

# Safely Enabling BYOD In the Workplace

NICT 2025

Presented By:

Matt Hall – Ruckus Systems Engineering Team Lead ANZ



# What Is BYOD?

---

## Bring Your Own Device:

- Device provided and owned by the end user.
- Normally used for personal use and sometimes work use.
- Wi-Fi connectivity is usually provided by the company enabling devices to have internet access and sometimes other internal resources.



# BYOD The Good and The Bad



- Cost benefit to the business as employee provides their own device.
- Studies suggest people more familiar with their own device are likely to be more productive.
- Connect workers not normally at a desk.
- Flexibility is key to an employee's happiness.

- If implemented poorly network security and performance can be an issue.
- Data security and privacy can be at risk if controls are not in place.
- Expectations from users that IT will provide device support can be problematic.

# Implementing BYOD In Your Environment

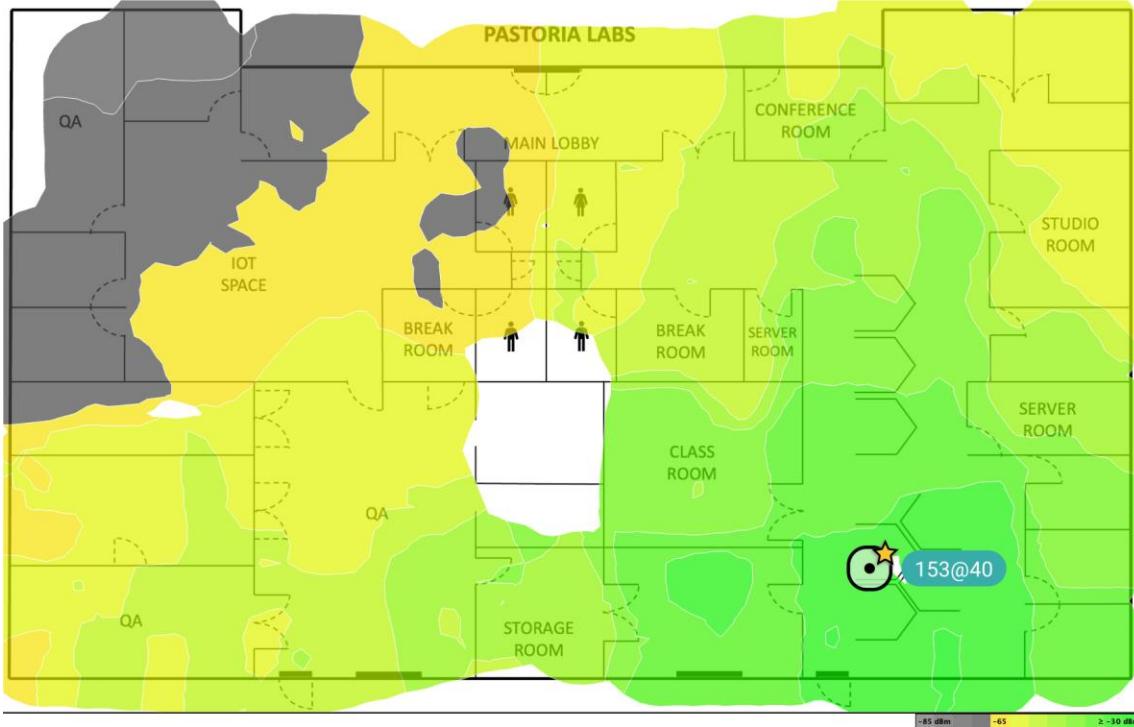
- **Implement an organization policy governing BYOD usage:**
  - Areas of the site where devices may not be allowed due to safety.
  - Will IT Support be providing for these devices?
  - Privacy and Intellectual Property Protection.
- **Are charging facilities required / to be provided?**
- **Device Management and Network Connectivity:**
  - If devices are to be used for work are applications web based?
  - Is an MDM solution required to manage apps and company data on the device?
  - Is the current Wi-Fi coverage and capacity suitable for an increase in connected users and devices?
  - Implement user-based authentication for the BYOD Wi-Fi service.
  - Ensure network segmentation is in place.



# Network Connectivity



# Wi-Fi Coverage and Capacity



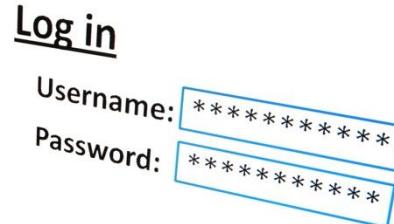
How far will your current Wi-Fi signal reach?

