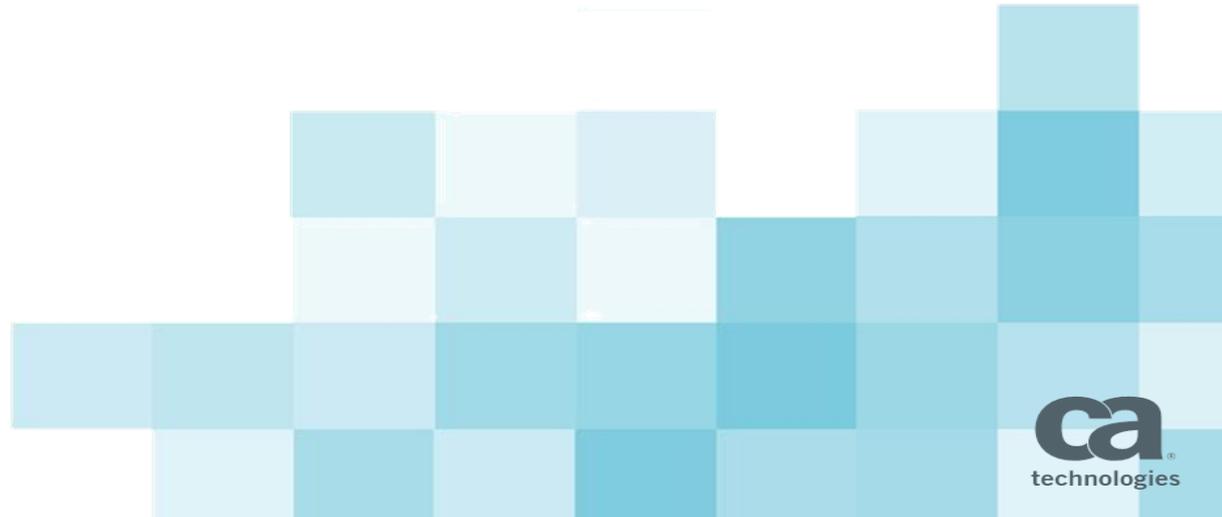


CA Spectrum Community Webcast: Wireless Monitoring with CA Spectrum

Nagesh Jaiswal

19th July 2017



Agenda

1

VALUE PROPOSITION

2

OVERVIEW

3

FEATURES

4

DEMO

5

ROADMAP

6

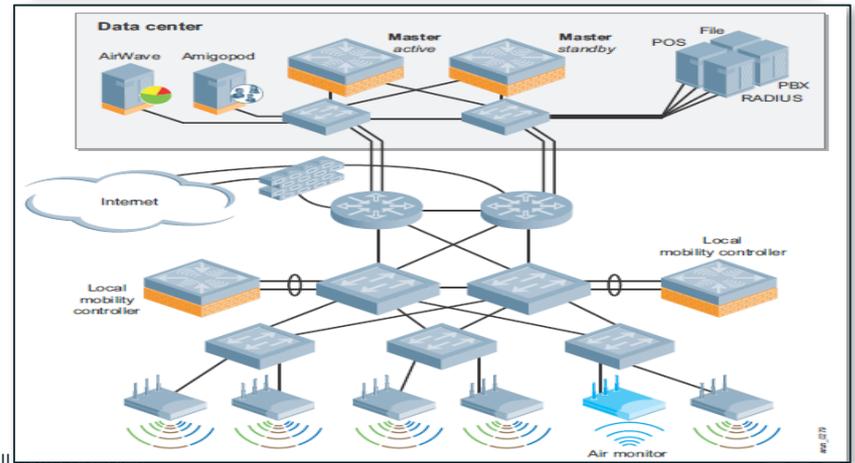
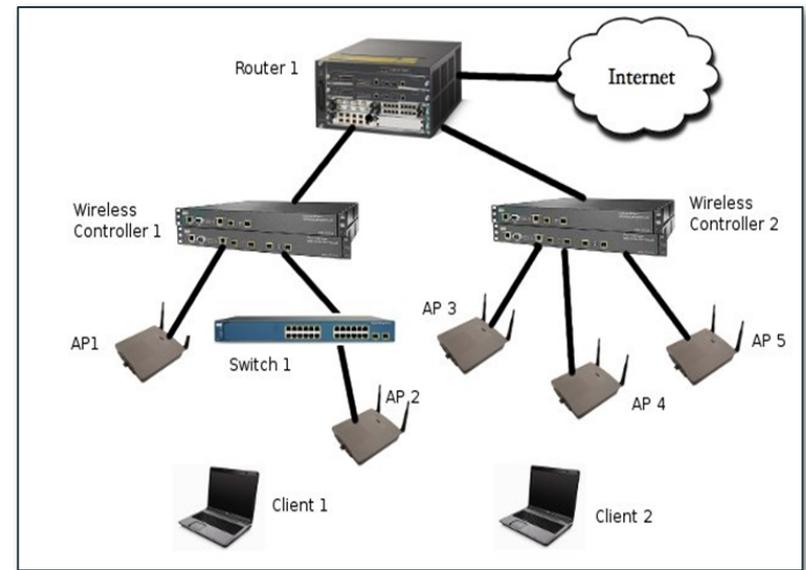
QUESTIONS

