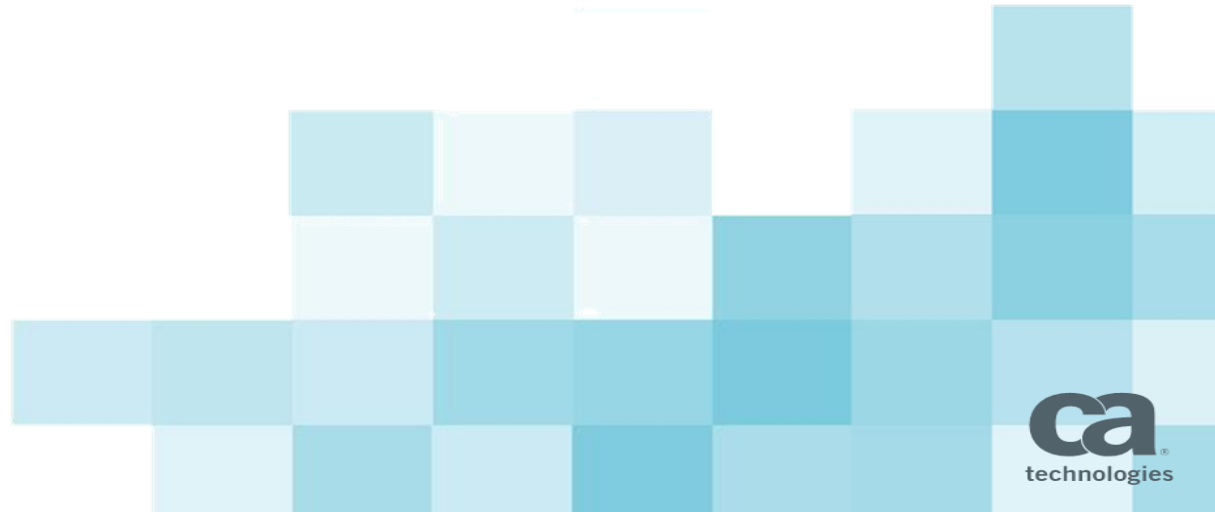


CA Spectrum Community Webcast: Wireless Monitoring with CA Spectrum

Nagesh Jaiswal

19th July 2017



Agenda

1

VALUE PROPOSITION

2

OVERVIEW

3

FEATURES

4

DEMO

5

ROADMAP

6

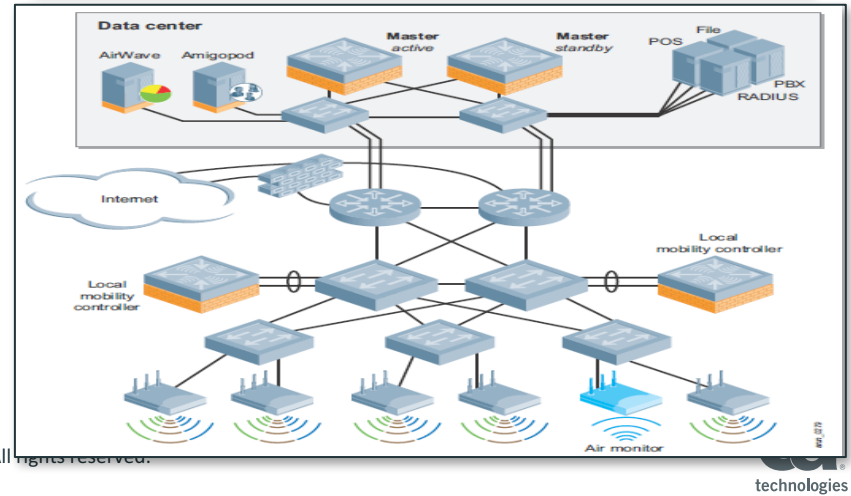
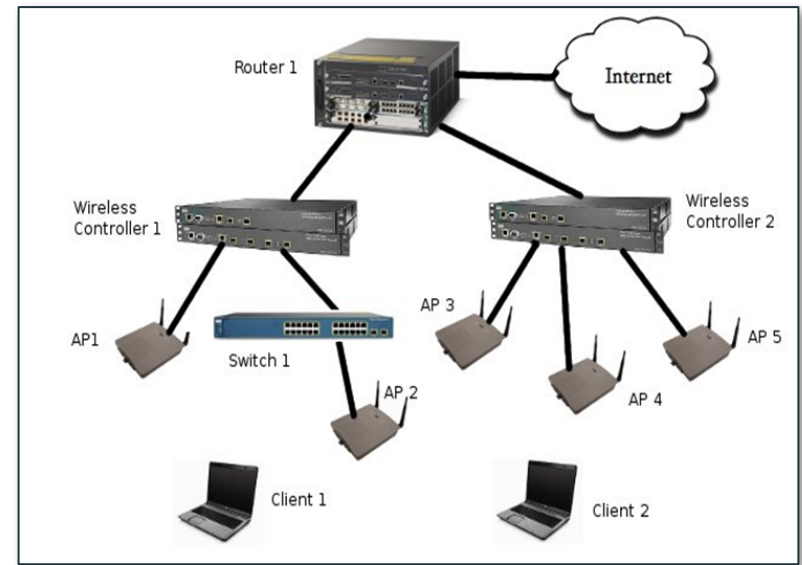
QUESTIONS

