up Time	7 days 7 hrs 28 mins 15 secs
System Time	2012-Aug-29, 19:53:46 UTC
Location	5th Fl, Room 10
Contact	Wade Test
Cisco Identity Capable	No

Cisco Prime Infrastructure 2.0

License Model Overview

Note: **Compliance Management** licenses are also sold as part of Prime Infrastructure 2.0, however, these licenses are used only with **Cisco Prime LMS 4.2**.



↑ Licence Dependency

Increases PI node from 20K to 80K flows per second

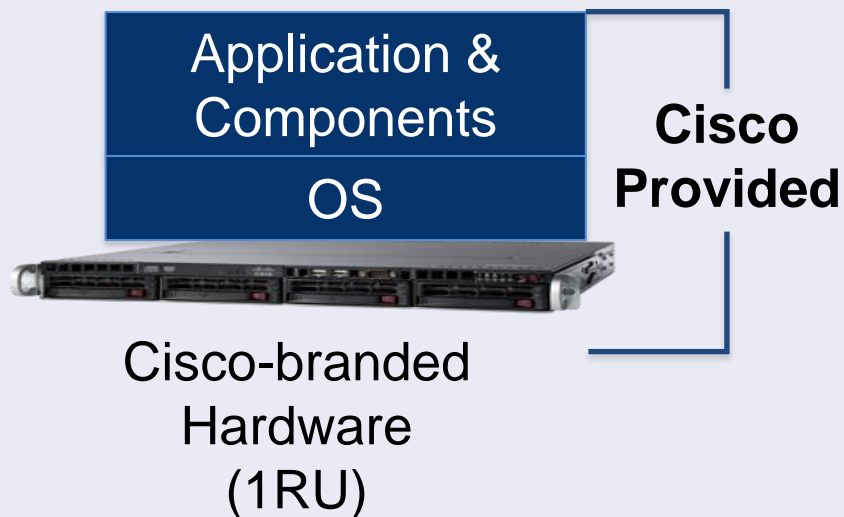
Available in incremental bundle sizes of 25, 50, 100, 500, 1K, 2.5K, 5K, 10K, and 15K Devices

Available in incremental bundle sizes of 25, 50, 100, 500, 1K, 2.5K, 5K, 10K, and 15K Devices

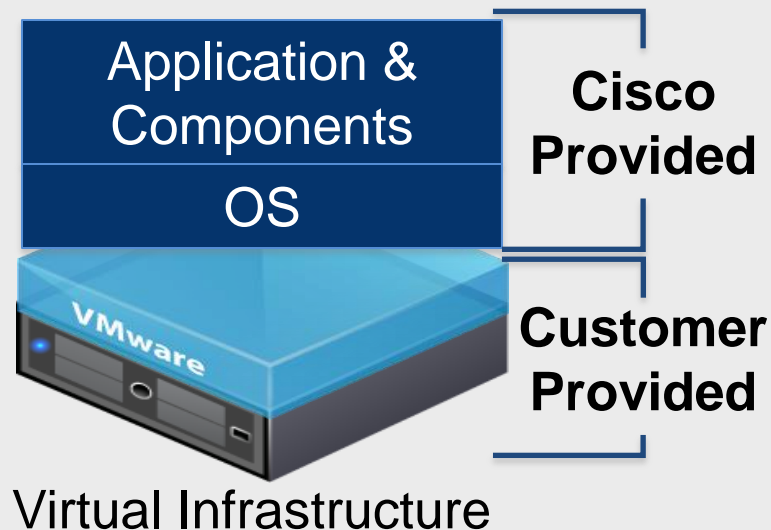
One Base license required for each management node (physical or virtual appliance)

Appliance Delivery Models

Physical Appliance



Virtual Appliance



Prime Infrastructure 2.0

Virtual OVA Server Requirement and Mapping

Virtual Appliance Size	Virtual CPU	Memory (DRAM)	HDD Size	Throughput (Disk I/O)	Concurrent Users (Max)	API Clients
Express	4	12 GB	300 GB	200 MBps	5	2
Custom Express*	8	16 GB	600 GB	200 MBps	10	2
Standard	16	16 GB	900 GB	200 MBps	25	5
Pro	16	24 GB	1200 GB	200 MBps	25	5

- Cisco UCS can be used as a virtual infrastructure deployment. i.e ESX/ESXi running on UCS

Mapping of Pre-2.0 to 2.x OVA/Bundle/SKU	
Pre-2.0	PI 2.0
WCS 7.x	Standard or Physical
Physical	Standard or Physical
Small	Express
Medium	Express or Custom Express
Large	Standard <=16K Netflow
Extra Large	Pro

** Important Field Notice **

If you are using a Small or Med OVA from PI 1.2/1.3 and have not significantly added more devices or turned on new features, you can migrate to the Express OVA. All their current numbers of scale with PI 1.2/1.3 will carry forward to PI 2.0

*Custom Express is not available as a separate OVA download. You will need to download the Express OVA and customise it for Custom Express

<https://supportforum.cisco.com/docs/DOC-37253>

Prime Infrastructure 2.0

Physical Appliance and Mapping

Physical Appliance	Physical CPU	Memory	HDD Size	Throughput (Disk I/O)	Web Clients	API Clients
Cisco Prime Appliance	2 CPUs 8 Cores (16 Threads)	32 GB	900 GB (4x300GB RAID5)	200 MBps	25	5

- In PI 2.0, the *PI Physical Appliance maps to the Standard OVA (for scalability purposes)*
- Physical Appliances are field upgradable
- Prime Infrastructure Appliance comes pre-installed with Prime Infrastructure 2.0
- Deploying Cisco Prime NCS Virtual Appliance on CiscoWorks Wireless LAN Solution Engine (WLSE) models 1130-19 or 1133 is **not** supported.

**** Important Field Notice ****

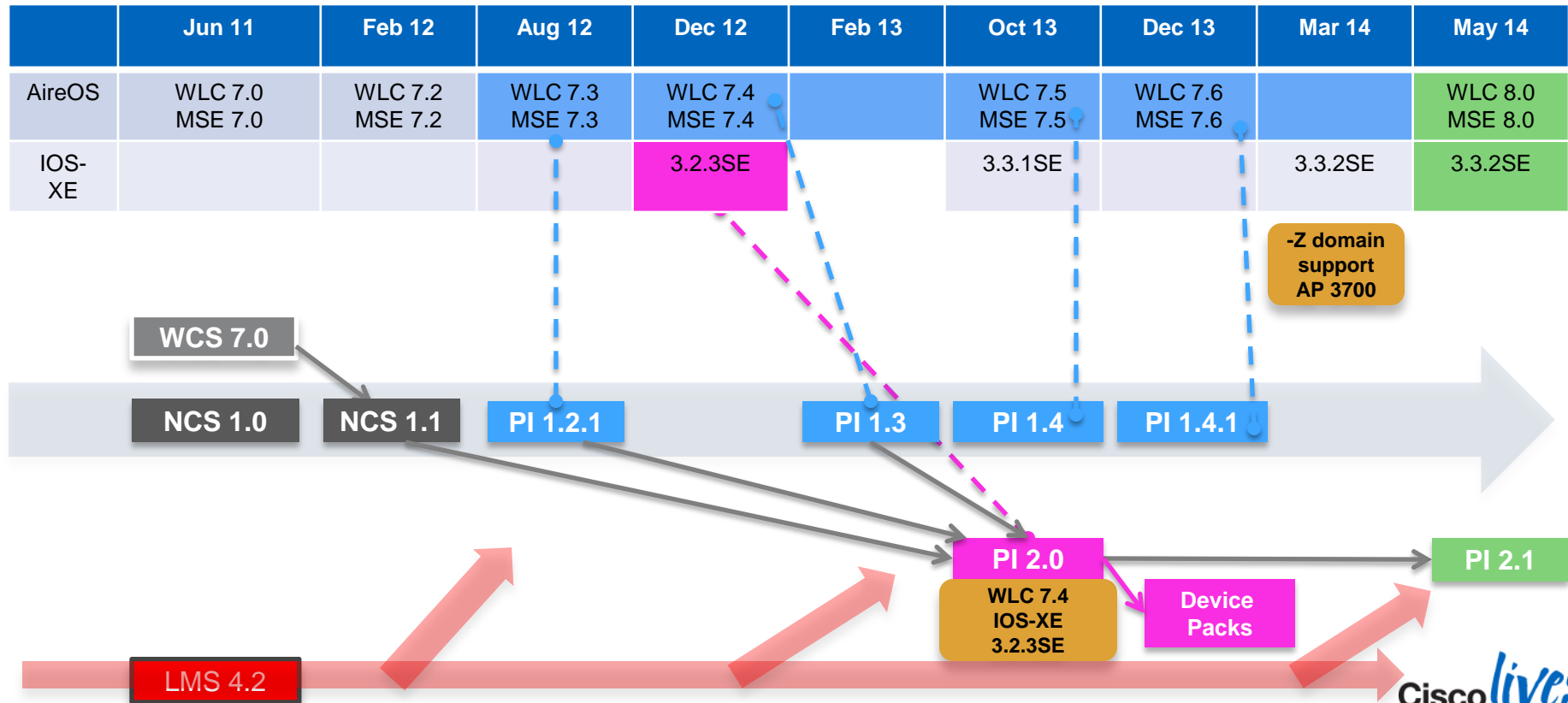
If you are using PI Physical Appliance with PI 1.2/1.3 and have not significantly added more devices or turned on new features, they can migrate to PI 2.0 with the same number of APs or devices.

Prime Infrastructure 2.0 Scalability

Parameter		Express	Custom Express	Standard	Pro
Devices	Max Unified AP	300	2,500	5,000	20,000
	Max. Autonomous AP	300	500	3,000	3,000
	Max. Wired	300	1,000	6,000	13,000
	NAMs	5	5	500	1,000
Clients	Wired Clients	6,000	50,000	50,000	50,000
	Wireless Clients	4,000	30,000	75,000	200,000
	Changing Clients	1,000	5,000	25,000	40,000
Monitoring	Events Sustained Rate (events/s)	100	100	300	1,000
	Netflow Rate (flows/s)	3,000	3,000	16,000	80,000
	Max. Interfaces	12,000	50,000	250,000	350,000
	Max. NAM Data Polled	5	5	20	40
System	Max. Number Sites/Campus	200	500	2,500	2,500
	Max. Groups	50	100	150	150
	Max. Virtual Domains	100	500	1,000	1,000

Cisco Prime Infrastructure

AireOS Controller Release and IOS Release Alignment



Software Upgrade Paths

From\To	WCS 7.0	NCS 1.0 (1.0.2.29)	NCS 1.1 (1.1.1.24)	PI 1.2.0 (1.2.0.103)	PI 1.2.1 (1.2.1.12)	PI 1.3 (1.3.0.20) PI-VA-1.3.0.20-size.ova	PI 1.4 PI-VA-1.4.0.45-size.ova	PI 1.4.1	PI 2.0 PI-VA-2.0.0.0.294-size.ova	PI 2.1	PI 2.2
WCS 7.0 (7.0.230.0)											
NCS 1.0 (1.0.2.29)					ncs_patch-1.0.2.29-upgrade-12						
NCS 1.1 (1.1.1.24)				ncs_patch-1.1.0.1114 ncs_patch-1.1.0.1116	ncs_1_1_1_24-Update.13.4	ncs_1_1_1_24-Update.13.4			ncs_1_1_1_24-Update.13.4		
PI 1.2.0 (1.2.0.103)					pi_1.2.1.12_update pi_1.2.1.12_patch_1	pi_1.2.1.12_update pi_1.2.1.12_patch_1 PI_1_2_1_12u-Update.1					
PI 1.2.1 (1.2.1.12)						PI_1_2_1_12-Update.1.0 PI_1_2_1_12u-Update.1			PI_1_2_1_12-Update.1.0		
PI 1.3 (1.3.0.20)									PI_1_3_0_20-Update.1.12		
PI 1.4								PI_1_4_0_45_Update_1-39			
PI 1.4.1											
PI 2.0									pi_dev_pack_update_2.0-13.ubf		
PI 2.1											



Installation and Initial Setup

Initial Setup

Setup script

- Guides network administration through set of questions for setting basic parameters
- Changes to set parameters can be made at a later time via CLI

Secondary server (High Availability) setup

- You will need to specify the Prime Infrastructure role (Primary or Secondary) during installation
- Server configured for Primary operation cannot be reconfigured for Secondary operation (or vice versa)
 - appliance needs to be re-installed and configured for Secondary operation
- Licensing based on (v)UDI (Unique Device Identifier) of Primary server

High-Availability - Components and Operation

- At the heart of the High-Availability design is the “Health Monitor” (HM) Process
- Health Monitor is sub-divided into the following sub-system:

Core HM - Configures, maintains state and starts/stops the HA configuration across Prime servers

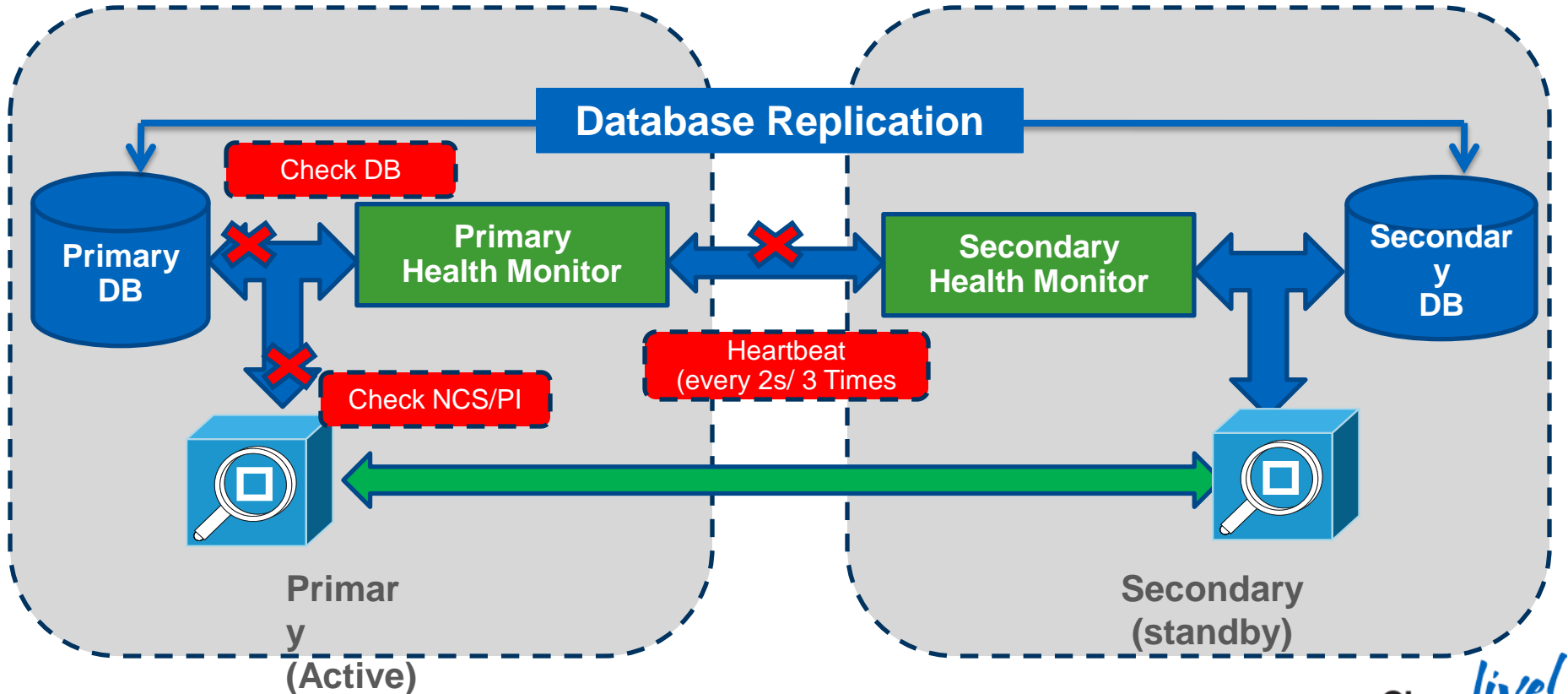
Heartbeat - Responsible for maintaining communication between the Primary and Secondary servers (over HTTPS, port 8082); timeout is set to 2s, with three re-tries

Application Monitor - Communicates with the Prime framework components on the primary server

DB Monitor - Configures database replication

File Sync - Identifies file changes, compression, and statistics maintenance

High-Availability - Components and Operation



Cisco Prime Infrastructure High Availability

- When an Primary Prime Server fails, the Secondary Prime Server takes over operations and continues to provide service.
- If the standby Prime doesn't receive 3 heartbeats (timeout 2 seconds) then either the Secondary Prime will become active (automatic failover) or email will be sent to network admin. (manual failover)
- **Failover** (Primary to Secondary) can be **Automatic** or **Manual**
- **Failback** (Secondary to Primary) is always **manual**

High-Availability - Things to Consider

- Both the Primary and Secondary Prime servers should run the same software version
- Both the Primary and Secondary Prime servers should be the same size
- Email server and receiver must be configured (used for notifications)
- For communication between the Primary and Secondary, HM port (8082) must be allowed through firewall if in the path between Primary and Secondary servers
- **Failover** mode must be carefully selected (and remembered): **Manual vs. Automatic**
- Authentication key is created during the install, and is used by the Primary and Secondary Prime servers for communication (and also logging into the HM web page)
- HM available at: <https://<ip.address>:HMport> (example: https://10.10.10.20:8082)

High Availability Setup

Cisco Prime Infrastructure Virtual Domain ROOT-DOMAIN | prime

Home Design Deploy Operate Report Administration Workflows

System Settings | **High Availability**

- HA Status
- HA Configuration**

HA Configuration

Administration > System Settings > High Availability > HA Configuration

Configuration

Configuration Mode **HA Not Configured**

General

Secondary Server ?

Authentication Key ?

Email Address ?

Failover Type ?