How much bandwidth is available:

- On your internet connection?
- At an Access Point level?

# Wi-Fi Networks: Authentication vs Encryption

## Authentication



Verifying a User or Device  
is Authorized to Access  
the Network

## Encryption



Encrypting Data During  
Transmission Over the Air  
Ensures Privacy and  
Protects Against Tempering

NOTE: Sometimes the function of Encryption can also be used for Authentication. EXAMPLE: In the case of a PSK (Pre Shared Key) network the password is also the encryption key.



# Wi-Fi Network: Authentication Options

Authentication Type	Over the Air Encryption?	Credential Type
MAC Address (Via Captive Portal)	No	MAC Address, Token or None
WPA2 / Personal	Yes (128 Bit)	Pre-Shared Key (s)
WPA2 / Enterprise	Yes (128 Bit)	RADIUS EAP (Cert or Username)
OWE	Yes (128 Bit)	MAC Address, Token or None
WPA3 / SAE	Yes (128 Bit)	Pre-Shared Key (s)
WPA3 Enterprise	Yes (256 Bit)	RADIUS EAP (Cert or Username)



Modern methods, but limited uptake due to legacy device compatibility.

# Data Encryption (Over the Air)

- Older Methods (Considered to be Weak):
  - WEP
  - TKIP (Original WPA)
- Todays Methods:
  - WPA2 Personal (PSK) – AES-CCMP 128bit
  - WPA2 Enterprise (802.1x) – AES-CCMP 128bit
  - WPA3 – Personal (SAE) – AES-CCMP 128bit
  - WPA3 – Enterprise (802.1x) – AES-GCM 256bit
  - OWE – Opportunistic Wireless Encryption - AES-CCMP 128bit



# OWE – Opportunistic Wireless Encryption

---

- Provides encryption without the need for predefined credentials
- Implemented by most vendors in 2021
- Required when operating an open network in 6GHz

NOTE: This is only encryption and NOT AUTHENTICATION

Common use cases see OWE networks deployed with captive portal

# Common Examples of Network Authentication

---

- **Employees or Permanent Users – WPA2/WPA3 Enterprise**
  - Credentials stored in a directory service such as an Active Directory
- **Contractors or Semi Permanent Users – WPA2 PSK or WPA3 SAE**
  - Ruckus Dynamic Pre Shared Keys provided via Self Service or from Administrator
- **Guests – Captive Portal (May include OWE)**
  - Well, can we address this as we are trying to implement security for

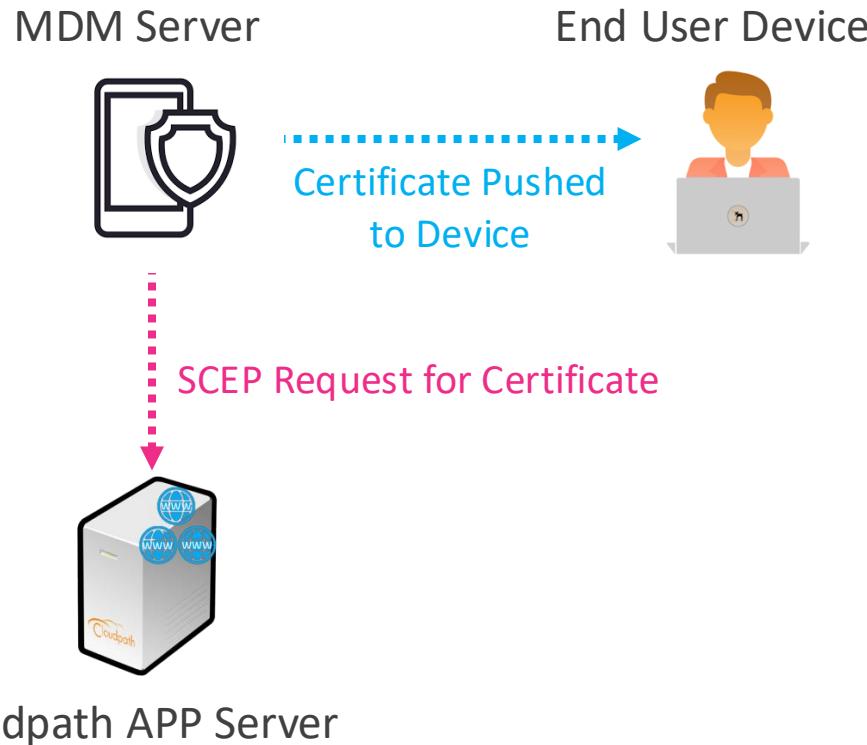
# Connecting BYOD Devices – Authentication Summary