Value Proposition

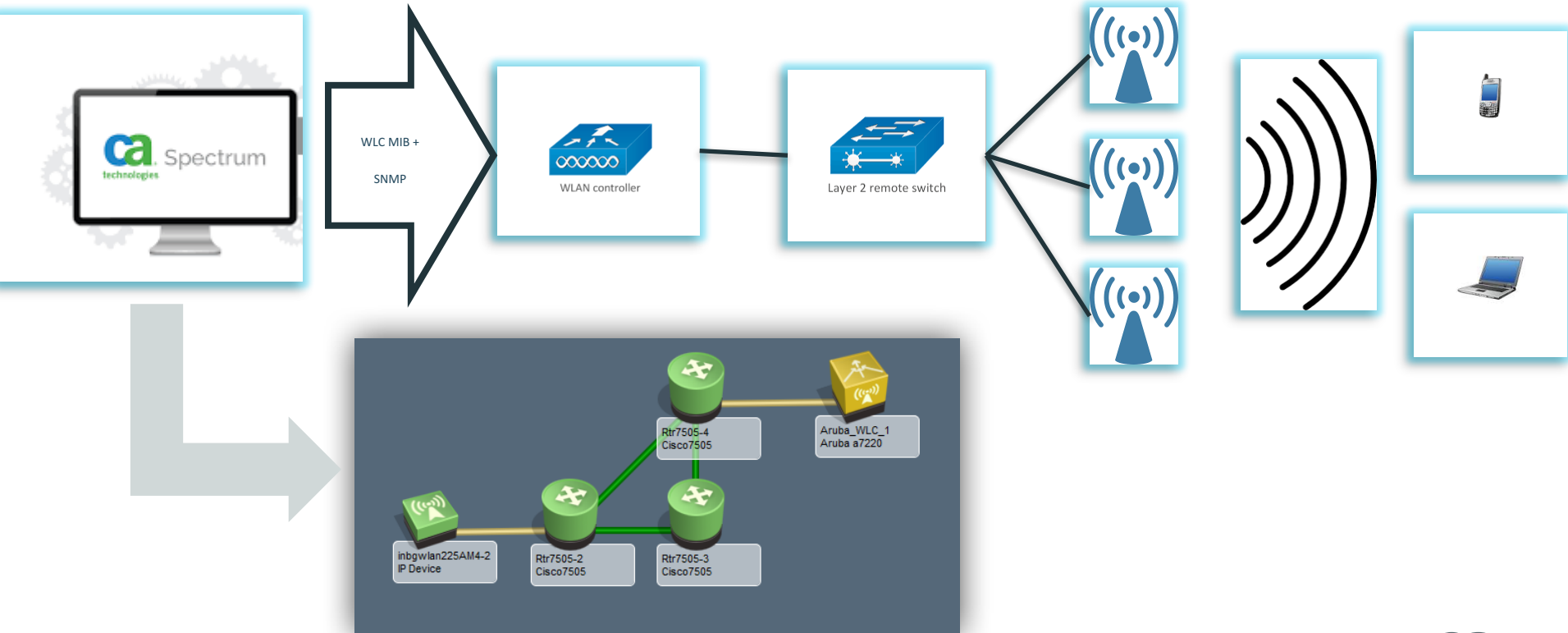
- Brings your wireless network logically into spectrum management, without treating it as an isolated technology
- Gives network operators the tools to manage and control the wireless network—which helps reduce outages and make your wireless network as stable as your wired network
- Specifically designed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