- Admin Dashboard
- Logging
- Users, Roles & AAA
- Virtual Domains
- User Preferences
- Software Update
- Import Policy Update
- Jobs Dashboard
- Jobs Approval
- Health Rules
- System Settings
 - Data Sources
 - Appliance
 - Background Tasks
 - High Availability
 - System Audit
- Licenses
 - Assurance License Manager



Planning and Deployment

Prime Infrastructure System Planning

- Consideration of the initial layout of the management system is key and can make daily operations such as configuration changes, reporting and templates easier to administer
- Placing controllers and AP's in designated groups can make deployment changes or maintenances updates easier to manage and control
- Identifying RF or Security issues can be easier to locate and mitigate
- Increase in High Availability and reduction of critical network coverage response time

Populating Inventory

- Device Addition
 - Single addition
 - Bulk Add
 - Discovery
- Device Collection
 - Inventory
 - Configuration
- Device Monitoring
 - Performance
 - Fault



The screenshot shows a 'Discovery Settings' dialog box with the following sections:

- Discovery Settings**: *Name [text input]
- Protocol Settings**: PingSweep Module [button with plus icon]
- Layer 2 Protocols**: CDP Module [button with plus icon], LLDP Module [button with plus icon]
- Advanced Protocols**: Routing Table [button with plus icon], Address Resolution Protocol [button with plus icon], Border Gateway Protocol [button with plus icon], OSPF [button with plus icon]
- Filters**: IP Filter [button with plus icon]
- Advanced Filters**: System Location Filter [button with plus icon], System Object ID Filter [button with plus icon], DNS Filter [button with plus icon]

Buttons at the bottom: Save, Run Now, Cancel. A vertical scrollbar is on the right side.

Grouping

Device Work Center

Device Group > User Defined > East-Switches

East-Switches

Device Name	Reachability
SW-POD1-E	Reachable
SW-POD2-E	Reachable
SW-POD3-E	Reachable
SW-POD4-E	Reachable
SW-POD5-E	Reachable
SW-POD6-E	Reachable
SW-POD7-E	Reachable

Port Groups

Device IP	Name	Speed	Type
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	100 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	FastEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.1	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD
10.14.201.2	GigabitEthernet1/0/14	10 Mbps	Ethernet CSMA/CD

Sites

API-S-Building-0-1

API-S-Building-0-1

Virtual Domains

Prime Infrastructure

IT Administrator #1 (Robert Edwards)

IT Administrator #2

IT Administrator #3

Device Groups

- Predefined groups per device type
- Custom groups Static or dynamic
- For Configuration purpose

Port Groups

- Predefined groups per port type
- Custom groups static or dynamic
- For configuration or Monitoring purpose

Sites

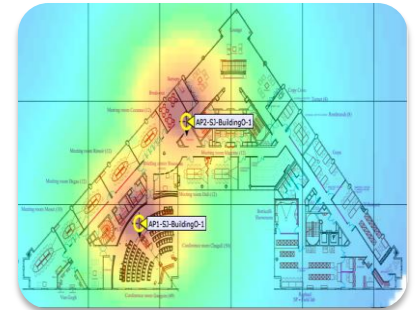
- Grouping per physical location
- Hierarchy campus/building/floor
- For Location services or Assurance

Virtual Domains

- Grouping of sites/Controllers/AP/wired devices
- For Role Based Access Control

Site Grouping

- **Sites** can be organised into a hierarchy of Campuses and Buildings
- **Sites** allows for Devices, Traffic, End-users and Alarms/Events to be organised based on the physical structure of the network
- Users of Prime Infrastructure can be assigned to manage specific groups of **Sites**, called **Virtual Domains** based on their responsibilities
- The Monitoring Dashboards allows all the data collected by Prime Infrastructure / Prime Assurance to be viewed based on **Sites**



Creating Site Groups

Design > Site Map Design (or Operate > Maps)

The screenshot displays the Cisco Prime Infrastructure interface for managing Site Maps. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The 'Operate' tab is active, showing the 'Maps' section. On the left, a 'Maps Tree View' shows a hierarchy starting with 'Root Area' and 'System Campus', followed by various branches like 'Amsterdam Branch', 'Boxborough Branch', etc. The main area shows a table of 'Site Maps' with columns for Name, Type, Incomplete, Total APs, a/n Radios, b/g/n Radios, Critical, and Status. A context menu is open over the table, listing actions such as 'New Campus/Site', 'New Building', 'Delete', 'Move Buildings', 'Copy Maps', 'Properties', 'Export Maps...', 'Import Maps...', 'RF Calibration Models', 'Location Presence', and 'Multi-Map Editor'. The status column shows green checkmarks for most items and yellow warning triangles for others.

Name	Type	Incomplete	Total APs	a/n Radios	b/g/n Radios	Critical	Status
System Campus	Campus/Site		0	0	0	0	✓
Unassigned	Campus/Site		0	0	0	0	✓
Amsterdam Branch	Campus/Site	1	1	1	0	0	⚠
Boxborough Branch	Campus/Site	0	0	0	0	0	✓
Dallas Branch	Campus/Site	0	0	0	0	0	✓
Denver Branch	Campus/Site	0	0	0	0	0	✓
India Branch	Campus/Site	0	0	0	0	0	✓
Japan Branch	Campus/Site	0	0	0	0	0	✓
London Branch	Campus/Site	0	0	0	0	0	✓
Los Angeles Branch	Campus/Site	0	0	0	0	0	✓
Management Apps	Campus/Site	0	0	0	0	0	✓
New York Branch	Campus/Site	0	0	0	0	0	✓
Paris Branch	Campus/Site	0	0	0	0	0	✓
RTP Branch	Campus/Site	0	0	0	0	0	✓
San Francisco Branch	Campus/Site	0	0	0	0	0	✓
San Jose Campus	Campus/Site	2	2	2	0	0	⚠
San Jose Data Center	Campus/Site	0	0	0	0	0	✓

Creating Site Groups from Device Work Centre

Cisco Prime Infrastructure | Virtual Domain ROOT-DOMAIN | prime | Search Menu/Prime Data

Home Design Deploy Operate Report Administration Workflows

Device Work Center | Discovery Configuration Archives Software Image Management Image Dashboard Plug and Play Status Network Audit

Device Group > ALL

ALL

Selected 0 | Total 83

Groups & Sites | Add Device | Bulk Import | Export Device

Availability	IP Address/DNS	Device Type	Admin Status	Inventory Collection Status	Last Successful Coll...	Software Type	Softw		
	10.0.252.4	Cisco Catalyst 3560E-24...	Managed	Completed	February 20, 2014 1...	IOS	12.2(5		
	10.0.252.3	Cisco 3750 Stackable S...	Managed	Completed	February 20, 2014 1...	IOS	12.2(3		
	192.168.152.1	Cisco 3945E Integrated ...	Managed	Completed	February 20, 2014 1...	IOS	15.1(4		
	10.0.103.1	Cisco 3945 Integrated S...	Managed	Completed	February 20, 2014 1...	IOS	15.1(4		
	10.0.255.42	Cisco 7206VXR Router	Managed	Completed	February 20, 2014 1...	IOS	12.2(1		
<input type="checkbox"/>	7206-Core-2	<input checked="" type="checkbox"/>	10.0.255.52	Cisco 7206VXR Router	Managed	Completed	February 20, 2014 1...	IOS	12.2(2
<input type="checkbox"/>	AMS-2921-RBR	<input checked="" type="checkbox"/>	192.168.152.2	Cisco 2921 Integrated S...	Managed	Completed	February 20, 2014 1...	IOS	15.2(4

Device Group > ALL

Site Groups

Name: Site Groups
 Description: Site Groups
 Type: Device
 Group Type: Static
 No. of Members: 77 Total (0 Direct, 77 Children)
 No. of SubGroups: 34 Total (22 Direct, 12 Children)

Actions
 + Add Site Group

Building View



Cisco Prime Infrastructure Virtual Domain ROOT-DOMAIN | prime ▾ Search Menu/Prime Data

Home Design ▾ Deploy ▾ Operate ▾ Report ▾ Administration ▾ Workflows ▾

Maps Tree View ▾

- Root Area
 - System Campus
 - Unassigned
 - Amsterdam Branch
 - Boxborough Branch
 - Dallas Branch
 - Denver Branch
 - East Sheen Branch
 - India Branch
 - Japan Branch
 - London Branch
 - Los Angeles Branch
 - Management Apps
 - New York Branch
 - Paris Branch
 - RTP Branch
 - San Francisco Branch
 - San Jose Campus
 - Building O
 - San Jose Data Center
 - Singapore Branch

Building View
Operate > Site Maps > San Jose Campus > Building O

Floor	Map	Details	
2		<ul style="list-style-type: none"> Floor Area 2 Floor Index 2 Contact Status ✔ a/n Clients 0 Wired Clients 0 	<ul style="list-style-type: none"> Total APs 0 a/n Radios 0 b/g/n Radios 0 Critical Radio Alarms 0 b/g/n Clients 0
1		<ul style="list-style-type: none"> Floor Area 1 Floor Index 1 Contact Status ⚠ a/n Clients 0 Wired Clients 0 	<ul style="list-style-type: none"> Total APs 2 a/n Radios 2 b/g/n Radios 2 Critical Radio Alarms 0 b/g/n Clients 0

✔ -- Select a command --

New Floor Area

Edit Building

Delete Building

Copy Building ...

Configure Interferer Notifications

Adding Devices to Sites and Groups

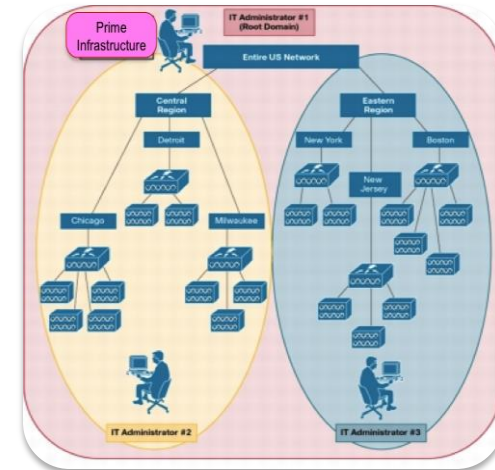
Operate > Device Work Centre > Groups & Sites

The screenshot displays the Cisco Prime Infrastructure Device Work Center interface. The main area shows a table of devices with columns for Device Name, Reachability, IP Address/DNS, Device Type, Admin Status, Inventory Collection Status, Last Successful Coll..., and Software Type. Three devices are selected, indicated by checked checkboxes in the first column. A red box highlights these three devices: 3560-DC-1, 3750-PHY-1, and 3945-East-1.cisco.com. An 'Add To Group' dialog box is open, showing a 'Select Group' dropdown menu. The dropdown menu is expanded, showing a list of site groups: Amsterdam Branch, Boxborough Branch, Dallas Branch, Denver Branch, India Branch, and Japan Branch. The 'Japan Branch' option is highlighted with a red box. The interface also shows a search bar, navigation tabs (Home, Design, Deploy, Operate, Report, Administration, Workflows), and a status bar at the bottom with workflow status, support cases, and alarm counts.

Device Name	Reachability	IP Address/DNS	Device Type	Admin Status	Inventory Collection Status	Last Successful Coll...	Software Type	Softwa
3560-DC-1	✓	10.0.252.4	Cisco Catalyst 3560E-24...	Managed	Completed	February 20, 2014 1...	IOS	12.2(5)
3750-PHY-1	✓	10.0.252.3	Cisco 3750 Stackable Sw...	Managed	Completed	February 20, 2014 1...	IOS	12.2(3)
3945-East-1.cisco.com	✓	192.168.152.1	Cisco 3945E Integrated	Managed	Completed	February 20, 2014 1...	IOS	15.1(4)
3945-West-1	✓	10.0.10...		Managed	Completed	February 20, 2014 1...	IOS	15.1(4)
7206-Core-1	✓	10.0.25...		Managed	Completed	February 20, 2014 1...	IOS	12.2(1)
7206-Core-2	✓	10.0.25...		Managed	Completed	February 20, 2014 1...	IOS	12.2(2)

Virtual Domains

- Virtual Domains allow controlled access to a specific set of devices and/or sites
- Used to provide administrative control. User can be added and assigned predefined static roles.
- Besides complete access, you can give administrative access with differentiated privileges to certain user groups
- A user can add new virtual domain by navigating to **Administration > Virtual Domains**
- To add users, navigate to **Administration > User Roles & AAA**.



Virtual Domains

■ Hierarchical Domains

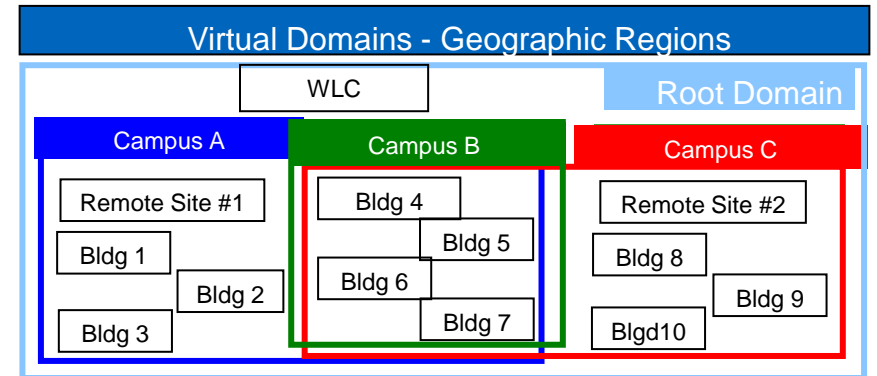
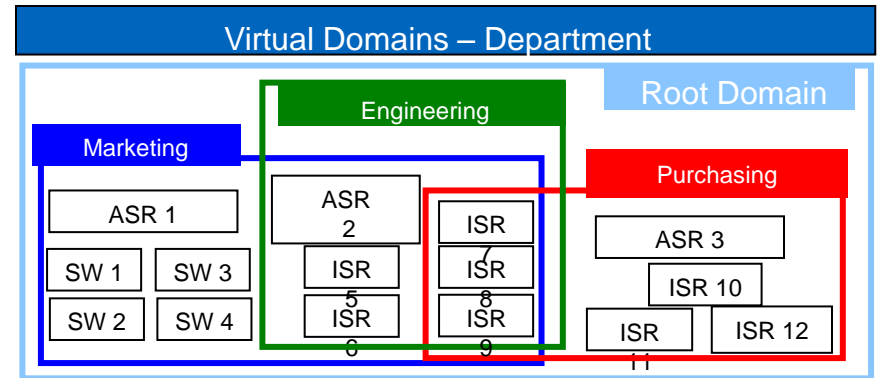
- Top (ROOT-DOMAIN) user has complete access to all domains
- Selected users have access to individual domains
- Standard Prime Infrastructure features for all domains

■ Distributed Device Deployment

- Dedicated Device per virtual domain
- Configuration and monitoring of Device allowed at individual domain level

■ Centralised Device Deployment

- e.g Shared Controller across multiple virtual domains
- Only monitoring views for particular domain; configuration of shared Controller at top most domain



Virtual Domains

What They Are (or do)	What They're Not (or don't do)
Quick way to partition PI objects	Not necessarily a complete replacement for RBAC (for example, via TACACS+)
Allows users to be mapped to separate virtual domains at the time of creation	If none specified, users are added to the “ROOT-DOMAIN” virtual domain by default
Separate Reports, Controllers, Access Points, Search, Templates, Config Groups, Alarms and other objects	Don't separate Google Earth Maps, Auto-Provisioning, MSEs, and Ethernet Switches
Objects may be assigned to multiple domains at the same time	Avoid changing configurations from multiple domains management simple
“ROOT-DOMAIN” domain is a superset of all sub-domains	Not all objects are available at the “root” level – objects such as Search and Reports are domain specific

Effects of Partitioning

	Effects of Partitioning
Reports	Only visible in current virtual domain. Cannot view reports from subvirtual domain
Search	Only includes components assigned to virtual domain.
Alarms	Only ROOT-DOMAIN can enable Location Notifications, Location Servers
Templates	Only available to Virtual Domain unless it is applied to Controller
Config Groups	Can be viewed/modified by Parent Domain
Maps	All Buildings in Campus, All Floors associated with Building, All Access Points associated with that floor. IF floor directly assigned you lose some map based features
Access Points	When controller or map assigned, the associated access points are assigned too. IF you assign Access Points directly lose some controller based features
Controllers	Recommendation to assign controller to only One Virtual Domain
Email	Can be configured per-Virtual Domain.

Virtual Domains vs. Roles

Network Partitioning

Provides the capability for PI to be segmented by network elements (controllers, AP's, switches, maps)

Partitioning Granularity

Alarms, reports, searches, applied templates, config groups are virtual domain aware.

User-Level Control

Granular control of user/admin privilege level (defined in PI and RADIUS/TACACS).

Virtual Domain – Setup

Virtual Domains

Virtual Domain Hierarchy
New Delete Import Export

Virtual Domains
Administration > Virtual Domains

Virtual Domains

Name: Live2014
Description: Live 2014 Example
Email Address: bacton@cisco.com (name@domain.com)
Time Zone: (GMT+10:0) Australia/Sydney

Add User
Administration > Users, Roles & AAA > Users > Add User

Summary Site Maps Controllers Access Points Wire

Available Site Maps
CISCO LISBOA
Dallas Branch
Denver Branch

Available Virtual Domains
DD-yyy
ROOT-DOMAIN
Sin-vd
canada-region
il-region
ny-region

Selected Virtual Domains
Live2014

Add >
< Remove

System Campus
System Campus > Oaklawn
System Campus > Oaklawn2
System Campus > Oaklawn2 > 1st floor
Unassigned

Define Virtual Domains

- Site Maps
- Controller
- Access Points

ces

Assign virtual domain to user to limit user-level visibility and control.

Virtual Domain – Roles: User Setup

Add User
Administration > Users, Roles & AAA > Users > Add User

General Virtual Domains

Username

New Password

Confirm Password

Groups Assigned to this User

- Admin
- Config Managers
- Lobby Ambassador
- Monitor Lite
- North Bound API
- Root
- Super Users
- System Monitoring
- User Assistant

User accounts provides granular level of user access.

Add User

Administration > Users, Roles & AAA > Users > Add User

General Virtual Domains

Available Virtual Domains	Selected Virtual Domains
DD-yyy ROOT-DOMAIN Sin-vd canada-region il-region ny-region	Live2014

Add >
< Remove

Assign virtual domain to user to limit user-level visibility and control.

