CA Spectrum Community Webcast: Wireless Monitoring with CA Spectrum

Nagesh Jaiswal

19th July 2017
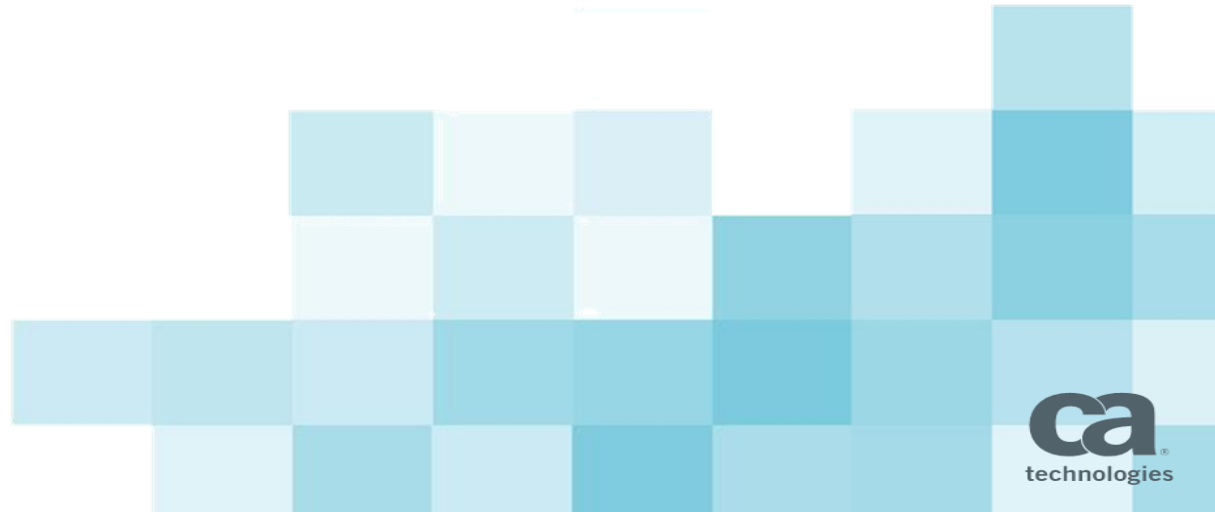
Agenda

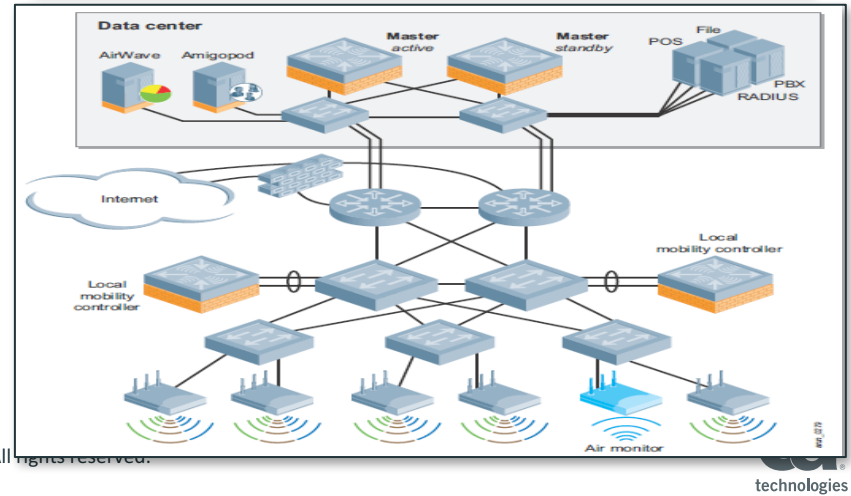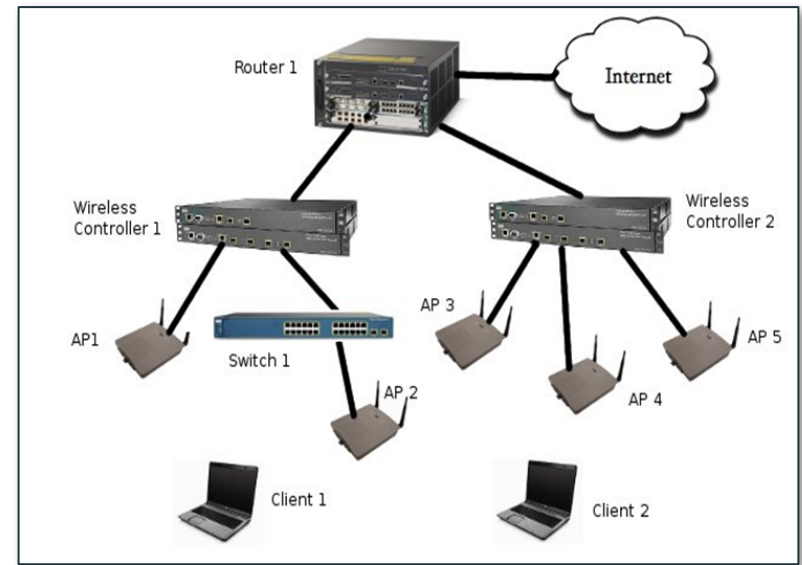|	
1	**VALUE PROPOSITION**
2	**OVERVIEW**
3	**FEATURES**
4	**DEMO**
5	**ROADMAP**
6	**QUESTIONS**