Value Proposition

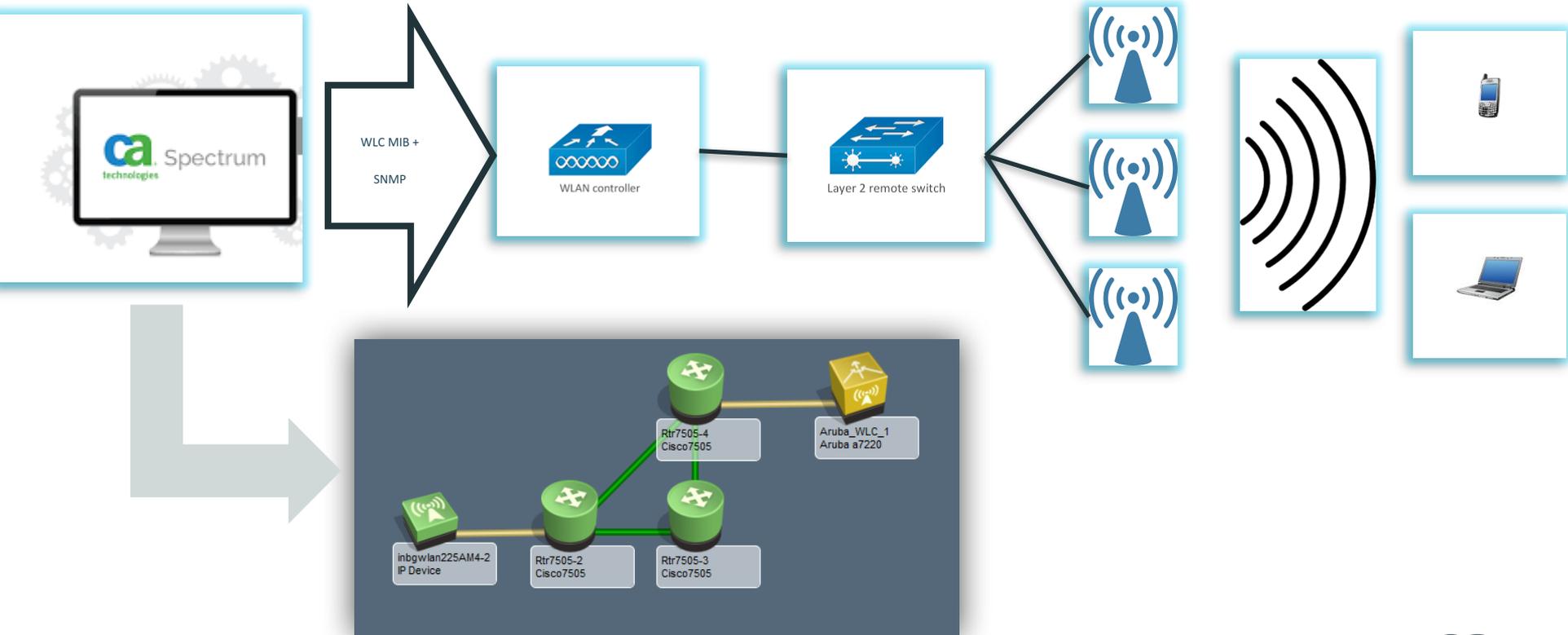
- Brings your wireless network logically into spectrum management, without treating it as an isolated technology
- Gives network operators the tools to manage and control the wireless network—which helps reduce outages and make your wireless network as stable as your wired network
- Specifically designed for a proactive approach to managing your wireless network
- Vendor Agnostic

Overview

- Discover controller & model those devices with the associated APs
- Connectivity between the APs & WLC device ports
- SpectroServer communicates with WLC devices using the SNMP protocols
- Fault Isolation & RCA:
 - WLC goes down
 - Up-stream device goes down



How it works?