RADIUS Custom Attributes
NCS:virt
NCS:virt
NCS:virt

TACACS+ Custom Attributes
virtual-domain0=ROOT-DOMAIN
virtual-domain1=floor 1 APs
virtual-domain2=11B-AP1



Cisco ACS



Cisco PI

Virtual Domain – Reports

Admin creates
report from
ROOT-DOMAIN



Cisco Prime Infrastructure



Users in all target
virtual domains
can see/execute
report

- Use case: admin at headquarters creates reports for virtual domains
- Reports created in parent domain can be pushed to child domain

Virtual Domain – Network Elements

ROOT-DOMAIN user
sees all network
elements



Cisco Prime Infrastructure

User manages devices
in virtual domain that
are assigned to their
username



- Use case: admin responsible for subset of network, i.e. devices in their domain
- Full control (super user) for all devices in their domain (config + monitoring)
- User should not have visibility into rest of the network



Configuration - Templates

Device Configuration with Templates

Feature Based

- Router (Security, Routing, AVC) and Wireless
- Intelligent template
- Understand current device configuration

Template Detail

Template Information

IKE Authentication: Authentication Type
Encryption Policy: Encryption Policy

Topology and Routing Information

Select Topology: Device Role
 Create dynamic connection between spokes
 Spoke
 Hub

NHRP and Tunnel Parameters

*Network ID: [text field]
*Hold Time: 300 (secs)
*NHRP Authentication String: [text field]
*Tunnel Key: [text field] (Bytes)
*IP MTU: 1400 (Bytes)
TCP Maximum Segment Size: 1360 (Bytes)
Tunnel Source Interface: [text field]

NHS Information

Cluster Support
*IP Address of Hub's tunnel interface: [text field]
*IP Address of Hub's physical interface: [text field]

Save as New Template Cancel

CLI Based

- Pre-defined (System)
- User defined
- Parameters and more with Apache VTL scripting

Configuration Templates

Templates

- Networks and Technologies
- CLI Templates
- Composite Templates
- Networks
- OCRS
- Hostnames
- TACACS

Template Basic

*Name: IP Phone DHCP Pool
Description: [text field]

Validation Criteria

*Device Type: Routers

Template Detail

CLI Content: **hostname**
excluded-address 10.8Branch_ID.11.1 10.8Branch_ID.11.10
excl-include-address 10.8Branch_ID.11.40 10.8Branch_ID.11.254
ip dhcp pool 10-Phones
network 10.8Branch_ID.11.0 255.255.255.0
default-router 10.8Branch_ID.11.254
option 150 ip Call_Manager

CLI Content dialog:
Enter the Branch ID: *
Call Manager: * 192.168.128.201
Save as New Template Cancel

Composite

Template of
CLI Templates

Management

Routing

Security

QoS

Configuration Group

Devices

Composite
Template

Feature Based Template Deployment Modes

Configuration in Device Work Centre

- Per device configuration
- Understand current device configuration
- Allows Add/Edit/delete
- All configuration options are not always available (AVC)
- Very simple
- Very fast
- No job Created
- Immediate deployment

The screenshot displays the Cisco Prime Infrastructure Device Work Centre interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The main content area is titled 'Device Work Centre' and shows a list of devices under the 'ALL' group. The 'Feature Configuration' section is expanded, showing 'AVC Interfaces' with a table of interface configurations. The table has columns for 'Template Name', 'Input Reports', and 'Output Reports'. The 'GigabitEthernet0' interface is selected, and its configuration is shown below the table.

Device Name	Reachability	IP Address/DNS	Device Type	Software Version
3560-DC-1	✓	10.0.252.4	Cisco Catalyst 3560E-24...	12.2(52)SE
3750-PHY-1	✓	10.0.252.3	Cisco 3750 Stackable S...	12.2(35)SE5
3945-East-1.cisco.c...	✓	192.168.152.1	Cisco 3945E Integrated ...	15.1(4)M1
3945-West-1	✓	10.0.103.1	Cisco 3945 Integrated S...	15.1(4)M1
7206-Core-1	✓	10.0.255.42	Cisco 7206VXR Router	12.2(15)T

Template Name	Input Reports	Output Reports	Tr...
IPv4 + IPv6 Default Policy			
2 <input type="checkbox"/> FastEthernet1			
3 <input type="checkbox"/> FastEthernet2			
4 <input type="checkbox"/> FastEthernet3			
5 <input type="checkbox"/> FastEthernet4			
6 <input type="checkbox"/> FastEthernet5			
7 <input type="checkbox"/> FastEthernet6			
8 <input type="checkbox"/> FastEthernet7			
9 <input type="checkbox"/> FastEthernet8			
10 <input checked="" type="checkbox"/> GigabitEthernet0			

GigabitEthernet0/1 10.0.104.1 UP UP ### Connection to NY Branch Gig0/0 ###

Feature Based Template Deployment Modes

Design/Deploy Lifecycle

Design > (Configuration) Feature Design

- Works for deployment on multiple devices
- Allows full customisation of the template (design)
- Deployment job
- Immediate or scheduled

The screenshot displays the Cisco Prime Infrastructure web interface. The breadcrumb navigation shows: Templates > Features and Technologies > Application Visibility > AVC Configuration. The main content area is titled "AVC Configuration" and contains several sections:

- Template Basic:** Includes fields for *Name, Description, and Tags. The Author is set to "prime" and the Feature Category is "AVC Configuration".
- Validation Criteria:** The *Device Type is set to "Routers".
- Template Detail:** The *Apply to Interface Role is set to "Any".
- Traffic Statistics:** Includes a toggle for "On/Off", "IPs, Subnets" set to "Any IPv4", and "Applications" set to "ANY".
- HTTP URL Visibility:** Includes a toggle for "On/Off", "IPs, Subnets" set to "Any IPv4", and a list of applications including "Flash Yahoo", "Flash Video", "Gmail", "Flash Myspace", and "RealMedia Traffic".

A tooltip is visible over the "Device Type" dropdown, stating: "Device Type can be either a **Product Family** (example: Routers or Switches and Hubs or Wireless Controller) or a **Product Series** within a Family (example: Routers > Cisco 1000 Series Routers) or a particular **Product Type** within a Product Series (example: Routers > Cisco 1000 Series Routers > Cisco 1000 Router)".

The interface also shows a left-hand navigation tree with categories like "Features and Technologies", "Application Visibility", "Controller", "Interfaces", "Network Analysis Module", "Security", "TrustSec", "VPN Components", "Zone Based Firewall", "ACL", "DMVPN", "Easy VPN Remote", "Easy VPN Server Proxy Setting", "Easy VPN Server", "GET VPN Group Member", "GET VPN Key Server", "ScanSafe", and "WAN Optimization".

At the bottom, there is a "Workflow Status" bar with various icons and a "Support Cases" section showing "Alarm Browser" and "Alarm Summary" with counts (199, 2, 187).

Templates: Discovery From Wireless Controller

- Templates are added to PI database when a WLC is first added to PI
- Template names can be changed to more meaningful names after discovery
- Additional configuration changes on the WLC may be pulled in to PI via the “Discover templates from controller” option

The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The main content area is titled 'Device Work Center' and shows a 'Wireless Controller' device group. A table lists discovered devices with columns for Device Name, Reachability, IP Address/DNS, Device Type, Software Version, AP Count, and Client Count. The device 'BXB-3850-1' is selected, and a context menu is open with options like 'Discover Templates from Controller' and 'Templates Applied to Controller'. Below the table, the 'Device Details' section shows a 'Summary' for the selected device, including its IP address (10.5.10.2) and device name (BXB-3850-1). A physical device image is also shown.

Device Name	Reachability	IP Address/DNS	Device Type	Software Vers...	AP Count	Client C...
AMS-5760-WL...	✓	192.168.152.11	Cisco 5760 Wir...	03.02.02.SE	1	0
✓ BXB-3850-1	✓	10.5.10.2	Cisco Catalyst ...	03.02.02.SE	1	0
LON-2504-WLC	✓	10.11.13.1	Cisco 2504 Wir...	7.4.100.0	2	0
PAR-3850-1	✓	10.12.10.2	Cisco Catalyst ...	03.02.02.SE	0	0
SI-WISM2-1	✓	192.168.136.49	Cisco WISM2 C...	7.4.121.0	1	0
WLC-4400-1	✓	192.168.136.48	Cisco 4404 Wir...	6.0.182.0	0	0

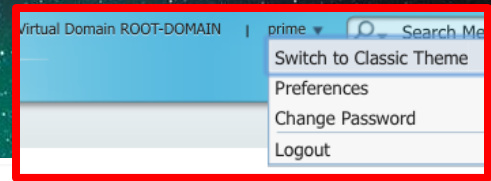
Summary
10.5.10.2 > System > Summary

General
IP Address/DNS Name: 10.5.10.2
Device Name: BXB-3850-1

Unique Device Identifier (UDI)
Name: Switch 1
Description: WS-C3850-48P

Controller Template LaunchPad

Classic Theme



System
General
SNMP Community
Network Time Protocol
User Roles
AP Username Password
AP 802.1X Supplicant Cr...
Global CDP Configuration
DHCP
Dynamic Interface
Interface Groups
QoS Profiles
AP Timers
Traffic Stream Metrics QoS
WLANs
FlexConnect
Security
802.11
802.11a/n
802.11b/g/n
Mesh
Management
CLI
Location
IPv6

Controller Template Launch Pad

Configure > Controller Template Launch Pad

System
General (i) New
SNMP Community (i) New
Network Time Protocol (i) New
User Roles (i) New
AP Username Password (i) New
AP 802.1X Supplicant Credentials (i) New
Global CDP Configuration (i) New
DHCP (i) New
Dynamic Interface (i) New
Interface Groups (i) New
QoS Profiles (i) New
AP Timers (i) New
Traffic Stream Metrics QoS (i) New
WLANs
WLAN Configuration (i) New
AP Group VLANs (i) New
FlexConnect
FlexConnect AP Groups (i) New
Security
General (i) New
File Encryption (i) New
RADIUS Auth Servers (i) New

802.11a/n
Parameters (i) New
Media Parameters (i) New
EDCA Parameters (i) New
Roaming Parameters (i) New
802.11h (i) New
High Throughput (802.11n) (i) New
CleanAir (i) New
802.11b/g/n
Parameters (i) New
Media Parameters (i) New
EDCA Parameters (i) New
Roaming Parameters (i) New
High Throughput(802.11n) (i) New
CleanAir (i) New
Mesh
Mesh Settings (i) New
Management
New
New
New
New
New

All-in-one, high-level view of template categories in PI which may be expanded or collapsed for easier navigation and viewing

Create or modify a template for configuring 802.11b/g/n parameters (such as power and channel status, data rates, channel list, and CCX location measurement) and applying those settings to multiple controllers.

Each template provides a callout icon which, on mouse-over, provides easy to understand description of what the template is and how it may be used to configure certain attribute(s).

Tree-based hierarchy continues to exist as left-hand navigation

CLI Based Templates

- Many Pre-Defined Systems Templates (e.g Flexible Netflow, Medianet, Performance Monitor, 802.1x ...)
- User [skilled] defined CLI based templates
- It's possible to create NEW templates for specific needs or to adapt existing templates (Duplicate)
- Template language is VTL (Apache) see <http://velocity.apache.org/>
- Operator then uses the template forms to **Deploy** configuration

The screenshot displays the Cisco Prime Infrastructure web interface. The main navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The current page is titled 'Configure SNMP' under the 'System Templates - CLI' category. A left-hand pane lists various templates, with 'Configure SNMP' selected. The main content area shows the configuration form for the 'Configure SNMP' template, including fields for Name, Description, Tags, Validation Criteria (Device Type, OS Version), and Template Detail (CLI Content). A modal window titled 'Configure SNMP' is open, displaying the following details:

Description	Configures SNMP
Type	CLI Template
Feature Category	CLI
Feature Path	CLITemplate
IOS Image	N/A
Last Updated	2013-Aug-01 14:07:36 PDT
Publish Status	No
Contact	root

Below the details, an 'Actions' section provides options: Edit, Delete, Duplicate, Move to Folder, and Publish. The 'Duplicate' action is highlighted with a red dashed box. The bottom of the interface shows 'CISCO PUBLIC' and a 'live!' logo.

CLI Template Scripting

- Templates have validation criteria on hardware and software
- Simple Parameter Types: String, Integer, IPv4
- New Parameter Types: Drop-Down, Check-Box, Radio-Box, Multi-Line
- Database Variables
- Scripting Capabilities: Conditional Statement, Foreach Loop
- Interactive and Enable Mode



Composite Template

The screenshot shows the Cisco Prime Infrastructure interface for configuring a composite template. The breadcrumb path is: Templates > Composite Templates > System Templates - Composite > Catalyst 3850 Switch Basic Configuration as MC.

Template Basic

- *Name: Catalyst 3850 Switch Basic Config
- Description: This template is used to convert
- Author: root
- Feature Category: Composite Template
- Tags: [Empty field]

Validation Criteria

- Device Type: Cisco Catalyst 3850 Series ...

Template Detail

Selected 0 | Total 13

	Name	Group	Description	Feature Category	Device Type	IOS Version
1	Configure Device IP	CLI Templates/System...	Configure Device IP	CLITemplate	Switches and Hubs,Wi...	
2	Configure NTP	CLI Templates/System...	Configure NTP	CLITemplate	Switches and Hubs,Wi...	
3	Configure SNMP	CLI Templates/System...	Configures SNMP	CLITemplate	Switches and Hubs,Wi...	
4	Local Management User	CLI Templates/System...	Configure Local Mana...	CLITemplate	Switches and Hubs,Wi...	
5	CUWN-IOS and UA Radius Aut...	CLI Templates/System...	CUWN-IOS and UA Ra...	CLITemplate	Switches and Hubs/Cis...	
6	Configure Interface	CLI Templates/System...	Configure Interface	CLITemplate	Switches and Hubs,Wi...	

Buttons: Save, Cancel, Publish, Deploy

Workflow Status: 0 | Support Cases | Alarm Browser | Alarm Summary: 199 | 2 | 175

Configuration Group Templates

Composite Templates with Selected Devices

The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The main content area is titled 'Configuration Groups' and is divided into two sections: 'Template Selection' and 'Device Selection'.

Configuration Group

Configuration Group

- Configuration Group
 - 3850 Switch Priority
 - 3945s
 - Test1234
 - WGBH_Config_Group
 - new

Template Selection

Selected 0 | Total 3

Selected Templates

Name	Group	Description	Feature Category	Device Type	IOS Version	
1	<input type="checkbox"/>	CUWN-IOS and...	System Templates - CLI	CLITemplate	Switches and Hubs/Cis...	
2	<input type="checkbox"/>	CUWN-IOS and...	System Templates - CLI	CUWN-IOS and UA Ra...	CLITemplate	Switches and Hubs/Cis...
3	<input type="checkbox"/>	CUWN-IOS and...	System Templates - CLI	Configure User Role P...	CLITemplate	Switches and Hubs/Cis...

Device Selection

To enable device selection at least one template needs to be added to the 'Selected Templates' table
Add and select devices to save the configuration group for deployment.

Selected 0 | Total 3

Selected Devices

Name	Description	Type	IP Address	Vendor		
1	<input type="checkbox"/>	AMS-5760-WLC.cisco.com	AMS-5760-WLC.cisco.com	Wireless Controller	192.168.152.11	Cisco
2	<input type="checkbox"/>	PAR-3850-1	PAR-3850-1	Switches and Hubs	10.12.10.2	Cisco
3	<input type="checkbox"/>	BXB-3850-1	BXB-3850-1	Switches and Hubs	10.5.10.2	Cisco

Controller Config-Groups Overview

What Are Controller Config-Groups?

- An easy way to group controllers logically
- Provides a way to manage controllers with similar configurations
 - Extract templates from existing controller to provision
 - Schedule configuration sets
 - Cascade Reboot
- Manage Mobility Groups, DCA, and Configuration Auditing

When Are Controller Config-Groups Used?

- Group sites together for easier management for:
 - Mobility Groups
 - DCA and Regulatory Domain Settings
 - Schedule remote configuration changes
- Groups sites to ensure compliance with configuration policies

Controller Config- Groups

How To Setup

The screenshot displays the Cisco Prime Infrastructure interface. On the left, the navigation menu is open, showing the path: Configuration > Wireless Configuration > Controller Configuration Groups. A red dashed box highlights 'Controller Configuration Groups' in the menu. A blue arrow points from this menu item to the main content area.

The main content area shows the 'Controller Config Groups' page with a table of existing groups:

Group Name	Mobility Group Name	Controllers	Templates	Scheduled	Next Scheduled Run	Last Modified	Last Applied
<input type="checkbox"/> Config	-	2	2	No	-	2013-Oct-02, 08:07:34 PDT	-
<input type="checkbox"/> Test2	-	0	0	No	-	-	-
<input type="checkbox"/> test	-	0	0	No	-	-	-
<input type="checkbox"/> WGBH_demo	WGBH_controllers	2	3	No	-	2014-Feb-18, 13:19:36 PST	-

Below the table, the 'Add Config Group' form is shown. The 'Group Name' field contains 'Campus ABC'. The 'Templates' section has two radio buttons: 'Select and add later' (selected) and 'Copy applied templates from a controller'. A dropdown menu is open, showing a list of controllers to copy templates from:

- 192.168.152.11 (AMS-5760-WLC.cisco.com)
- 10.5.10.2 (BXB-3850-1)
- 10.11.13.1 (LON-2504-WLC)
- 10.12.10.2 (PAR-3850-1)
- 192.168.136.49 (SJ-WISM2-1)
- 192.168.136.48 (WLC-4400-1)
- Add selected controller to this group.

Only create the config group and then add controllers and templates at another time

Copy templates from one of the controllers currently in PI and then apply them to controllers in this config group.

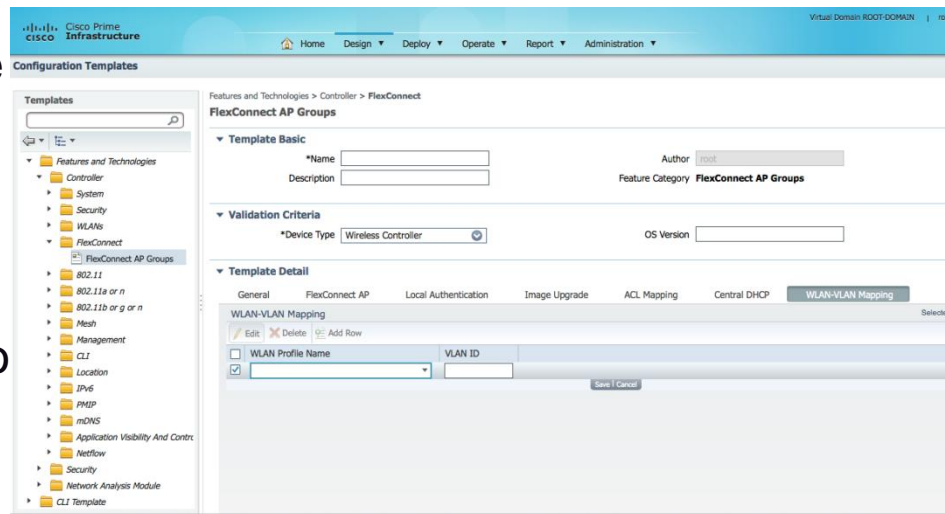


Controller Config-Groups: Things to Remember

- Template order is very important!
- Background audit is performed during network and controller audit
- Background audit and audit enforcement can only run when template-based audit is selected (under Administration—Settings)
- WLC(s) may be part of multiple configuration groups so be careful while setting mobility group names

FlexConnect – WLAN to VLAN Mapping

- Prior to WLC 7.5 release, WLAN to VLAN mapping was done on per AP basis
- Made it difficult for the users to configure in the case of large number of access points deployed.
- WLC 7.5 release adds WLAN to VLAN mapping from the FlexConnect group
- Will push the WLAN to VLAN mapping to all AP's present in FlexConnect group
- Will not override the WLAN-VLAN mapping done on the AP.