ca
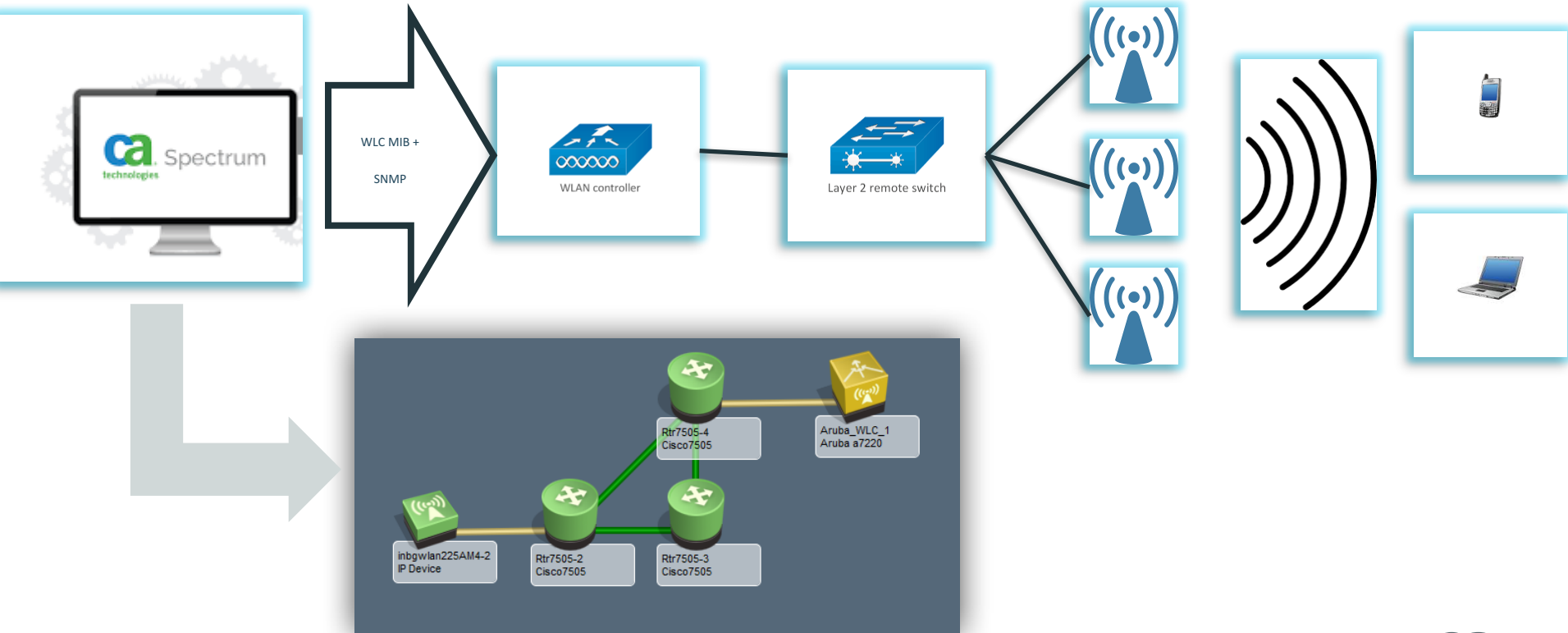technologies

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

ca
technologies

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

4

How it works?