Discovery Workflow

- Create by IP
 - Controller(s)/AP(s) will be modelled as SNMP, individual entities with no connections discovered in between

- WLC Manager
 - WLC Manager > Information Tab > Configuration > "Run Access Points discovery"

- Discovery Console
 - Tools > Utilities > Discovery Console... > Create & Select Configuration > Modeling Options... > "Discover Access Points" checkbox

| Entry List in Discovery Console | "Model Access Points" disable | "Model Access Points" enable |
|--|---|---|
| Only Controller(s) | Controller(s) are discovered and modeled alone. | Controllers are modelled as SNMP. AP's are modelled as Pingable with no associations with controller(s). |
| Controller(s) & APs | Controller(s) & APs are modelled as SNMP with no associations. | Controller(s) & APs given in Discovery List are modelled as SNMP devices. Remaining APs under the Controller(s) are modelled as Pingable with no associations with controller(s). |
| Controller(s) with L2/L3 devices. | Controller(s) & L2/L3 devices are modelled as SNMP with connections discovered between them. No APs will be discovered. | Controller(s) & L2/L3 devices are modeled as SNMP devices. APs are modeled as Pingable with connections discovered between them. |
| Controller(s) with L2/L3 devices and APs | Controller(s), L2/L3 devices & given APs are modeled as SNMP with connections discovered. | Controller(s), L2/L3 devices & given APs are modeled as SNMP. Remaining APs under the Controller(s) are modelled as Pingable with connections discovered between them |

Alarms, Events & Traps

- Supports Traps provided by WLC MIB
- All alarms on AP's are asserted on respective WLC

The image displays two screenshots from a network management system. The top screenshot shows the 'Component Detail' for a Cisco 8500 WLC, highlighting a critical alarm: 'WIRELESS CLIENTS CONNECTED TO WLC CONTROLLER EXCEEDED CRITICAL THRESHOLD'. The alarm details include the severity (Critical), impact (0), and a probable cause: 'Total number of wireless clients connected to WLC Controller exceeded the critical threshold limit.' The interface also shows the number of clients connected (1412) and the maximum supported (1466).

The bottom screenshot shows a list of 167 events from October 19, 2015, at 6:27:44 AM IST. The events are categorized by severity (Minor and Major) and include details such as the event name, description, and the system that generated the event.

| Severity | Created On | Name | Event | Created By | Cleared On | Cleared By |
|----------|----------------------------|--------------------|--|------------|----------------------------|------------|
| Minor | Oct 19, 2015 10:09:04 A... | Sim23998:Sim238... | WIRELESS CLIENTS CONNECTED TO WLC CONTROLLER EXCEEDED CRITICAL THRESHOLD | System | Oct 19, 2015 10:14:04 A... | System |
| | Oct 19, 2015 10:08:44 A... | Sim23998:Sim238... | Access Points Minor Threshold: 70% Connected : 1876 Maximum Supported : 2396 | System | | |
| | Oct 19, 2015 10:08:24 A... | Sim23998:Sim238... | Auto-discovery mapping process finished on model Sim23998:Sim23846:10.253.161.244 of type Rtr_Cisco | System | | |
| | Oct 19, 2015 10:07:52 A... | Sim23998:Sim238... | Auto-discovery mapping process started on model Sim23998:Sim23846:10.253.161.244 of type Rtr_Cisco | System | | |
| | Oct 19, 2015 10:07:52 A... | Sim23998:Sim238... | Auto-discovery mapping process can not run on model Sim23998:Sim23846:10.253.161.244 of type Rtr_Cisco because another mapping process is currently running. So it is queued | System | | |
| Major | Oct 19, 2015 10:04:03 A... | Sim23998:Sim238... | The number of Access Points connected to WLC Controller Sim23998:Sim23846:10.253.161.244 exceeded the major threshold limit. | System | Oct 19, 2015 10:09:04 A... | System |
| | Oct 19, 2015 10:03:17 A... | Sim23998:Sim238... | Access Points Major Threshold: 80% Connected : 1875 Maximum Supported : 2227 | System | | |
| | Oct 19, 2015 10:03:17 A... | Sim23998:Sim238... | Auto-discovery mapping process finished on model Sim23998:Sim23846:10.253.161.244 of type Rtr_Cisco | System | | |