Configuration - Auditing

Administration > Background Tasks > Other Background Tasks > Configuration Sync

Configuration Sync
Administration > Background Tasks > Other Background Tasks > Configuration Sync

Last Execution Information

Start Time	End Time	Elapsed Time (Seconds)	Result
2012-Apr-09, 04:00:00 PDT	2012-Apr-09, 04:00:30 PDT	30	Success
2012-Apr-10, 04:00:00 PDT	2012-Apr-10, 04:00:21 PDT	21	Success
2012-Apr-11, 04:00:00 PDT	2012-Apr-11, 04:00:23 PDT	23	Success
2012-Apr-12, 04:00:00 PDT	2012-Apr-12, 04:00:22 PDT	22	Success
2012-Apr-13, 04:00:00 PDT	2012-Apr-13, 04:00:23 PDT	23	Success

Edit Task

Description: Configuration Sync

Used By Report(s): Network Configuration Audit

Enabled: Enabled

Network Audit: Enabled

Security Index Calculation: Enabled

RRM Audit: Enabled

Interval: (Days)

Time of Day: (hh:mm AM | PM)

Save Cancel

- Automatic audits based on “configuration sync” background task.
- Specify frequency of audit

- Allows easy reconciliation in the event of a configuration mismatch
- Helps ensure WLCs comply with configuration policies

Quick Audit Summary and Reconciliation

Controllers

Configure > Controllers

-- Select a command -- Go

<input type="checkbox"/>	IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
<input type="checkbox"/>	171.71.122.80	WCS-Beta	5500		7.0.112.2	WNBU-TME	Reachable	Identical
<input type="checkbox"/>	171.71.128.157	sjc14-wl-wlc3	2500	SJC Bld 14 - FL 1/2	7.0.116.0	SJCwireless	Reachable	Mismatch
<input type="checkbox"/>	171.71.128.75	SJC 14 LWAPP1	5500	SJC Bld 14 - FL 1/2	7.0.116.0	SJCwireless	Reachable	Mismatch
<input type="checkbox"/>	171.71.128.78	SJC 14 LWAPP2	5500	SJC Bld 14 - FL 3/4	7.0.116.0	SJCwireless	Reachable	Identical

Audit Summary

Restore or Maintain Config

Audit Result

Device name **sjc14-wl-wlc3**

Audit Time **Apr 14, 2012 12:02:06 AM**

Audit Status **Mismatch**

Total Enforcements for Config Groups with background audit enabled **0**

Failed Enforcements for Config Groups with background audit enabled **0**

Applied Template and Config Group Template Discrepancies

(Template Type)Template Name	Template Applied Via	Audit Status	Attribute	NCS Value	Controller Value
(WLAN Template) test	Independent Template	Not Present in Controller	-	-	-
(AP / MSE Authorization Templates) d8d385c122da	Independent Template	Mismatch	Key Hash	08df221b75f0153c4f4f72dac24434018ebfc62e	****

NCS Config Discrepancies

(Type)Configuration Name	Audit Status	Attribute	NCS Value	Controller Value
(Local Management User) allia1	Not Present in NCS	-	-	-
(AP Groups VLANs) 171.71.128.157/default-group	Mismatch	Profile	test	-
(AP Groups VLANs) 171.71.128.157/default-group	Mismatch	Interface Mapping	management	-

[Restore NCS Values to Controller](#) [Refresh Config from Controller](#)

Audit Settings

Audit Settings

■ Audit Mode

- Basic Audit: Perform an audit on current WLC configuration and compare it with the configuration in PI
- Template-Based Audit: Perform an audit on current WLC configuration with respect to applied templates, config groups' background templates and then the configuration in PI

■ Audit On

- All Parameters: Audit on entire WLC configuration
- Selected Parameters: Audit on selected parameters from the templates

Scheduled Image Download to Controller

Download Software to Controller
Configure > Controllers > Download Software to Controller

Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version	Operation Status	Details
171.71.128.157	7.2.103.0	NOT_INITIATED	-

Download Type

Download Type *i*

Now *i*

Scheduled

Schedule *i*

Download software to controller

Pre-download software APs *i*

APs download the image and then reboot when the controller reboots.

FlexConnect AP Upgrade

Upgrade Image

Schedule Details

Task Name

Reboot Type Manual Automatic Scheduled

Schedule *i*

Download date/time :

Reboot date/time :

Current Server Time: 2012-Apr-14, 00:06:13 PDT

Notification (Optional) *i*

To be notified on download completion, enter an email address.

- Provides option to schedule software download (FTP/TFTP) to controllers.
- Task can be saved for future scheduling.
- Reboot can be scheduled at a future date/time.
- Email notification can be sent after completion of download.

Mobility Work Centre

Converged Access View

Operate ▾ Report ▾ Administration ▾ Workflows ▾

- Monitoring Dashboards
 - Overview
 - Incidents
 - Performance
 - Detail Dashboards
- Device Work Center
 - Discovery
 - Configuration Archives
 - Software Image Management
 - Image Dashboard
 - Plug and Play Status
 - Network Audit
- Alarms & Events
- Clients and Users
- Maps
 - Google Earth Maps
- Container Services
 - Services Catalogue
 - Deployed Services
- Applications and Services
 - Application Server Management
- Operational Tools
 - Application Troubleshooting
 - Mediatrace
 - Device Resource Estimation
 - Packet Capture ▾
 - Media Streams

Mobility Work Centre

Device role can be changed to MO/MC/MA

Virtual Domain ROOT-DO1

Home Design ▾ Deploy ▾ Operate ▾ Report ▾ Administration ▾ Workflows ▾

Mobility Domains

- All Mobility Devices
- Default-Domain
- test

All Mobility Devices

Change Role To Mobility Controller Change Role To Mobility Agent Assign Mobility Group

Device Name	Management IP	Wireless Interface IP	Mobility Group
AMS-5760-WLC.cisco.com	192.168.152.11	192.168.152.11	default
PAR-3850-1	10.12.10.2	169.254.1.1	default
<input checked="" type="checkbox"/> BRX-3850-1	10.5.10.2	10.5.13.2	default

Show All

Mobility Role

- Admin - MC, Operational - MC
- Admin - MA, Operational - MA
- Admin - MC, Operational - MC

Tree hierarchy displays mobility domain, SPG and device-level relationship

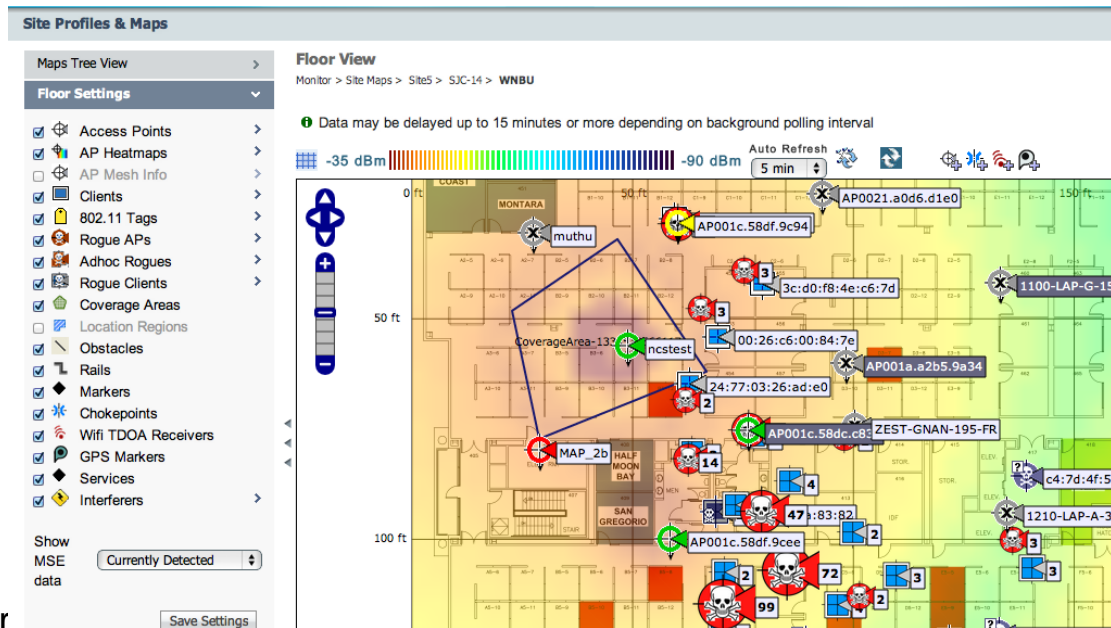
Lists NGWC devices and their role (MO, MC, MA).
Operational: current role
Admin: role after next reboot



Configuration - Maps

Configuration Maps

- Track wireless clients and tags, and play location history across campus
- Track and mitigate rogue devices
- Display Chokepoints
- Display Mesh AP relationships
- Integrate outdoor wireless mesh with Google Earth
- Represent wireless coverage on campus, and plan for growth
- View Channel and Tx Power plans provisioned by RRM
- View AP and RF Profile at the floor level
- Provision and display coverage areas, markers, and other objects and use them with location notifications
- Post-Deployment: VoWLAN and Location Readiness tools



Map Export/Import

Export Map
Monitor > Maps > **Export Map**

Include Map Information
 Include Calibration Information
 Calibration Information for selected maps All Calibration Information

Select All Maps

Cisco San Jose - Site 5
 BLD 14
 1st floor
 2nd floor
 3rd floor
 4th floor
 System Campus

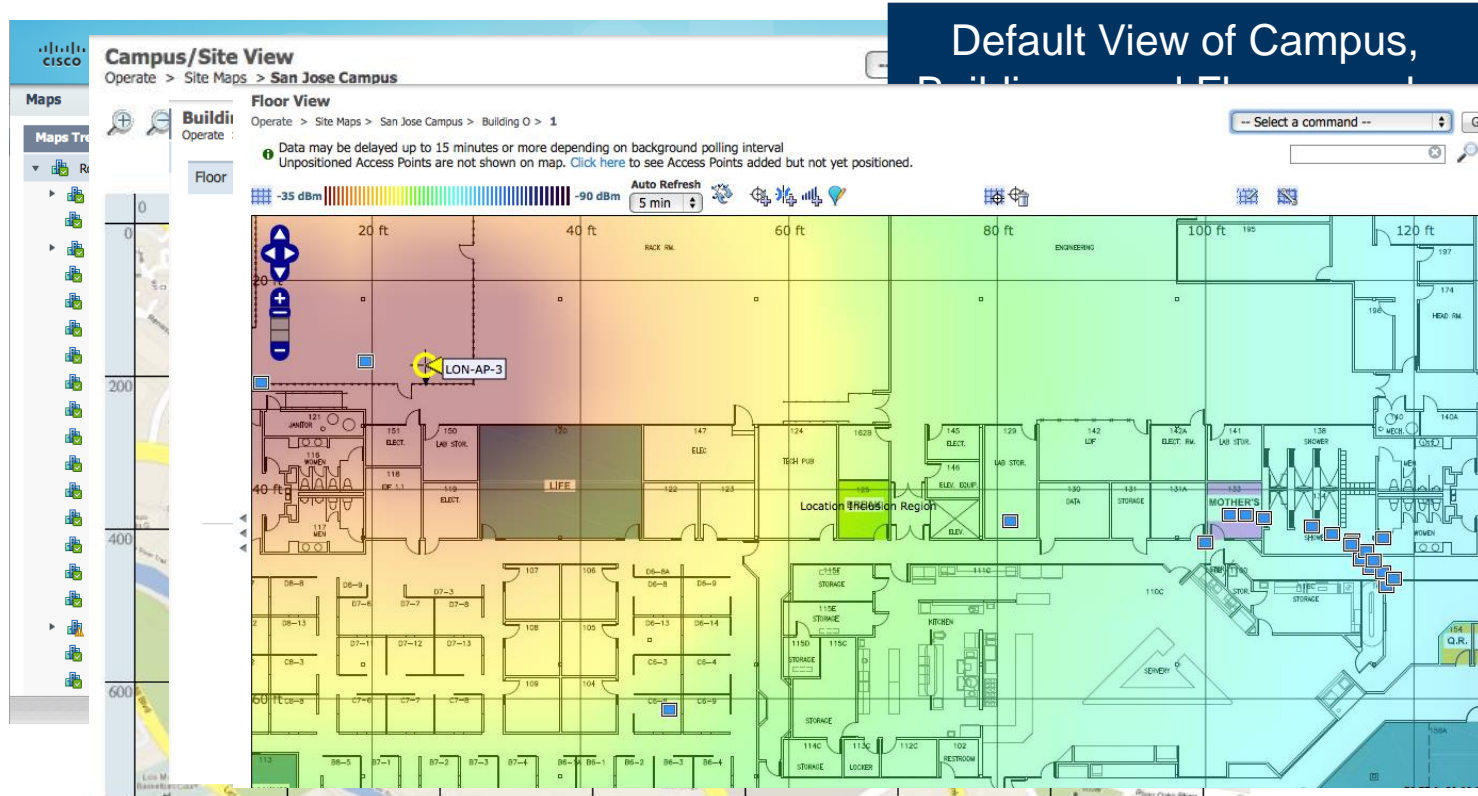


Monitor > Maps > **Import Map -- Choose map format**

XML Format
 AP/WiFi TDOA Receiver/Chokepoint Placement
 WLSE Map and AP Location Data

- Provides ability to export maps from source WCS/NCS to destination PI server.
- Can select all maps or subset.
- Export/import of map includes both map and AP's placed on MAP.
- Option to export calibration information.
- Exported via tar gzipped XML file.
- Import process ungzips/untars XML file automatically.

Maps Layout



Default View of Campus,

Buildings are
easily accessible through an easy
to use interface that provides a
summary view of floors' status
for troubleshooting

Maps Layout – AP's and Clients

Floor Settings

- Access Points
- AP Heatmaps
- Clients
- 802.11 Tags
- Rogue APs
- Adhoc Rogues
- Rogue Clients
- coverageAreas
- Location Regions
- Rails
- Markers
- Choquepoints
- Wifi TDOA Receivers
- GPS Markers
- Interferers

AP Filter

Total APs: 20
Show Radio Status AP Status

Protocol: 802.11b/g/n

Display: Assoc. Client

RSSI Cutoff: -75 dBm

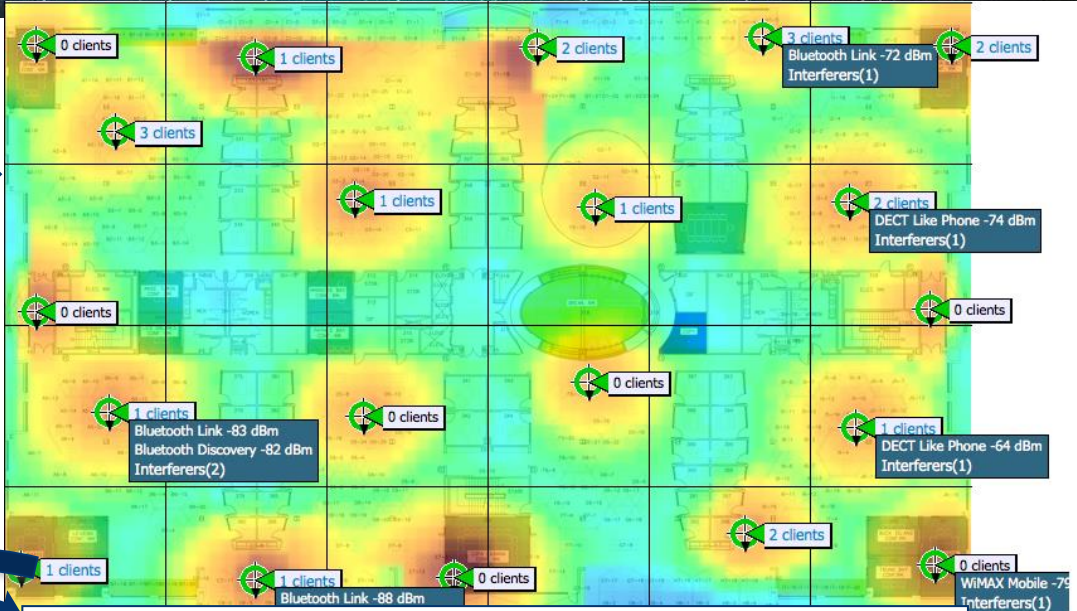
Show Detected Interferers:

Max. Interferers / label: 2

OK

Display client count as AP label, and detected interferers per AP.

Client count is hyperlink that takes user to “Clients and Users” list page with filters list of clients connected to AP.