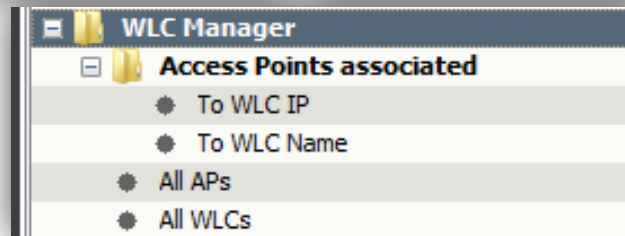
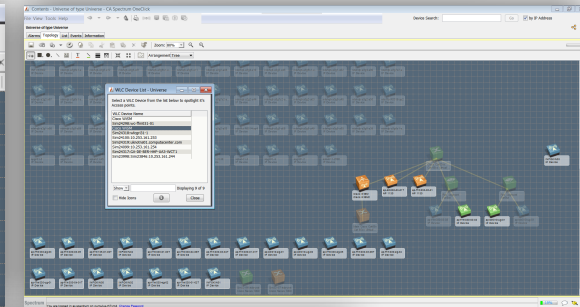
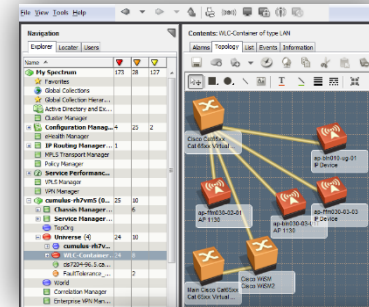
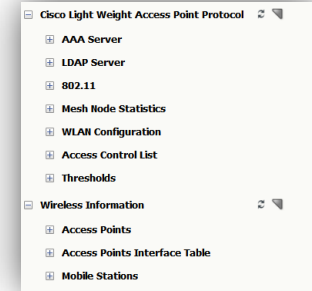
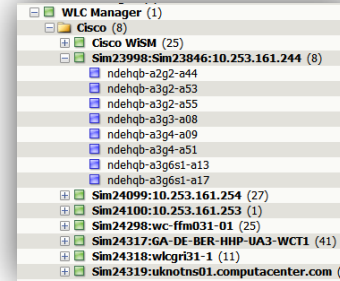
■ Discovery Console

- 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

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



Alarms, Events & Traps

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

The screenshot displays the Cisco Prime Network Manager interface, specifically the 'Alarms' section for a Cisco 8500 WLC. The top panel shows a list of alarms, with one critical alarm highlighted: 'WIRELESS CLIENTS CONNECTED TO WLC CONTROLLER EXCEEDED CRITICAL THRESHOLD'. The bottom panel provides a detailed view of this alarm, including its severity (Critical), impact (0), and a list of symptoms and probable causes. The 'Symptoms' section indicates that the number of wireless clients connected to the WLC Controller exceeded the critical threshold limit. The 'Probable Cause' section lists three potential reasons: 1) Watch out for further increase of clients connections on this WLC Controller, 2) Consider distribution of clients to other WLC Controllers, and 3) Consider addition of a new WLC Controller before number of client connections reaches maximum supported limit.