Others

- Support for maintenance mode
- Support for AP Migration
- Supports Cisco WLC FT Scenarios (AP SSO)
- Support for DHCP enabled AP's

The screenshot shows a network management interface with two main panels. The top panel is an event log titled "7 event(s) from 13-Oct-2015 B40B35 EDT - now". It contains a table with columns: Severity, Created On, Name, Event, Created By, and Cleared On. The events are related to WLC configuration changes and agent status. The bottom panel shows "Component Details" for a Cisco WLC (sn24298-wc-fm031-01). It includes a table with columns: Name, ID, Type, Name, and Value. The table lists various attributes like agent attributes, activation status, and agent IP addresses.

| Severity | Created On | Name | Event | Created By | Cleared On |
|----------|--------------------------|---------------------|--|------------|------------|
| Info | 13-Oct-2015 08:00:11 EDT | sn24298-wc-fm031-01 | Access Point '104h-qj-392-1107' has migrated from WLC 'sn24298-wc-fm031-01' to WLC 'sn24298-wc-fm031-01' | System | |
| Info | 13-Oct-2015 08:00:56 EDT | sn24298-wc-fm031-01 | Device or SNMP agent on Device sn24298-wc-fm031-01 of type GrCiscoDev has been rebooted. | System | |
| Info | 13-Oct-2015 08:03:30 EDT | sn24298-wc-fm031-01 | Model sn24298-wc-fm031-01 of type GrCiscoDev has been contacted. | System | |
| Info | 13-Oct-2015 08:03:30 EDT | sn24298-wc-fm031-01 | The condition causing the loss of contact on the device model (name = sn24298-wc-fm031-01, type = GrCiscoDev) ... | System | |
| Info | 13-Oct-2015 08:03:30 EDT | sn24298-wc-fm031-01 | The condition causing the loss of contact on the device model (name = sn24298-wc-fm031-01, type = GrCiscoDev) ... | System | |
| Info | 13-Oct-2015 08:03:29 EDT | sn24298-wc-fm031-01 | sn24298-wc-fm031-01 has started participating in event correlation, done on sn24298-wc-fm031-01, wlc_ssdDomain (brande 04021463). | System | |
| Info | 13-Oct-2015 08:03:29 EDT | sn24298-wc-fm031-01 | The interfaces of device sn24298-wc-fm031-01 of type GrCiscoDev are being configured for the first time. | System | |
| Info | 13-Oct-2015 08:03:20 EDT | sn24298-wc-fm031-01 | A model has been created. The model is sn24298-wc-fm031-01 of type GrCiscoDev, modelId is 04021463, and device is sn24298-wc-fm031-01. | System | |

| Name | ID | Type | Name | Value |
|--------------------------------|----------|--------------|---------------------|-------|
| agent_attr | 0:1049 | Integer | sn24298-wc-fm031-01 | |
| acknowledge | 0:1346 | Boolean | | |
| activation_status | 0:10073 | Integer | | |
| aliasDataIdAp | 0:1142F | Model Handle | | |
| aliasDataIdApMap | 0:1306B | Integer | | |
| agent_port | 0:10023 | Integer | | |
| agentApAssocIdAssocIdApCount | 0:21142 | Integer | | |
| agentApCoverageOfLeafTrapCount | 0:215166 | Integer | | |

The screenshot shows a network topology diagram titled "Contents: Universe of Type Universe". It displays a central Cisco Catalyst switch (sn24298-wc-fm031-01) connected to several Cisco WLCs (sn24298-wc-fm031-01) and APs (sn24298-wc-fm031-01). The diagram is zoomed in to show the details of a Cisco WLC component. The component details panel shows the "Condition" as "Maintenance" and the "System Up Time" as "22 Days + 09:56:42". It also lists various attributes like "Contact Status", "Network Address", "Secure Domain", "MAC Address", "Last Successful Poll", and "In Maintenance".