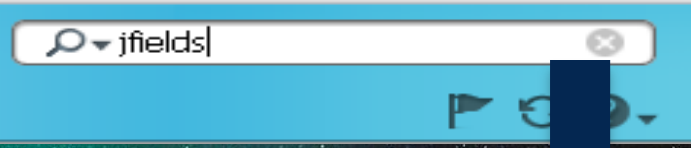
Clients and Users

Clients Search Results - Reset

Troubleshoot Test Disable Remove More Track Clients Identify Unknown U

MAC Address	IP Address	User Name	Type	Location
00:24:d7:1d:76:78	171.70.241.202	CISCO\ajaggi		Cisco San Jose - Site 5 > BLD 14 > 3rd floor

Automated Wired/Wireless Client Discovery



Search Results

i 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](#)

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	Controller Name	SSID
2012-Aug-23, 09:37:45 PDT	3 hrs 8 min 4 sec	jfields	192.168.152.37	Dual-Stack	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Aug-22, 15:15:34 PDT	3 hrs 43 min 59 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Aug-21, 14:38:21 PDT	17 hrs 21 min 22 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X
2012-Aug-20, 17:12:58 PDT	10 hrs 37 min 1 sec	jfields	192.168.152.37	IPv4	NMTG-AP3500-2	AMS-2504-WLC	AMS-DOT1X

Achieve Operational Excellence

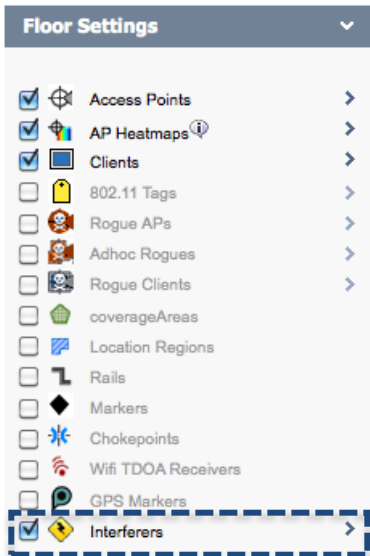
The 360 Experience

- **Simplified troubleshooting and remediation improves application, services and end user experience**
 - Brings together multiple sources of information for effective problem isolation
- **User 360 – quickly isolate and fix end-user or end-point issues**
(response time, network access, configuration etc.)
- **Device 360 – identify and fix device related problems** (performance, faults, interface, modules)
- **Application 360 – identify and fix network issues related to app delivery**
(app discovery, utilisation, user/device/site association)

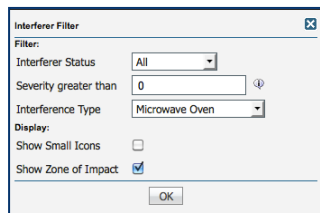
The screenshot displays the 'User 360 View' for user 'jfields'. It features three device status cards: Workstation, SonyPS3, and Apple-iPad. Below these is a detailed endpoint information section with fields for IP, MAC, Location, Connected to (Switch, Interface, VLAN), Session (Authorization Profile, Compliance, Association Time, Session Length), and Location. At the bottom, there is a table for application usage.

End Point	Mac Address	Application	Last 1 Hour Volume (...)
192.168.152.27	dc::0:e::a1::b:9:	youtube	1149.3889
192.168.152.27	dc::0:e::a1::b:9:	http	0.7073
192.168.152.27	dc::0:e::a1::b:9:	unclassified	0.1429

Maps Layout – CleanAir



Quickly filter on subset of interferers on floor.
Can specify other parameters: severity level, zone of impact.



Real-Time Heat Maps

- Based on AP-to-AP RSSI measurements
- Predictive (legacy) heat maps still supported
- Provides graphical view of RSSI based on set of nearest AP's vs. AP transmit power (predictive heat map)
- Configurable options for real-time heat maps:

Min. number of APs
Recompilation interval

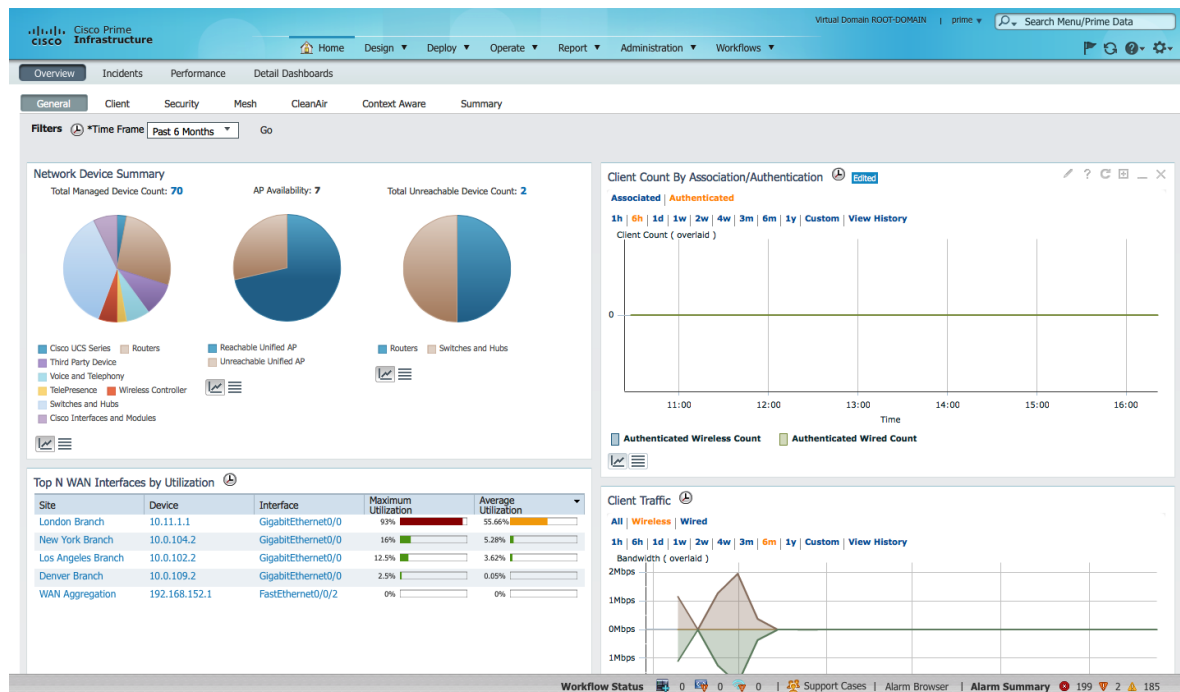




Monitoring The Network

Monitoring — Dashboard Concepts

- Canned tabs of high-level system views
- Ability to add/remove tabs
- Ability to add/remove components within tabs
- Customise individual components
- Introduction of trending information at system level
- Quick drill-downs



Information Layout and Workflow Concepts

- Presents many **intuitive** ways to arrive at information
- Ability to **drill-down** to an individual client-level detail from dashboard
- Ability to drill-down with the help of “**Quick Filters**”
- Ability to **sort** on different attributes in client list pages
- Ability to perform and **save intelligent searches**
- Ability to **customise** list layout, items per page and content
- Perform advanced **context-sensitive actions** (such as launching a report from AP page) from page drop-downs

Dashboard Customisation Dashlets

Virtual Domain ROOT-DOMAIN | prime | Search Menu/Prime Data

Home Design Deploy Operate Report Administration Workflows

Overview Incidents Performance Detail Dashboards

General Client Security Mesh CleanAir Context Aware Summary

Filters *Time Frame Past 6 Months Go

Network Device Summary

Total Managed Device Count: **70** AP Availability: **7** Total Unreachable Device Count: **2**

Legend: Cisco UCS Series, Routers, Third Party Device, Voice and Telephony, TelePresence, Wireless Controller, Switches and Hubs, Cisco Interfaces and Modules

Client Count By Association/Authentication

Associated | Authenticated

Coverage Area

List coverage areas and details about each coverage area

Name	Total APs	APs Online	APs Offline	APs Not Configured	APs Not Found	APs Not Responding	APs Not Responding	APs Not Responding	APs Not Responding
London	115	115	115	0	0	0	0	0	0
NYC	1	1	1	0	0	0	0	0	0
LA	1	1	1	0	0	0	0	0	0
Denver	1	1	1	0	0	0	0	0	0
WAN Aggregation	1	1	1	0	0	0	0	0	0

Top N WAN Interfaces by Utilization

Site	Device	Interface	Maximum Utilization	Average Utilization
London Branch	10.11.1.1	GigabitEthernet0/0	93%	55.66%
New York Branch	10.0.104.2	GigabitEthernet0/0	16%	5.28%
Los Angeles Branch	10.0.102.2	GigabitEthernet0/0	12.5%	3.62%
Denver Branch	10.0.109.2	GigabitEthernet0/0	2.5%	0.05%
WAN Aggregation	192.168.152.1	FastEthernet0/0/2	0%	0%

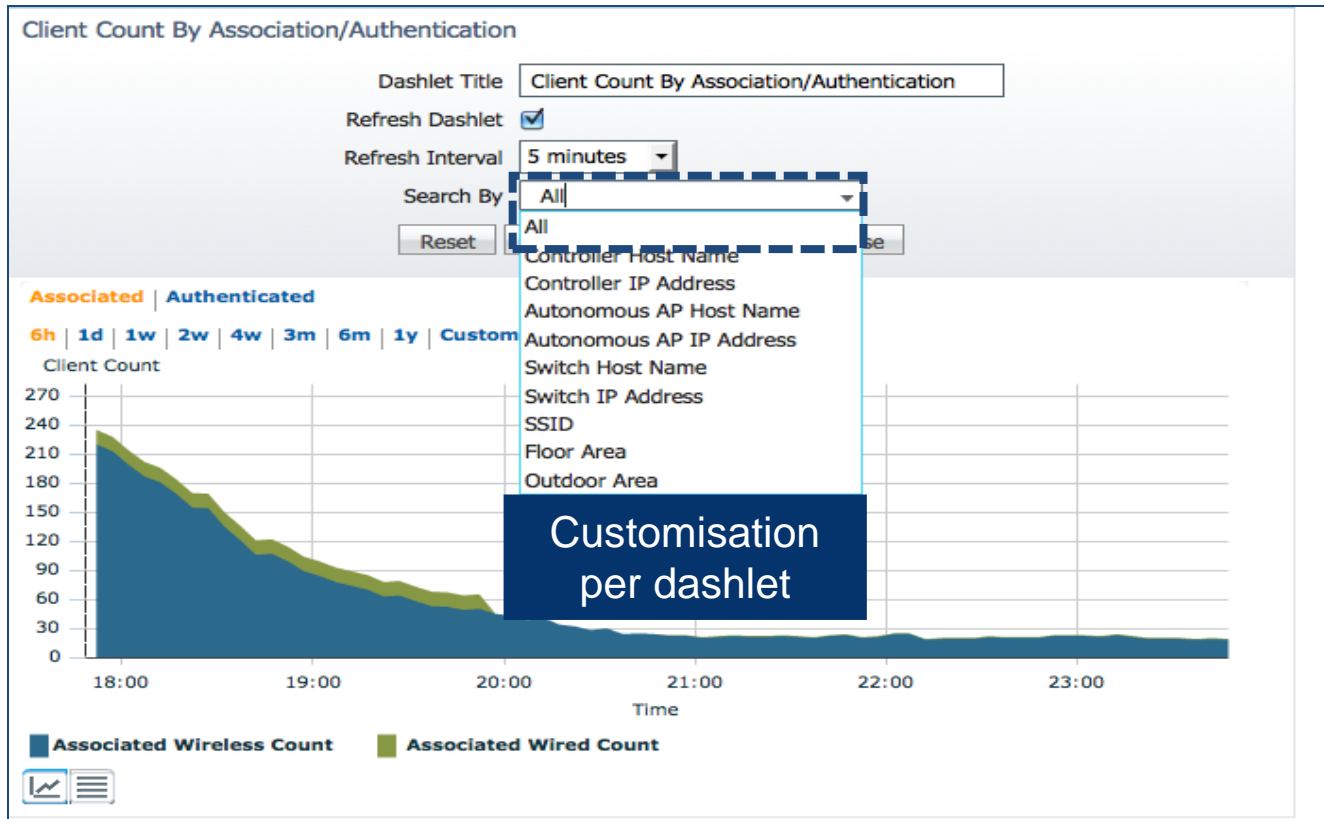
Client Traffic

Authenticated Wireless Count Authenticated Wired Count

Menu: Add New Dashboard, Rename Dashboard, Add Dashlet(s), General Dashlets, AP Join Taken Time, AP Uptime, ADM/AD I Uptime, AP Uptime, Coverage Area, Device Uptime, GETVPN Network Stat..., Job Information Status, Most Recent AP Alarms, Network Device Sum..., Recent Alarms, Recent Coverage Holes, Layout Template, Manage Dashboards

“drag and drop” dashboard customisation

Dashlet Customisation



Finding Data – Search Capability

- PI and MSE represent a large data store
- PI provides Advanced Search capability
- Various filter criteria depending on search categories

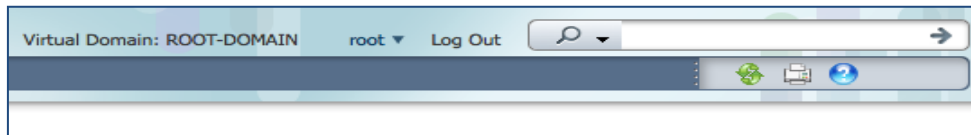
Basic Search	Searches for: clients, devices (AP's, controllers, switches), rogue (AP, ad hoc), alarms. Output is categorised.
Advanced Search	Multiple search categories and criteria (alarms, AP's, controller licenses, switches, clients, chokepoints, interferers, TDOA receivers, maps, rogue clients, shunned clients, RFID tags). Searches can be saved for future use.

Using Search

Global Search Capability

- Searches can be performed on partial input
- Search output provides configuration and monitor links based on device type found
- Search parameters include IP Address, Usernames, MAC Addresses, SSIDs ,Rogues and AP Names

Advanced searches can be saved for easy future reference and use



Search Results

i Your search 'ap' matched following Item(s). Please click on the 'View List' to access the matched items list under either Monitor or Configuration

Item Type	Item Count	Monitor	Configuration
Client	33	View List	
AP	128	View List	View List
Controller	2	View List	View List
Rogue AP	79	View List	
Alarm	1624	View List	

Footnotes

1. The search was performed to applicable for different item type

New Search

Search Category: Clients
Media Type: Wired Clients
Search By: Floor Area
Clients Detected By: NCS
Speed: Any
Client States: Authenticated
Campus: Cisco S3-5
Building: Bld-14
Floor Area: 4
Access Point: All Access Points
Posture Status: All
Include Disassociated:
Items per page: 50
Save Search: []

Go

IP Address or Name or SSID as Rogue Clients.

Finding Data – Security Alarms

Customised search for specific alarm criteria

New Search

Search Category: Alarms
Severity: All Severities
Alarm Category: Security
Condition: Too many user unsuccessful logins
(Select from dropdown box or key in Condition)
Time Period: Any Time
Acknowledged State:
Assigned State:
Save Search:
Go

Alarms
Search Results - Reset
Selected 0 | Total 2

	Severity	Failure Source	Time	Message	Category	Condition
<input type="checkbox"/>	Critical	WLAN Controller sjc14-wl...	2011-Sep-02, 11:23:37 PDT	User 'admin' with IP Address '171.71.133.238' has made too many unsuccessful login attempts.	Security	Too many user unsuccessful logins
<input type="checkbox"/>	Critical	WLAN Controller SJC 14 L...	2011-Sep-02, 08:51:58 PDT	User ';!' with IP Address '10.21.65.14' has made too many unsuccessful login attempts.	Security	Too many user unsuccessful logins

- Use case: admin wants to search for all security alarms “too many user unsuccessful logins”

Finding Data – Client Search

The screenshot displays the 'New Search' configuration window on the left and the 'Clients and Users' search results table on the right. A blue box with the text 'Customised search for specific client criteria' is overlaid on the search criteria, with a double-headed arrow indicating the relationship between the criteria and the results. A blue arrow points from the search criteria to the results table.

Search Criteria:

- Search Category: Clients
- Media Type: Wireless Clients
- Wireless Type: Lightweight Clients
- Search By: Floor Area
- Clients Detected By: NCS
- Client States: Authenticated
- Campus: Cisco San Jose - Site 5
- Building: BLD 14
- Floor Area: 4th floor
- Access Point: All Access Points
- Posture Status: All
- Restrict By Radio Band: 5GHz
- Restrict By Protocol: 802.11n
- Search on Devices Now:
- SSID: blizzard
- Profile:
- NAC State:

Search Results Table:

IP Address	MAC Address	User Name	Type	Vendor	AP Name	Device Name	Location	SSID	Status	Interface	Protocol
171.70.240.193	00:24:d7:a8:74:94	CISCO\antonino	Client	Intel	SJC14-42B-AP7	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.121	00:24:d7:9d:f6:e4	CISCO\yizhang	Client	Intel	SJC14-42B-AP3	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.60	e4:ce:8f:06:7b:08	antvagi	Client	Apple	SJC14-42B-AP3	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.15	00:21:6a:4a:bf:bc	viviliu	Client	Intel	SJC14-42B-AP3	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.107	00:24:d7:17:ad:fc	CISCO\lbeutels	Client	Intel	SJC14-41B-AP3	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.42	00:26:bb:1d:e9:db	rangoel	Client	Apple	SJC14-41B-AP3	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.146	f8:1e:df:e1:2a:b5	towan	Client	Apple	SJC14-41B-AP2	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.242.18	58:b0:35:7c:6b:17	rkomali	Client	Apple	SJC14-42B-AP9	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.240.195	00:24:d7:2a:43:9c	CISCO\htamvada	Client	Intel	SJC14-41B-AP6	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.243.214	00:21:6a:95:4c:46	nsundare	Client	Intel	SJC14-41B-AP6	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)
171.70.241.93	00:21:6a:ab:0e:5c	qjirma	Client	Intel	SJC14-42B-AP6	SJC 14 LWAPP1	Unknown	blizzard	Associated	corp1	802.11n(5GHz)

- Use case: admin wants to search for all authenticated wireless clients (802.11n, 5 GHz) on 4th floor

Finding Data – AP Search

New Search ✕

Search Category:

Search By:

AP Name:

AP Type:

AP Mode:

Radio Type:

802.11n Support:

OfficeExtend AP Enabled:

CleanAir Support:

CleanAir Enabled:

Items per page:

Save Search:

Customised search
for specific AP
criteria

Access Points [Edit View](#)

Monitor > Access Points

Generate report for selected APs

Entries 1 - 20 of 20

AP Name	Ethernet MAC	IP Address	Radio	Map Location	Oper Status	CleanAir Capable	CleanAir Sensor Status	CleanAir Status	Controller	Controller Name	Radio Client Count	Admin Status	AP Mode	Alarm Sta
<input type="checkbox"/> SJC14-32B-AP7	f8:66:f2:67:69:b9	171.71.130.160	802.11a/n	Cisco San Jose - Site 5 > BLD 14 > 3rd floor	Up	Yes	Up	Enabled	171.71.128.78	SJC 14 LWAPP2	14	Enabled	Local	⚠
<input type="checkbox"/> SJC14-32B-AP3	f8:66:f2:67:67:af	171.71.131.83	802.11a/n	Cisco San Jose - Site 5 > BLD 14 > 3rd floor	Up	Yes	Up	Enabled	171.71.128.78	SJC 14 LWAPP2	1	Enabled	Local	✅
<input type="checkbox"/> SJC14-31B-AP9	f8:66:f2:67:6e:31	171.71.130.147	802.11a/n	Cisco San Jose - Site 5 > BLD 14 > 3rd floor	Up	Yes	Up	Enabled	171.71.128.78	SJC 14 LWAPP2	5	Enabled	Local	✅