Below the alarm details, the 'Events' section 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...	Access Points Minor Threshold: 70% Connected : 1876 Maximum Supported : 2396	System	Oct 19, 2015 10:14:04 A...	System
	Oct 19, 2015 10:08:44 A...	Sim23998:Sim238...	Auto-discovery mapping process finished on model Sim23998:Sim23846:10.253.161.244 of type Rtr_Cisco	System		
	Oct 19, 2015 10:08:24 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 The number of Access Points connected to WLC Controller Sim23998:Sim23846:10.253.161.244 exceeded the major threshold limit.	System		
Major	Oct 19, 2015 10:04:03 A...	Sim23998:Sim238...	Access Points Major Threshold: 80% Connected : 1875 Maximum Supported : 2227	System	Oct 19, 2015 10:09:04 A...	System
	Oct 19, 2015 10:03:37 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 displays the 'Alarms' tab in the Cisco Prime Network Manager. It shows a list of events with columns for Severity, Created On, Name, Event, Created By, and Cleared On. The selected event is 'Access Point 'f0003-01' has migrated from WLC 'f0003-01' to WLC 'f0003-01'.' Below the list, the 'Component Detail' for 'Cisco WSM' is shown, including a table of attributes.

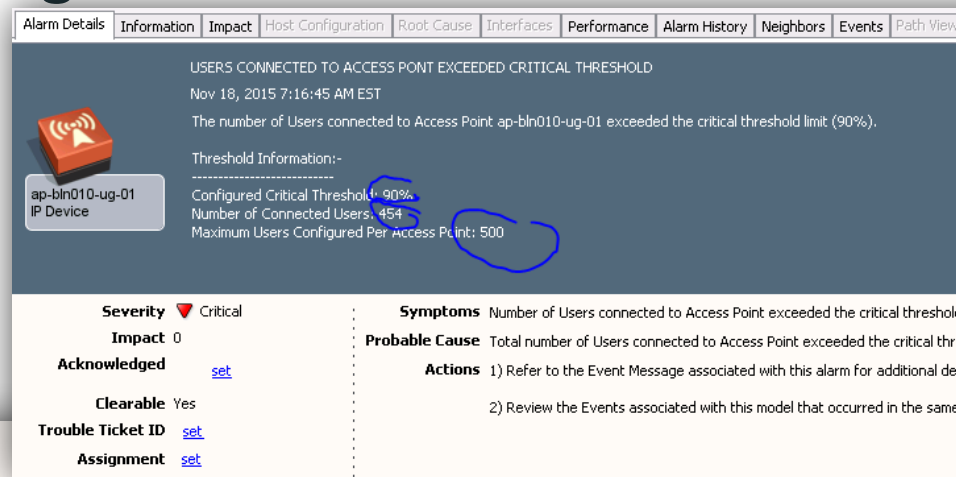
Name	ID	Type
Admstr_attr	0x1049	Integer
Admstr_attr	0x104e	Boolean
Admstr_attr	0x104f	Integer
Admstr_attr	0x1050	Integer
Admstr_attr	0x1051	Integer
Admstr_attr	0x1052	Integer
Admstr_attr	0x1053	Integer
Admstr_attr	0x1054	Integer
Admstr_attr	0x1055	Integer

The screenshot displays the 'Topology' tab in the Cisco Prime Network Manager. It shows a network diagram with a central 'Cisco WSM' (Cisco WSM) connected to several 'AP' (Access Point) devices. The 'Component Detail' for 'Cisco WSM' is shown, including a table of attributes.