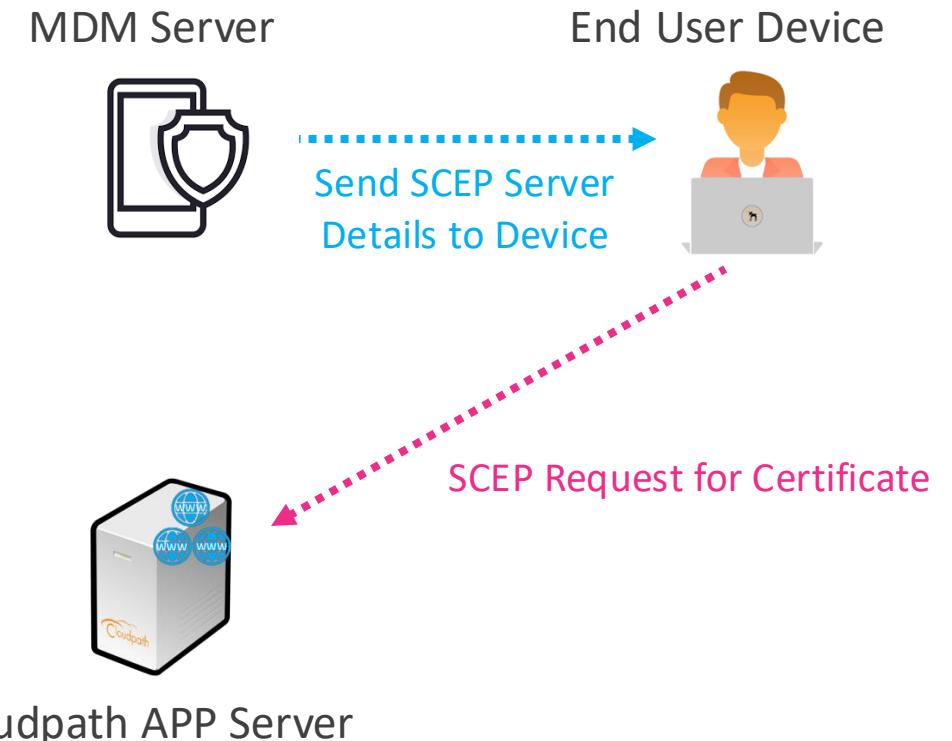
Authentication Type	Credential	Notes
WPA2 Personal	Single or Multiple Shared Key	
WPA2 Enterprise	Certificate	Must be loaded on device and really requires MDM.
WPA2 Enterprise	Username / Password	Required Windows Server with NPS.
Captive Portal / Open	Username / Password	No Encryption, User required to login frequently.