- Use case: admin wants to search for CAPWAP, 802.11a (5 GHz) AP's by AP name (partial string search) that are operating in local mode

Finding Data – Controller Search

New Search

Search Category: Controllers

Search for controller by: All Controllers

Audit Status: Mismatch

Items per page: 50

Save Search:

Controllers [Edit View](#)

Monitor > Controllers

IP Address	Device Name	Device Type	Location	Mobility Group Name	RF Group Name	Reachability Status	AP Count	Client Count	Audit Status
171.71.128.157	sjc14-wi-wlc3	2500	SJC Bld 14 - FL 1/2	SJCwireless	SJCwireless	Reachable	0	0	Mismatch
171.71.122.80	WLC-mesh	5500	WNBU-TME	WNBU-TME	WNBU-TME	Reachable	6	0	Mismatch
171.71.128.75	SJC 14 LWAPP1	5500	SJC Bld 14 - FL 1/2	SJCwireless	SJCwireless	Reachable	43	114	Mismatch
172.20.225.154	Talwar-TME	5500	mobile-t	mobile-t	mobile-t	Reachable	1	0	Mismatch
171.71.128.78	SJC 14 LWAPP2	5500	SJC Bld 14 - FL 3/4	SJCwireless	SJCwireless	Reachable	20	246	Mismatch

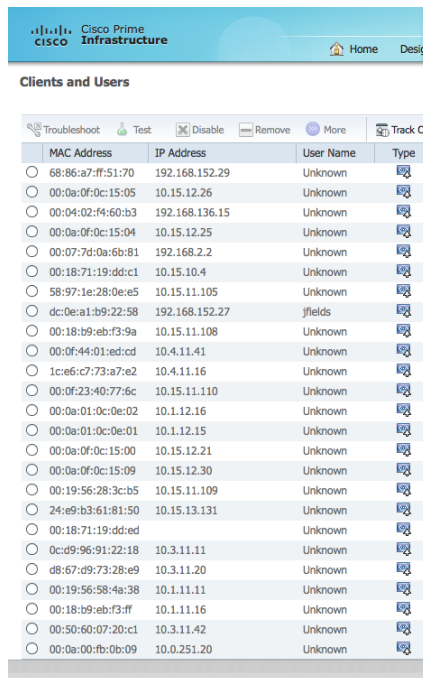
Entries 1 - 5 of 5

- Use case: admin wants to search for all controllers where config mismatch has occurred

Monitoring Clients and Users

Common Steps in a Troubleshooting Scenario:

- Lookup a client: MAC Address, Username, IP Address, Client type, Client state, From AP Details Page
- Where is the client now (and how is their RF profile)
- Where has this client been (Location playback, session and AP history)
- Active troubleshooting



Cisco Prime Infrastructure
Clients and Users

MAC Address	IP Address	User Name	Type
68:86:a7:ff:51:70	192.168.152.29	Unknown	
00:0a:0f:0c:15:05	10.15.12.26	Unknown	
00:04:02:f4:60:b3	192.168.136.15	Unknown	
00:0a:0f:0c:15:04	10.15.12.25	Unknown	
00:07:7d:0a:6b:81	192.168.2.2	Unknown	
00:18:71:19:dd:c1	10.15.10.4	Unknown	
58:97:1e:28:0e:e5	10.15.11.105	Unknown	
dc:0e:a1:b9:22:58	192.168.152.27	jfields	
00:18:b9:eb:f3:9a	10.15.11.108	Unknown	
00:0f:44:01:ed:cd	10.4.11.41	Unknown	
1c:e5:c7:73:a7:e2	10.4.11.16	Unknown	
00:0f:23:40:77:6c	10.15.11.110	Unknown	
00:0a:01:0c:0e:02	10.1.12.16	Unknown	
00:0a:01:0c:0e:01	10.1.12.15	Unknown	
00:0a:0f:0c:15:00	10.15.12.21	Unknown	
00:0a:0f:0c:15:09	10.15.12.30	Unknown	
00:19:56:28:3c:b5	10.15.11.109	Unknown	
24:e9:b3:61:81:50	10.15.13.131	Unknown	
00:18:71:19:dd:ed	Unknown	Unknown	
0c:d9:96:91:22:18	10.3.11.11	Unknown	
d8:67:d9:73:28:e9	10.3.11.20	Unknown	
00:19:56:58:4a:38	10.1.11.11	Unknown	
00:18:b9:eb:f3:ff	10.1.11.16	Unknown	
00:50:60:07:20:c1	10.3.11.42	Unknown	
00:0a:00:fb:0b:09	10.0.251.20	Unknown	

User 360° View

Username : jfields



Microsoft-Worksta... Android Apple-Device

Endpoint	Location
IP 192.168.152.27 MAC dc:0e:a1:b9:22:58	Unknown

Connected to	Session
Switch AMS-3750-SBR Interface FastEthernet1/0/6 VLAN 12	Authorization Profile Not Available Compliance Unknown Association Time 2014-Feb-18, 19:28:58 Session Length 6 days 21 hrs 53 min 51 sec

Time	Source	Message
January 9, 2014 5:25:...	192.168.152...	Port 'FastEthernet1/0/38' is down ...
February 6, 2014 1:4...	192.168.152...	Port 'FastEthernet1/0/41' is down ...

Monitoring: Client Details - 1

Client dc:0e:a1:b9:22:58 (Refreshed :2014-Feb-18, 00:28:58 PST)

Note: None >>

Client Attributes

General

User Name **jfields** ⓘ
IP Address **192.168.152.27**
MAC Address **dc:0e:a1:b9:22:58**
Vendor **Compal**
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 **AMS-3750-SBR**
Switch IP Address **192.168.152.10**
Interface **FastEthernet1/0/6**
Wired Speed **100Mbps**
VLAN ID **12**
VLAN Name **Campus_Data**
Status **Associated**
On Network **Yes**

Traffic

Basic Client Properties—can be expanded for further details

Security

Authenticating ISE **Data Not Available**
Authentication Method **802.1X**
Auth Status **Authorization Succeeded**
Authorization Profile Name **Data Not Available**
Posture Status **Unknown**
TrustSec Security Group **Data Not Available**
Audit Session ID **COA8980A00003B26EC9A555C**
Windows AD Domain **Data Not Available**
EAP Type **Unknown**

Session History

Association Time	Duration	User Name	IP Address	IP Address...	Hostname	Switch Name	Interface	VLAN ID	Traffic (MB)
2014-Jan-15, 21:06:15 PST	30 days 0 hrs 19 min 5 sec	jfields	192.168.152.27	IPv4	unknown	AMS-3750-SBR	FastEthernet1/0/6	12	0.0
2014-Feb-15, 00:01:15 PST	3 days 0 hrs 13 min 14 sec	jfields	192.168.152.27	IPv4	unknown	AMS-3750-SBR	FastEthernet1/0/6	12	0.0
2014-Feb-18, 00:28:58 PST	6 days 21 hrs 46 min 39 sec	jfields	192.168.152.27	IPv4	unknown	AMS-3750-SBR	FastEthernet1/0/6	12	0.0

Client Association, Session History and Roam Reason

Events

Event Type	Event Time	Description
------------	------------	-------------

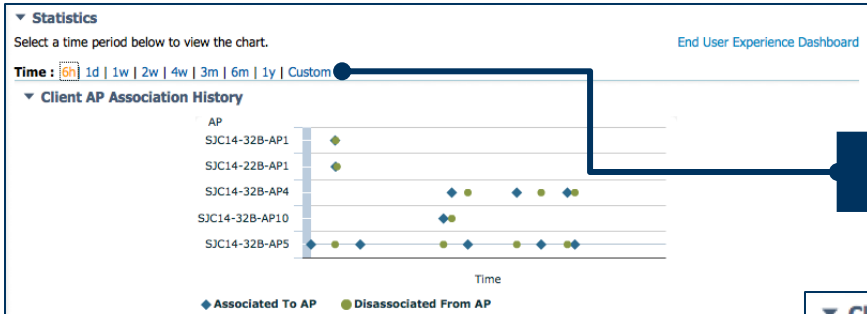
No data available

Time : 6h | 1d | 1w | 2w | 4w | 3m | 6m | 1y | Custom

Bytes Sent and Received (Kbps)

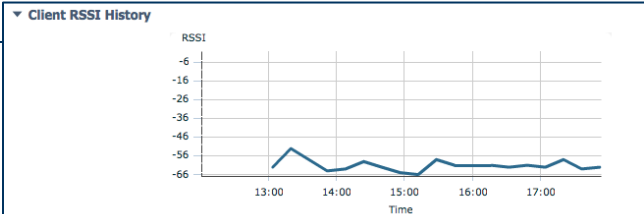
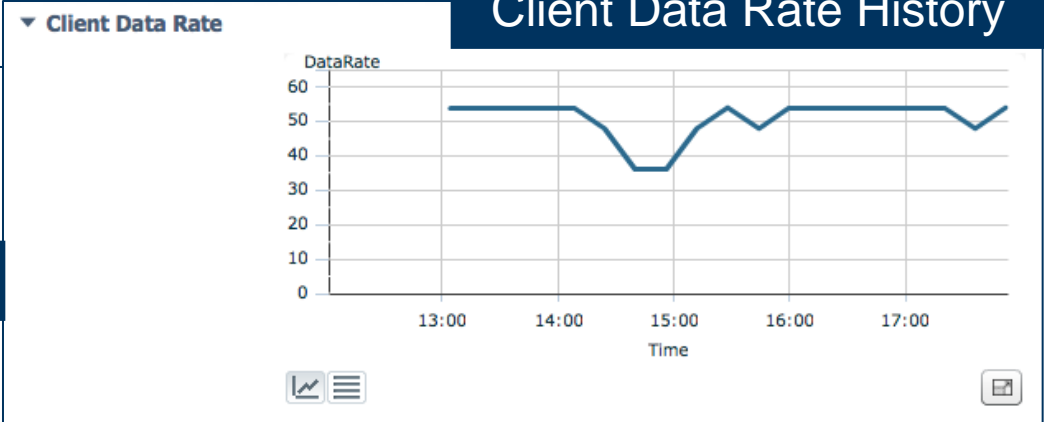
Time	Send Rate	Receive Rate	Dropped Byt...	Dropped Byt...

Monitoring: Client Details - 2

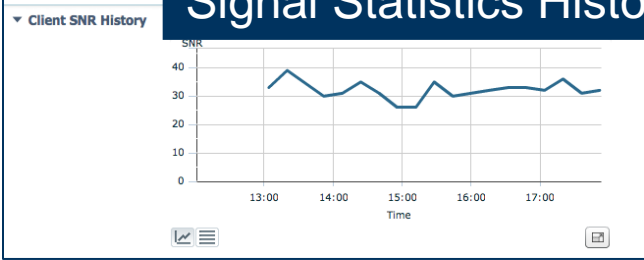


Client AP Association History

Client Data Rate History



Signal Statistics History



Sleeping Client

- Prior to WLC 7.5 release, client device connected to the WLC on web-auth enabled WLANs has to enter login credentials every time the client goes to sleep and wakes up.
- In WLC 7.5 release, client entry is cached for a configurable duration (up to 30 days / 720 hours)
- Sleeping interval is configured on a per WLAN basis
- When exceeding the user-idle timeout, client database entry is moved to a cache section of the database for the duration of the cache duration

New Controller Template

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > **New Controller Template**

General

Security

QoS

Advanced


HotSpot

Policy Configuration

Layer 2

Layer 3


AAA Servers

Layer 3 Security 

None

Web Policy



- Authentication
- Passthrough
- Conditional Web Redirect
- WebAuth on MAC Filter Failure 

Preauthentication ACL

IPv4 none

IPv6 none

WebAuth none

Sleeping Client

Enable

Sleeping Client Timeout

12 (hrs)

Global WebAuth Configuration

Enable

Web Auth Type

Default Internal

Enable sleeping client
and timeout value in
WLAN template

Track Clients

The screenshot shows the 'Track Clients' configuration page. At the top, there's a header 'Track Clients' and a sub-header 'Get notified when specific MAC addresses are detected on the network.?' Below this is a toolbar with 'Add', 'Import', 'Edit', and 'Remove' buttons, and a 'Show' dropdown set to 'All'. A table with columns 'MAC Address', 'Expiration', and 'Detected' is shown with 'No data available'. Below the table is the 'Notification Settings' section with fields for 'Purge Expired Entries' (set to 'Never'), 'Notification Frequency' (set to 'On First Detection'), 'Notification Method' (set to 'Alarm'), and 'Email Address'. Three callout boxes are present: 'Add MAC Address to Track' points to the 'Add' button; 'Import MAC Addresses' points to the 'Import' button; and 'On Every Detection On First Detection' and 'Email Alarm' point to the 'Notification Frequency' and 'Notification Method' dropdowns respectively.

Add MAC Address to Track

MAC Address

Expiration Never Date (MM/DD/YYYY)

Import MAC Addresses

CSV file:

[sample csv template](#)

Track Clients

Get notified when specific MAC addresses are detected on the network.?

Show

MAC Address	Expiration	Detected
No data available		

Notification Settings

Purge Expired Entries

Notification Frequency

Notification Method

Email Address

**On Every Detection
On First Detection**

**Email
Alarm**

Create policy for tracking one or more clients detected on the network

Unknown Users

The screenshot shows the 'Identify Unknown Users' interface with three overlapping windows:

- Identify Unknown Users:** The main window with the title 'Identify Unknown Users' and the instruction 'Assign client MAC addresses to usernames. ?'. It features a toolbar with 'Add', 'Import', 'Edit', and 'Remove' buttons. Below the toolbar is a table with columns for 'MAC Address' and 'Username', and the text 'No data available'. At the bottom are 'Save' and 'Cancel' buttons.
- Add User:** A smaller window with the title 'Add User' and two input fields: 'MAC Address' and 'Username'. It has 'Add' and 'Cancel' buttons at the bottom.
- Import Unknown User Identities:** A window with the title 'Import Unknown User Identities'. It contains a 'CSV file:' label, an empty text box, and a 'Browse...' button. Below these is a blue link 'sample csv template' and 'Import' and 'Cancel' buttons.

Black lines indicate the flow of data: one line connects the 'Add' button in the 'Identify Unknown Users' window to the 'Add User' window, and another line connects the 'Import' button in the 'Identify Unknown Users' window to the 'Import Unknown User Identities' window.

Assign username to client on network not authenticated via ISE.

IPv6 - Client Details

- IP Type – The type of client based on what IP addresses have been seen from the client. Possible options are IPv4, IPv6, or Dual-Stack which signifies a client with both IPv4 and IPv6 addresses.
- IPv6 Assignment Distribution - displays how the client acquired its IPv6 address. Possible assignment types are DHCPv6, SLAAC or Static, and Self Assigned.
- Global Unique – The most recent IPv6 global address used by the client. A mouse-over on the column reveals any additional IPv6 global unique addresses used by the client.
- Local Unique – The most recent IPv6 local unique address used by the client. Reveals any additional IPv6 global unique addresses used by the client.
- Link Local – The IPv6 address of the client which is self-assigned and used for communication before any other IPv6 address is assigned.
- IPv6 RA's Dropped – The number of router advertisements sent by the client and dropped at the access point. Can be used to track down clients that may be misconfigured or maliciously configured to act like an IPv6 router.

IPv6 Client Details

Client e8:06:88:51:5c:56 (Refreshed :2013-Apr-15, 17:39:05 PDT)

▼ **Client Attributes**

General

User Name **ekudey** ⓘ
IP Address **171.70.243.137**
MAC Address **e8:06:88:51:5c:56**
Vendor **Apple**
Endpoint Type **Unknown**
Client Type **Regular**
Media Type **Lightweight**
Mobility Status **Local**
Hostname **dhcp-171-70-243-137.cisco.c**
E2E **Not Supported**
802.11u Capable **No**
Power Save **ON**
CCX **Not Supported**

▼ **Client IPv6 Addresses**

IP Address	Scope	Assignment
fe80::ea06:88ff:fe51:5c56	Link Local	Self Assigned

Link local address derived from MAC address.

Monitoring Device Work Centre

Cisco Prime Infrastructure

Home
Design
Deploy
Operate
Report

Device Work Center

Device Group > ALL

ALL

Edit Delete Sync Groups & Sites Add Device

Device Name	Reachability	IP Address/DNS
<input type="checkbox"/> 3750-PHY-1	✔	10.0.252.3
<input checked="" type="checkbox"/> 3945-East-1.cisco.com	✔	192.168.152.1
<input type="checkbox"/> 3945-West-1	✔	10.0.103.1
<input type="checkbox"/> 7206-Core-1	✔	10.0.255.42
<input type="checkbox"/> 7206-Core-2	✔	10.0.255.52

Device Details
Configuration
Configuration Archive
Image

System

- Summary
- User Defined Field
- Memory Pools
- Environment
- Modules
- Physical Ports
- Interfaces

Summary
192.168.152.1 > System > Summary

General

IP Address/DNS Name: **192.168.152.1**

Device Name: **3945-East-1.cisco.com**

Device Type: **Cisco 3945E Integrated Services Router G2**

Up Time: **28 days 9 hrs 51 mins 21 secs**

Reachability Status: **Reachable**

Location

Contact: **nmtg**

Cisco Identity Capable: **No**

Location Capable: **No**

Device 360° Views

✔ 3945-East-1.cisco.com

192.168.152.1

WAN Aggregation

Cisco 3945E Integrated Services Router G2

up for 28 days 9 hrs 51 mins 25 secs

OS Type **IOS**

OS Version **15.1(4)M1**

Last Config Change **November 1, 2013 2:15:47 PM PDT**

Last Inventory Collection **February 24, 2014 10:02:59 PM PST**

CPU Utilization

11.00% ▼-1.00%

Low: 10.00% High: 12.00% Average: 11.00%

Memory Utilization

14.00% 0.00%

Low: 14.00% High: 14.00% Average: 14.00%

I/O

Alarms Modules **Interfaces** Neighbors

Op. Status	Admin S...	Interface	Top 3 Applications
✔	✔	Backplane-GigabitEthernet0/4	Not Available
✔	✔	GigabitEthernet0/0	Not Available
✔	✔	GigabitEthernet0/1	Not Available
✔	✔	GigabitEthernet0/2	Not Available
✔	✔	GigabitEthernet0/3	Not Available
✔	✔	GigabitEthernet4/0	Not Available

Inventory

Software Version: **15.1(4)M1**

Model No.: **CISCO3945-CHASSIS**

Workflow Status

Support Cases | Alarm Browser | Alarm Summary

197

VLAN Information

VLANs
10.5.10.2 > Layer 2 > VLANs

VLAN ID	VLAN Name	
15	3850-MGMT	Ethernet
10	data	Ethernet
12	Data	Ethernet
1	default	Ethernet
1002	fddi-default	FDDI
1004	fddinet-default	FDDI Network Entity Title
11	Phns	Ethernet
1003	token-ring-default	Other
1005	trnet-default	Other
100	VLAN0100	Ethernet
20	voice	Ethernet

Per VLAN details – all VLANs configured per switch.