Name	ID	Type
Admstr_attr	0x1049	Integer
Admstr_attr	0x104e	Boolean
Admstr_attr	0x104f	Integer
Admstr_attr	0x1050	Integer
Admstr_attr	0x1051	Integer
Admstr_attr	0x1052	Integer
Admstr_attr	0x1053	Integer
Admstr_attr	0x1054	Integer
Admstr_attr	0x1055	Integer

Control and Proactive Monitoring

- Threshold Configuration
- Threshold violation alarms



The screenshot shows an alarm titled "USERS CONNECTED TO ACCESS POINT EXCEEDED CRITICAL THRESHOLD". It includes a timestamp "Nov 18, 2015 7:16:45 AM EST" and a description: "The number of Users connected to Access Point ap-bln010-ug-01 exceeded the critical threshold limit (90%)." Below this, a "Threshold Information" section shows "Configured Critical Threshold: 90%", "Number of Connected Users: 454", and "Maximum Users Configured Per Access Point: 500". The "90%" and "500" values are circled in blue. At the bottom, there are fields for "Severity" (Critical), "Impact" (0), "Acknowledged" (set), "Clearable" (Yes), "Trouble Ticket ID" (set), and "Assignment" (set). To the right, "Symptoms" and "Probable Cause" are listed, along with "Actions" such as "Refer to the Event Message" and "Review the Events".

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-bln010-ug-01 exceeded the critical threshold limit (90%).

Threshold Information:-

Configured Critical Threshold: 90%

Number of Connected Users: 454

Maximum Users Configured Per Access Point: 500

ap-bln010-ug-01
IP Device

Severity ▼ Critical

Impact 0

Acknowledged [set](#)

Clearable Yes

Trouble Ticket ID [set](#)

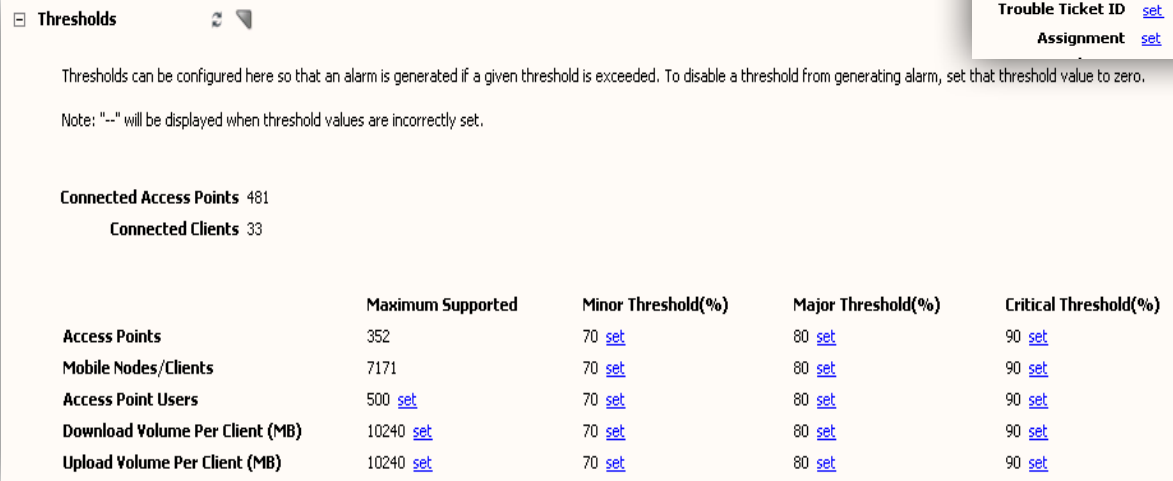
Assignment [set](#)

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 time period



The screenshot shows the "Thresholds" configuration page. It includes a note: "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." Below this, it shows "Connected Access Points 481" and "Connected Clients 33". A table lists various thresholds for Access Points, Mobile Nodes/Clients, Access Point Users, Download Volume Per Client (MB), and Upload Volume Per Client (MB). Each row has columns for "Maximum Supported", "Minor Threshold(%)", "Major Threshold(%)", and "Critical Threshold(%)", with "set" links for the latter three.

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