| Condition | Maintenance |
|--------------------------------|---|
| Contact Status | Established |
| Network Address | 10.241.119.2 set |
| Secure Domain | Directly Managed |
| MAC Address | 11:22:03:04:05:07 |
| Last Successful Poll | Oct 19, 2015 11:12:10 AM IST |
| In Maintenance | Yes set Schedule... |
| Assigned Maintenance Schedules | |

| System Up Time | 22 Days + 09:56:42 |
|-------------------|---|
| System Name | Cisco WISM set |
| Contact | DC1455940_SLS-PL4_UV_Suplt= set |
| Device Location | Fm_Eschb_Landstr.100_E_Sheher set |
| Value When Yellow | 1 set |
| Value When Orange | 3 set |
| Value When Red | 7 set |
| Notes | set |

Control and Proactive Monitoring

- Threshold Configuration
- Threshold violation alarms

Alarm Details | Information | Impact | Host Configuration | Root Cause | Interfaces | Performance | Alarm History | Neighbors | Events | Path View

USERS CONNECTED TO ACCESS POINT EXCEEDED CRITICAL THRESHOLD
 Nov 18, 2015 7:16:45 AM EST
 The number of Users connected to Access Point ap-blh010-ug-01 exceeded the critical threshold limit (90%).

 ap-blh010-ug-01 IP Device

Threshold Information:-
 Configured Critical Threshold: 90%
 Number of Connected Users: 454
 Maximum Users Configured Per Access Point: 500

Severity ▼ Critical
Impact 0
Acknowledged [set](#)
Clearable Yes
Trouble Ticket ID [set](#)
Assignment [set](#)

Symptoms Number of Users connected to Access Point exceeded the critical threshold
Probable Cause Total number of Users connected to Access Point exceeded the critical threshold
Actions 1) Refer to the Event Message associated with this alarm for additional details
 2) Review the Events associated with this model that occurred in the same model

Thresholds

Thresholds can be configured here so that an alarm is generated if a given threshold is exceeded. To disable a threshold from generating alarm, set that threshold value to zero.
 Note: "--" will be displayed when threshold values are incorrectly set.

Connected Access Points 481
 Connected Clients 33

| | Maximum Supported | Minor Threshold(%) | Major Threshold(%) | Critical Threshold(%) |
|---------------------------------|---------------------------|------------------------|------------------------|------------------------|
| Access Points | 352 | 70 set | 80 set | 90 set |
| Mobile Nodes/Clients | 7171 | 70 set | 80 set | 90 set |
| Access Point Users | 500 set | 70 set | 80 set | 90 set |
| Download Volume Per Client (MB) | 10240 set | 70 set | 80 set | 90 set |
| Upload Volume Per Client (MB) | 10240 set | 70 set | 80 set | 90 set |

Persona

Organization: ABC Bank Corporation

User Name: Tom

User Persona: NOC engineer

Key Responsibilities:

- Network availability

Tools:

- CA Spectrum



Use Case 1: Threshold Configurations

- *Problem Statement:* User is unable to connect to the Wireless network despite getting the strong signal. Sr. management is having a meeting in the board room with few delegates. Steve prepared the presentation to showcase some of the key capabilities/features of the product. Steve login to his laptop and tried to connect to the Wi-Fi network but getting authentication failure message, where other members in the room could able to connect.
- *Value:*
 - As Tom has configured thresholds into Spectrum it will generate an Alarm for number of connection reached to max. Hence Tom understands that why Steve is facing this issue.
 - Capacity Planning: Based on the threshold alarms received the network engineer gets a pattern of usage and hence can plan for additional access point.

Use Case 2: Fault Isolation

- *Problem Statement*: The operator receives some tickets that users are not able to access the network via phones and laptops
- *Value*:
 - Using CA Spectrum fault isolation capability the network engineer is able to figure out the issue is with connected L2 switch.

Demo

Roadmap

- Reporting
- Heatmap
- Flow information
- Support for more vendors
 - Ruckus
 - Extreme devices

Questions





Nagesh Jaiswal

Principal Product Manager
Nagesh.Jaiswal@ca.com

 @nageshjaiswal



 [Linkedin.com/in/nageshjaiswal](https://www.linkedin.com/in/nageshjaiswal)