Spanning Tree – Details/Monitoring

Per VLAN configured parameters: single pane of glass view of all VLANs configured on switch

Spanning Tree Details

10.5.10.2 > Layer 2 > Spanning Tree > VLAN0001

VLAN ID	Root Path Cost	Designated Root	Bridge Priority	Root Bridge Priority	Max Age (sec)	Hello Interval (sec)	Forward Delay (sec)
1	4	00:1b:0c:02:ab:80	32769	32769	20	2	15

Per VLAN status: operational details for troubleshooting

VLAN Interfaces

Monitor > Switches > 172.20.224.54 > Interfaces > VLAN Interfaces

Port Name	VLAN ID	Operational Status	Admin Status	Port Type	Maximum Speed (Mbps)	MTU
Vlan1	1	●	●	Propvirtual	1000	1500
Vlan10	10	●	●	Propvirtual	1000	1500






Monitoring - Alarms and Events

What Are Events?

- An occurrence of a condition (or change in condition) in the network managed by PI
- Not necessarily generated for every condition but could be a result of a pattern or threshold match by the WLC
- Events may not be useful in their raw form (unless troubleshooting, for example) and usually need further processing

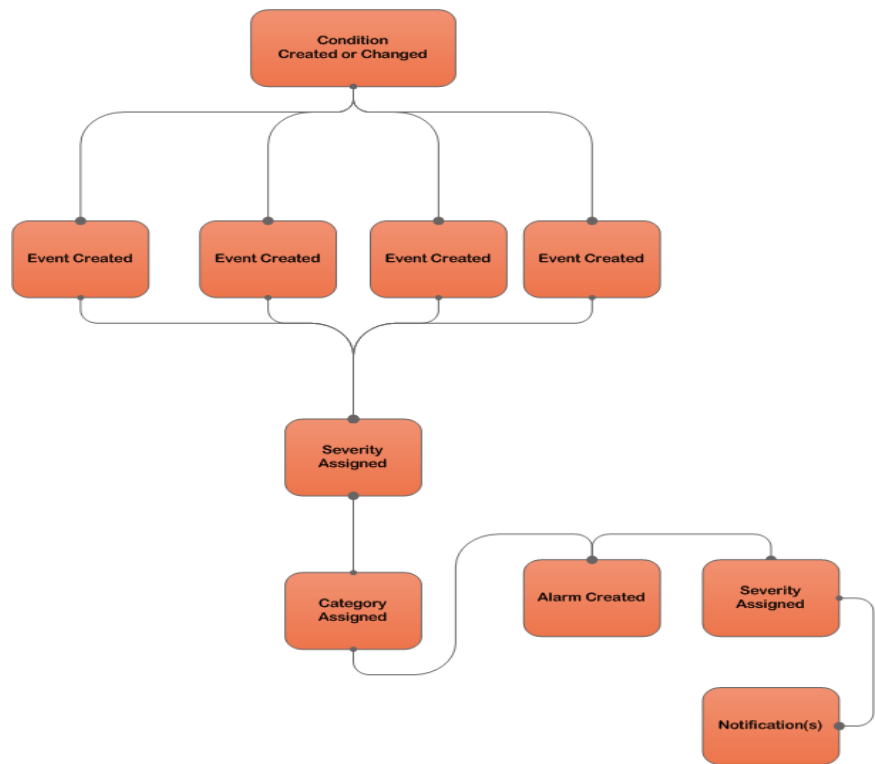
What Are Alarms?

- Correlated events result in alarms (PI allows looking up event history for alarms)
- Both Alarms and Events are categorised by severities

- Critical 
- Major 
- Minor 
- Warning 
- Informational 

Notifications, Alarms and Events

- A notification is triggered when a fault occurs in the network.
- An event is created, based on the notification.
- An alarm is created after checking if there is no active alarm corresponding to this event.
- Events can be trap, syslog or threshold violation
- Conventional actions are available :
 - Filter
 - Clear
 - Acknowledge
 - Annotate
- Troubleshooting tools are available :
 - ping, traceroute
 - show commands



PI - Alarms and Events

- Single page view of alarms and events for wired and wireless
- Persistent alarm summary and browser
- Quick and Advanced Filtering
- Advanced search capabilities

Wireless Controller

Alarms Events Syslogs

Selected 0 | Total 1927

Troubleshoot Show Events in last 8 hours

Description	Failure Source	Timestamp	Severity	Category	Condition	Correla
▶ Rogue AP '84:4b:f5:b4:f8:32' with SSID 'HP-Print-32-Las...	Rogue AP 84:4b:f5:b4:f8:32	February 24, 2014 10:00:49...	Minor	Rogue AP	Unclassified Ro...	✓
▶ Rogue AP 'f4:ea:67:12:7a:61' with SSID '' and channel n...	Rogue AP f4:ea:67:12:7a:61	February 24, 2014 10:00:49...	Minor	Rogue AP	Unclassified Ro...	✓
▶ Rogue AP '3c:ce:73:f9:b3:4d' is no longer detected; it w...	Rogue AP 3c:ce:73:f9:b3:4d	February 24, 2014 10:00:35...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Rogue AP '3c:ce:73:f9:b3:4d' is no longer detected; it w...	Rogue AP 3c:ce:73:f9:b3:4d	February 24, 2014 10:00:35...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Port '5' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 10:00:05...	Critical	Controller	Link down	✓
▶ Port '6' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 10:00:05...	Critical	Controller	Link down	✓
▶ Port '7' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 10:00:05...	Critical	Controller	Link down	✓
▶ Port '8' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 10:00:05...	Critical	Controller	Link down	✓
▶ Port '4' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 10:00:05...	Critical	Controller	Link down	✓
▶ Rogue AP 'f4:ea:67:0a:e0:70' with SSID 'blizzard' and ch...	Rogue AP f4:ea:67:0a:e0:70	February 24, 2014 9:57:51 ...	Minor	Rogue AP	Unclassified Ro...	✓
▶ Rogue AP 'f4:ea:67:0a:c6:8d' is no longer detected; it w...	Rogue AP f4:ea:67:0a:c6:8d	February 24, 2014 9:55:41 ...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Port '5' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 9:55:03 ...	Critical	Controller	Link down	✓
▶ Port '6' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 9:55:03 ...	Critical	Controller	Link down	✓
▶ Port '7' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 9:55:03 ...	Critical	Controller	Link down	✓
▶ Port '8' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 9:55:03 ...	Critical	Controller	Link down	✓
▶ Port '4' is down on device '192.168.152.11'.	Port 192.168.152.11/TenGigabitEt...	February 24, 2014 9:55:03 ...	Critical	Controller	Link down	✓
▶ Rogue AP 'f4:ea:67:12:7a:60' is no longer detected; it w...	Rogue AP f4:ea:67:12:7a:60	February 24, 2014 9:54:03 ...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Rogue AP 'c8:f9:f9:4c:29:41' with SSID '' and channel nu...	Rogue AP c8:f9:f9:4c:29:41	February 24, 2014 9:51:54 ...	Minor	Rogue AP	Unclassified Ro...	✓
▶ Rogue AP 'f4:ea:67:12:7a:63' is no longer detected; it w...	Rogue AP f4:ea:67:12:7a:63	February 24, 2014 9:51:06 ...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Rogue AP 'f4:ea:67:12:7a:61' is no longer detected; it w...	Rogue AP f4:ea:67:12:7a:61	February 24, 2014 9:51:06 ...	Cleared	Rogue AP	ROGUE_AP_RE...	✓
▶ Rogue AP '70:10:5c:7c:2e:bd' with SSID '5760' and chan...	Rogue AP 70:10:5c:7c:2e:bd	February 24, 2014 9:50:30 ...	Minor	Rogue AP	Unclassified Ro...	✓

Workflow Status 0 0 0 | Support Cases | Alarm Browser | Alarm Summary 199 2 190

Alarms – Layout and Search

Alarms sorted by Categories and Severities are hyperlinked to allow quick drill-down

On-demand refresh and view customisation

	Critical	Major	Minor
Alarm Summary	311	1164	964
AP	11	0	12
Controller	24	1	0
Coverage Hole	0	0	0
Mesh Links	0	19	12
Mobility Service	1	0	3
NCS	0	1	6
Performance	0	0	57
Rogue AP	0	1143	866
Security	275	0	8

Alarm Browser | Alarm Summary 311 1164 964

Persistent Alarm Summary toolbar. Expands to display alarm categories.

Alarm Browser

Expandable view for each alarm for details

Provides filtered view of alarms for wired and wireless

The screenshot displays the Alarm Browser interface. At the top, there are action buttons: Change Status, Assign, Annotation, Delete, Email Notification, and Troubleshoot. A search bar on the right shows 'Selected 0 | Total 3665'. Below this is a table of alarms with columns for Severity, Message, Status, Failure Source, Timestamp, Owner, Category, and Condition. The table contains three rows of alarm data.

Severity	Message	Status	Failure Source	Timestamp	Owner	Category	Condition
Minor	Rogue AP '00:27:0d:08:7a:8e' wit...	Not Acknowledg...	Rogue AP 00:27:0d:08:7a:8e	April 15, 2013 10:49:06 PM PDT	japitche	Rogue AP	Unclassified Rog...
Critical	IDS 'Deauth flood' Signature attac...	Not Acknowledg...	WLAN Controller sjc14-wl-wlc1/17...	April 15, 2013 11:33:20 PM PDT	japitche	Security	Signature attack
Major	Rogue AP 'c4:7d:4f:53:38:60' with...	Not Acknowledg...	Rogue AP c4:7d:4f:53:38:60	April 15, 2013 10:51:09 PM PDT	japitche	Rogue AP	Malicious Rogue
Critical	IDS 'NULL probe resp 2' Signature...	Not Acknowledg...	WLAN Controller sjc14-wl-wlc1/17...	April 15, 2013 2:22:56 PM PDT	japitche	Security	Signature attack

The 'General Info' section for the selected alarm is expanded, showing the following details:

- Signature Name: **NULL probe resp 2**
- Signature Type: **Standard**
- Reported From: **WLAN Controller sjc14-wl-wlc1/171.71.128.75**
- Attack active at: **1 AP(s)**
- Observer MAC List: **c4:0a:cb:88:80:30,64:d9:89:42:26:60,64:d9:89:42:45:b0,64:d9:89:42:4b:b0,64:d9:89:42:44:50,64:d9:89:42:41:d0**
- Owner: **japitche**
- Acknowledged: **false**
- Category: **Security**
- Created: **April 1, 2012 3:40:22 AM PDT**
- Modified: **April 15, 2013 2:22:56 PM PDT**
- Severity: **Critical**
- Previous Severity: **Critical**

The 'Messages' section shows a message: **IDS 'NULL probe resp 2' Signature attack cleared by 'SJC14-31B-AP5' protocol '802.11b/g' on Controller 'SJC14-31B-AP5'. The Signature description is 'NULL Probe Response - Controller Name: sjc14-wl-wlc1'. This Signature was detected by 1 APs.**

The 'Annotations' section shows a table of messages:

Message	Posted By	Date/Time
Reviewed and thr...	japitche	March 8, 2013 9:02:...
Alarm assigned	japitche	March 8, 2013 9:02:...

The 'Description' section shows: **NULL Probe Response - No SSID element**

Application Visibility and Control (AVC)

- AVC on a controller can classify and take action on 1039 different applications
- Two Actions, either DROP or MARK, are possible on any classified application
- A maximum of 16 AVC profiles can be created on a WLC
- Each AVC Profile can be configured with a maximum of 32 rules
- Same AVC profile can be mapped to multiple WLANs. However, one WLAN can only have one AVC Profile
- AVC is supported on WLANs configured for central switching only
- Any application, which is not supported or recognised by the AVC engine on WLC, is captured under the bucket of UNCLASSIFIED traffic

Application Visibility and Control Assurance Licence

Cisco Prime Infrastructure Virtual Domain ROOT-DOMAIN | prime

Home Design Deploy Operate Report Administration Workflows

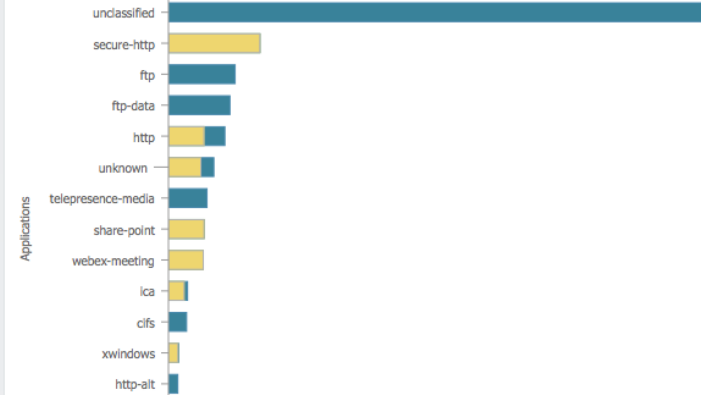
Overview Incidents Performance **Detail Dashboards**

Site Device Interface Application Voice/Video End User Experience WAN Optimization

Filters *Site London Branch *Time Frame Past 24 Hours Application All Applications Network Aware All

Top N Applications

Rate | Volume

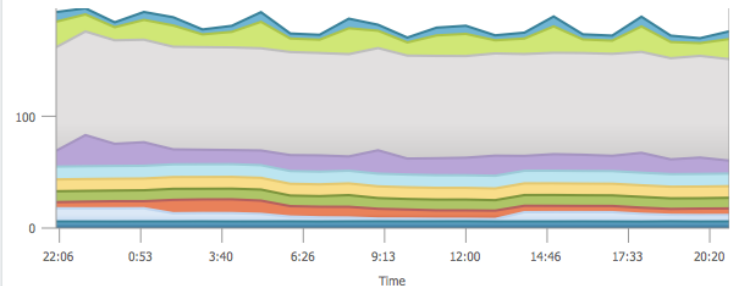


Top Application Traffic Over Time

Applications | Application Categories

Rate | Volume

Megabits/sec



2014 February 25, 03:01:

Traffic Wireless Wired

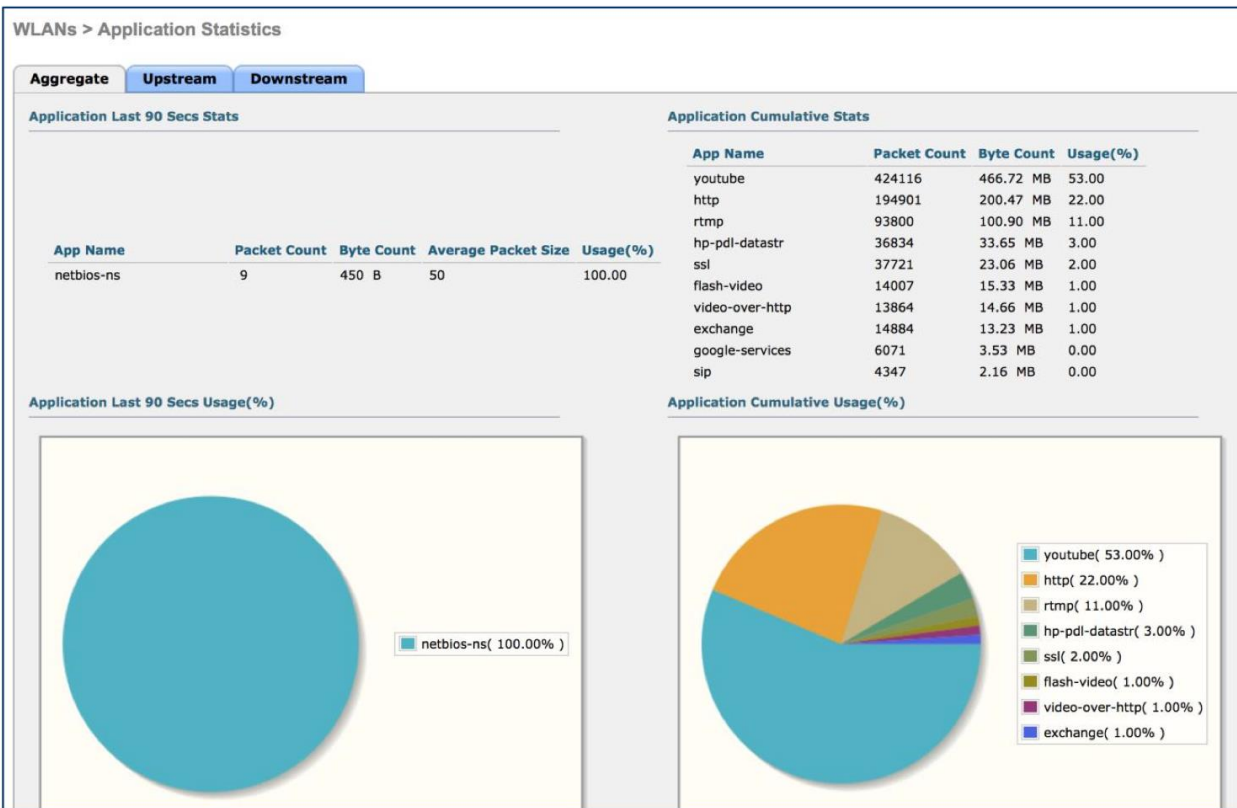
2014 February 25,

Traffic - Wired or Wireless traffic. Add the Access Switch or Controller where the client is connected in Device Work Center