WLC MIB +

SNMP

WLAN controller

Layer 2 remote switch

Rtr7505-4
Cisco7505

Aruba_WLC_1
Aruba a7220

inbgwlan225AM4-2
IP Device

Rtr7505-2
Cisco7505

Rtr7505-3
Cisco7505

technologies

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

ca technologies®

OneClick Views for better management

- WLC Manager in explorer view for organization of wireless devices

- OneClick content pane views for LWAP and Wireless information and its sub views

- End to end visualization in topology view

- Spotlight view for a quick view of WLC and associated AP's

- Locator search for WLC & APs

ca technologies
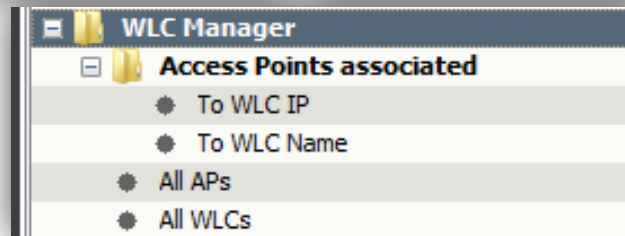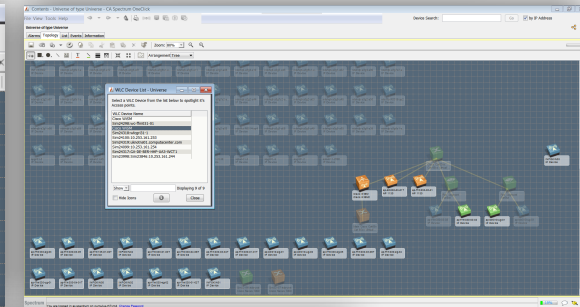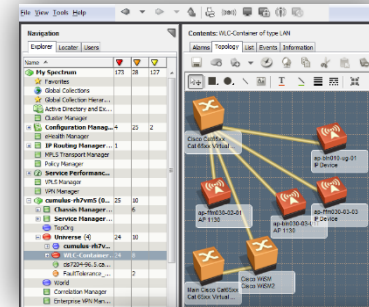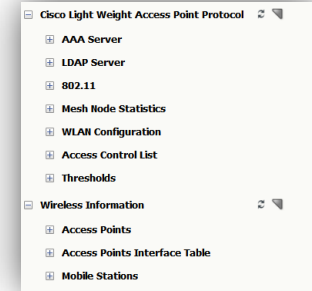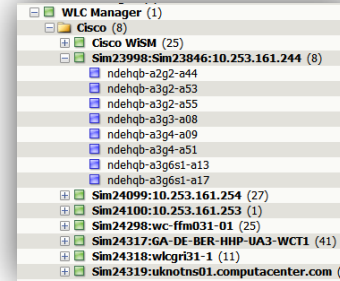
Alarms, Events & Traps

- Supports Traps provided by WLC MIB

- All alarms on AP's are asserted on respective WLC

Others

- Support for maintenance mode

- Support for AP Migration

- Supports Cisco WLC FT Scenarios (AP SSO)

- Support for DHCP enabled AP's

Control and Proactive Monitoring

- Threshold Configuration

- Threshold violation alarms

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.

ca
technologies

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.

ca
technologies

Demo

Roadmap

- Reporting

- Heatmap

- Flow information

- Support for more vendors
  - Ruckus
  - Extreme devices

ca
technologies

Questions

Nagesh Jaiswal
Principal Product Manager
Nagesh.Jaiswal@ca.com

@nageshjaiswal

Linkedin.com/in/nageshjaiswal