Wired - Wired Traffic from clients identified by Access Switch

Wireless - Wireless Traffic from clients identified by Wireless Controller

AVC – Wireless LAN Controller GUI

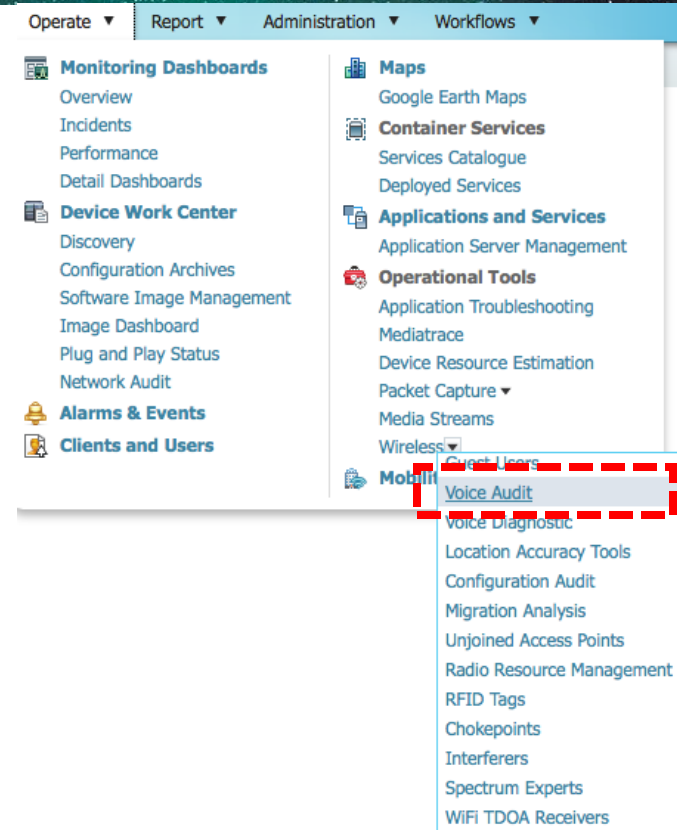




Operational Tools

Operational Tools - Voice Audit Tool

- Allows auditing current **network configuration** from a VoWLAN deployment perspective
- Use default rules and thresholds based on Cisco best practices
- Ability to customise the rules to match your network and requirements
- Provides a simple report with a list of configuration gaps



Voice Audit - Example

Voice Audit
Operate > Operational Tools > Wireless > Voice Audit

Save Save and Run

Controllers Rules Report

Run audit on:

- ✓ All Controllers
- A Floor Area
- A Single Controller

Voice Audit Report
Tools > Voice Audit Report

Save Save and Run

Controllers Rules Report

VoWLAN SSID

Rule List

- ✓ VoWLAN SSID
- ✓ CAC: 7920 AP
- ✓ CAC: 7920 Client
- ✓ DHCP Assignment
- ✓ MFP Client
- ✓ Platinum QoS
- ✓ Non Platinum QoS
- ✓ WMM
- ✓ CCKM
- ✓ Aggressive Load Balancing
- ✓ Aironet IE
- ✓ TSM
- ✓ DFS

Rule Details

Description
Check that QoS is set to Platinum (Voice) for VoWLAN

Rule validity
User defined VoWLAN SSID

Customisable Rules

Voice Audit Report
Tools > Voice Audit Report

Save Save and Run

Controllers Rules Report

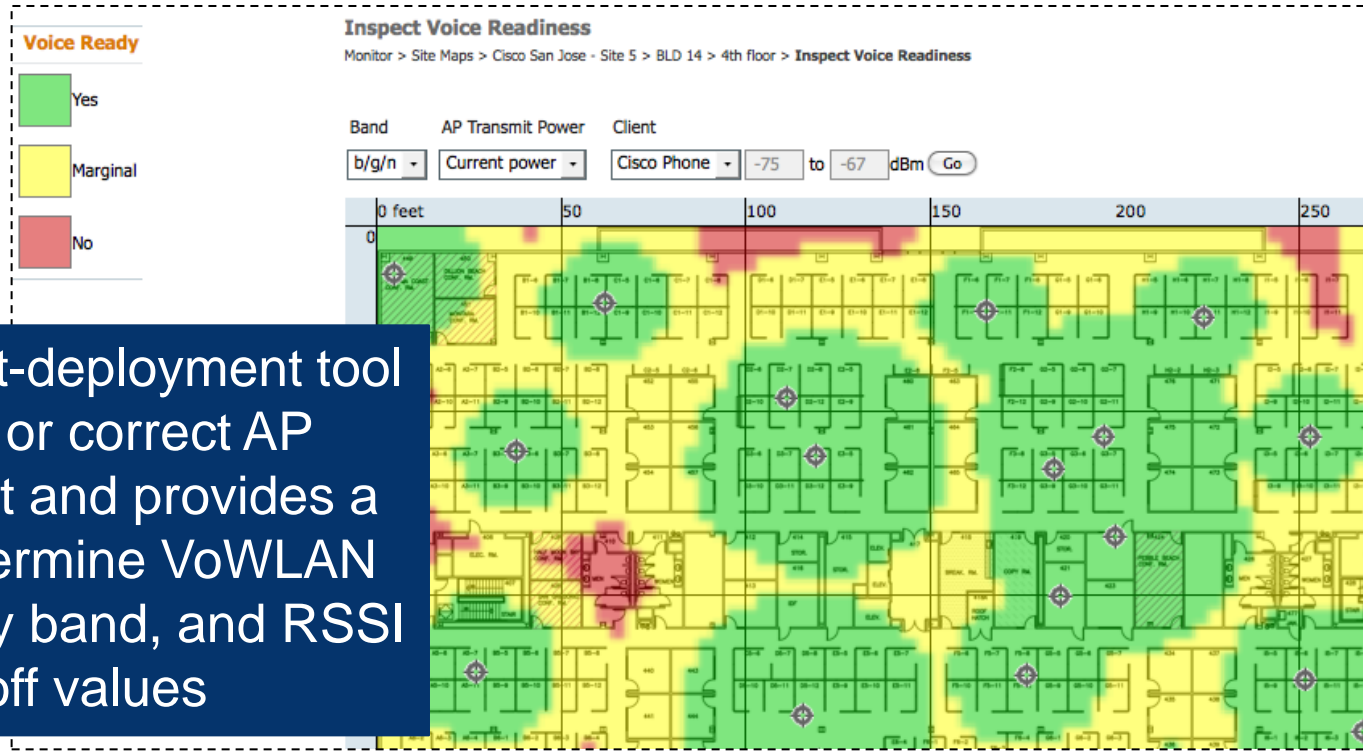
Audit Status	Start Time	End Time	#Total Devices
Complete	2012-Mar-26, 06:42:44 PDT	2012-Mar-26, 06:42:45 PDT	5

IP Address	Rule	Result	Details
171.71.122.80	VoWLAN SSID	Skipped	Rule skipped since it was invalid
171.71.122.80	CAC: 7920 AP	Skipped	Rule skipped since it was invalid
171.71.122.80	CAC: 7920 Client	Skipped	Rule skipped since it was invalid
171.71.122.80	DHCP Assignment	Skipped	Rule skipped since it was invalid
171.71.122.80	MFP Client	Skipped	Rule skipped since it was invalid

Voice Audit Tool Report

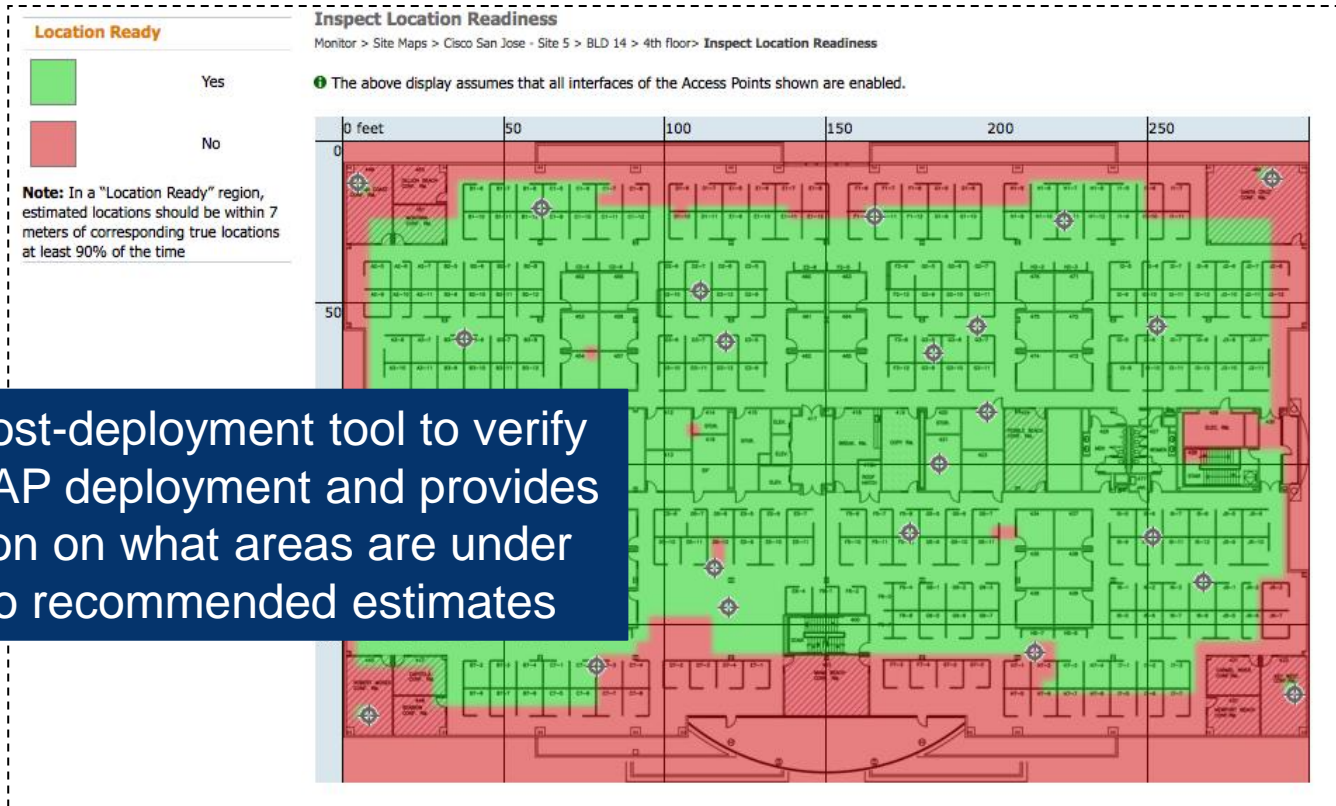
Voice Readiness Tool - Example

Launch from Floor View in Maps



Simple, post-deployment tool to verify or correct AP deployment and provides a way to determine VoWLAN readiness by band, and RSSI cutoff values

Location Readiness - Example



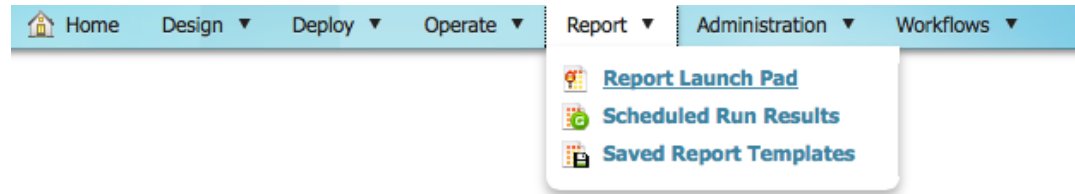
Simple, post-deployment tool to verify or correct AP deployment and provides information on what areas are under the Cisco recommended estimates



Reporting

Reporting

- Report LaunchPad
- Report Customisations
 - Multi-Level Filtering
 - Customising Report Output
 - Multi-Level Sorting in Report Output
- Report Scheduling
- PI + ISE Reporting



Report LaunchPad

Report LaunchPad – Easy Drill-Down

Autonomous AP

- Autonomous AP Memory and C...
- Autonomous AP Summary
- Autonomous AP Tx Power and...
- Autonomous AP Uptime
- Autonomous AP Utilization
- Busiest Autonomous APs

CleanAir

- Air Quality vs Time
- Security Risk Interferers
- Worst Air Quality APs
- Worst Interferers

Client

- Busiest Clients
- CCX Client Statistics
- Client Count
- Client Sessions
- Client Summary
- Client Traffic
- Client Traffic Stream Metrics
- Dormant Clients
- Mobility Client Summary

Busiest Clients

Reports > Report Launch Pad > Client > Busiest Clients

	Report Title	Report Type	Scheduled	
<input type="checkbox"/>	Ian Client Report	Busiest Clients	Disabled	New
<input type="checkbox"/>	haidertest	Busiest Clients	Disabled	New
<input type="checkbox"/>	kukku	Busiest Clients	Disabled	New
<input type="checkbox"/>	leksan rappari	Busiest Clients	Disabled	New
<input type="checkbox"/>	tonparke_Busiest_Client	Busiest Clients	Disabled	New

New Enable Schedule Disable Schedule Delete

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 Authentication Summary

MSE Analytics

- Client Location
- Client Location
- Device Count

Mesh

- Alternate Parent



Report Customisation

Busiest Clients : Ian Client Report

Reports > Report Launch Pad > Client > Busiest Clients > Busiest Clients Report Details

Run Save Run and Save Save and Export Save and Email Cancel Delete

Settings

Report Title: Ian Client Report

Report By: Floor Area

Report Criteria: Cisco San Jose - Site 5 > BLD 14 > 1st floor Edit

Connection Protocol: All Clients

Reporting Period: Last 7 Days From : : To : :

Show: Up to records

Customize Report: Customize Customize the data for this report

Schedule

Scheduling: Enable

Export Format: CSV

Create Custom Report

Custom Report Name: Busiest Clients

Available data fields

- Global Unique
- Unique Local
- Link Local
- On Device
- Bytes Sent (MB)
- Bytes Received (MB)
- Packets Sent
- Packets Received

Data field sorting

Sort by: Throughput Ascending Descending

Then by: Utilization (%) Ascending Descending

Then by: Bytes Received (MB) Ascending Descending

Then by: Bytes Sent (MB) Ascending Descending

* Only reports in tabular format can be sorted.
* Only fields that can be sorted appear in the selection menus.

After clicking Apply, click Save on the Report Details page to save the custom report settings. Apply Reset Cancel

Run report immediately or schedule to be run one-time only or periodically. Save report in user-specified destination, or mailed to one or more recipients.

Customise reports: select data most relevant for each report.

Client Profiling

PI 1.4 + WLC 7.5 Client Profiling

- Client profiling **without** ISE
- WLC profiling of devices based on HTTP/DHCP to identify endpoint devices
- Configure device-based policies and enforce per user or per device policy on the network
- WLC also displays statistics based on per user or per device end points and policies applicable per device.

Profiling based on

- device Type (iPad iPhone, Android, etc.), user name/password, EAP method, time of day (when end point is allowed on the network), etc.

Configure > Controller Template Launch Pad > WLANs > WLAN Configuration > New Controller Template

General Security QoS **Advanced** HotSpot Policy Configuration

Client Exclusion [?] Enable
Timeout Value (secs)
Passive Client [?] Enable
Maximum Clients [?]

Off Channel Scanning Defer

Scan Defer Priority 0 1 2 3 4 5 6 7
Scan Defer Time (ms)

DTIM Period [?]

802.11a/n (1-255) (ms)
802.11b/g/n (1-255) (ms)

mDNS Configuration

mDNS Snooping Enable
mDNS Profile

DHCP Server Override
DHCP Address Assignment Required

Management Frame Protection (MFP)

MFP Signature Generation [?] Enable
MFP Client Protection [?]
MFP Version 1

Load Balancing and Band Select

Client Load Balancing Enable
Client Band Select Enable

NAC

NAC State

Voice

Media Session Snooping Enable
KTS based CAC Enable

Client Profiling

DHCP Profiling [?] Enable
HTTP Profiling [?] Enable

Local Client Profiling

Local DHCP Profiling [?] Enable
Local HTTP Profiling [?] Enable

Enable client
profiling via
WLAN template

Define rule
for profiling
device

Create
action for
device
category

New Controller Template

Configure > Controller Template Launch Pad > WLANs > Policy Configuration > **New Controller Template**

Policy Name

policy-1

Rules

Policy Role

EAP Type

Eap-tls

Device Type

Actions

VLAN

0

ACL

None

QOS

None

Session Timeout

1800

Sleeping Client Timeout

12

Save

Cancel

Device Type selector

- Vista-Workstation
- Windows7-Workstation
- Windows8-Workstation
- WindowsXP-Workstation
- Xandros-Workstation
- CentOS-Workstation
- Debian-Workstation

Clear Selections

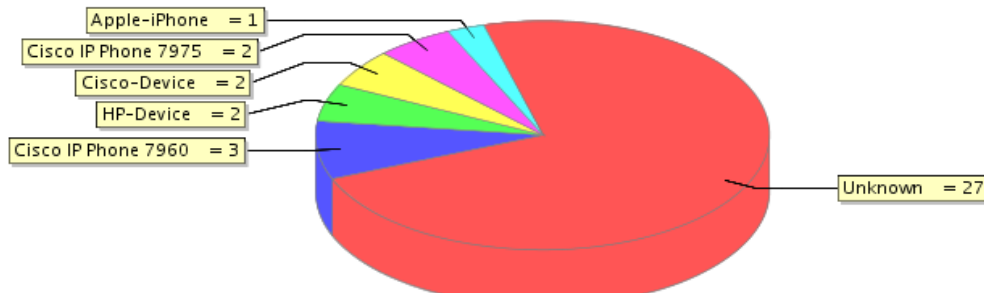
OK

Cancel

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 ⓘ		
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

New
New
New



Identity Services Engine

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>

Key Takeaways

- PI provides full lifecycle management for wired/wireless infrastructure and endpoints
- Wired/wireless access – infrastructure and endpoints – need to be managed together
- PI builds on the features/functionality of WCS/NCS and adds wired management
- Provides license and data migration from WCS/NCS to PI

Final Thoughts

- Get hands-on experience with the Walk-in Labs located in World of Solutions,
- Come see demos of many key solutions and products in the main Cisco booth
- Visit www.ciscoLive365.com after the event for updated PDFs, on-demand session videos, networking, and more!
- Follow Cisco Live! using social media:
 - Facebook: <https://www.facebook.com/ciscoliveus>
 - Twitter: <https://twitter.com/#!/CiscoLive>
 - LinkedIn Group: <http://linkd.in/CiscoLI>

Maths Quiz

- Can you find a number, under 3000, which
- When divided by 2 leaves a remainder of 1;
- When divided by 3, a remainder of 2;
- When divided by 4, a remainder of 3;
- When divided by 5 a remainder of 4;
- When divided by 6 a remainder of 5;
- When divided by 7 a remainder of 6;
- When divided by 8 a remainder of 7;
- When divided by 9 a remainder of 8;
- When divided by 10 a remainder of 9?



Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2014 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 21 March 12:00pm - 2:00pm



Learn online with Cisco Live!

Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



CISCO TM