# Automatic Certificate Enrolment Through MDM

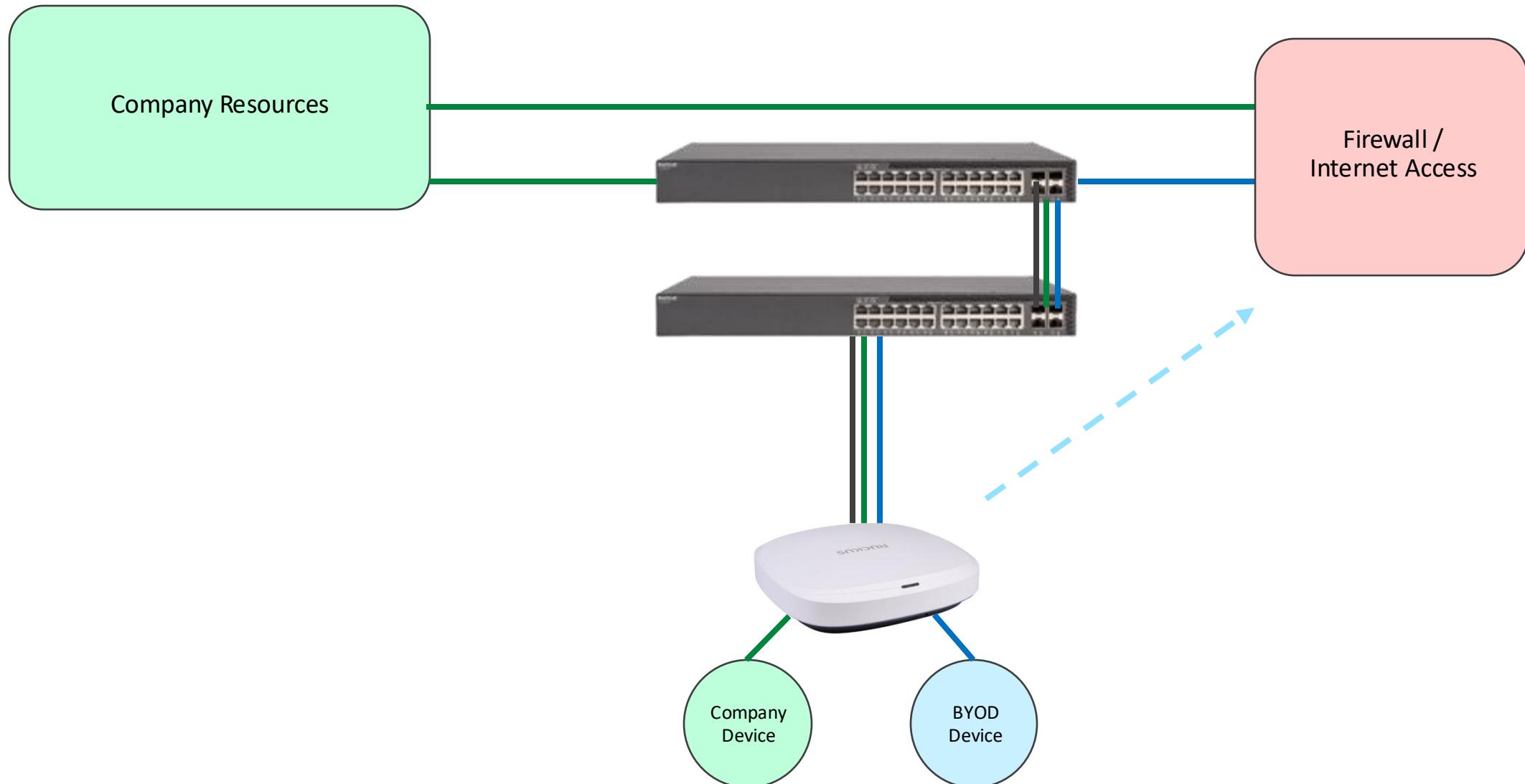
## MDM Solution with SCEP Proxy



## MDM Solution with device SCEP Enrolment

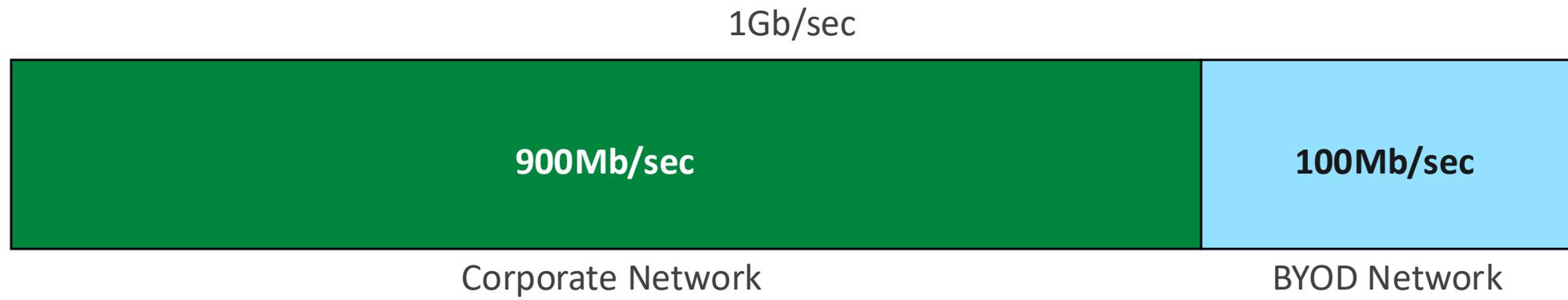


# Traffic Segmentation



# Traffic Bandwidth Control

Ensure Quality of Service for Corporate Traffic and Restrict Total BYOD Bandwidth



## Load Control

Max Rate:

Upload Limit

100 1 Mbps 500 Mbps

Download Limit

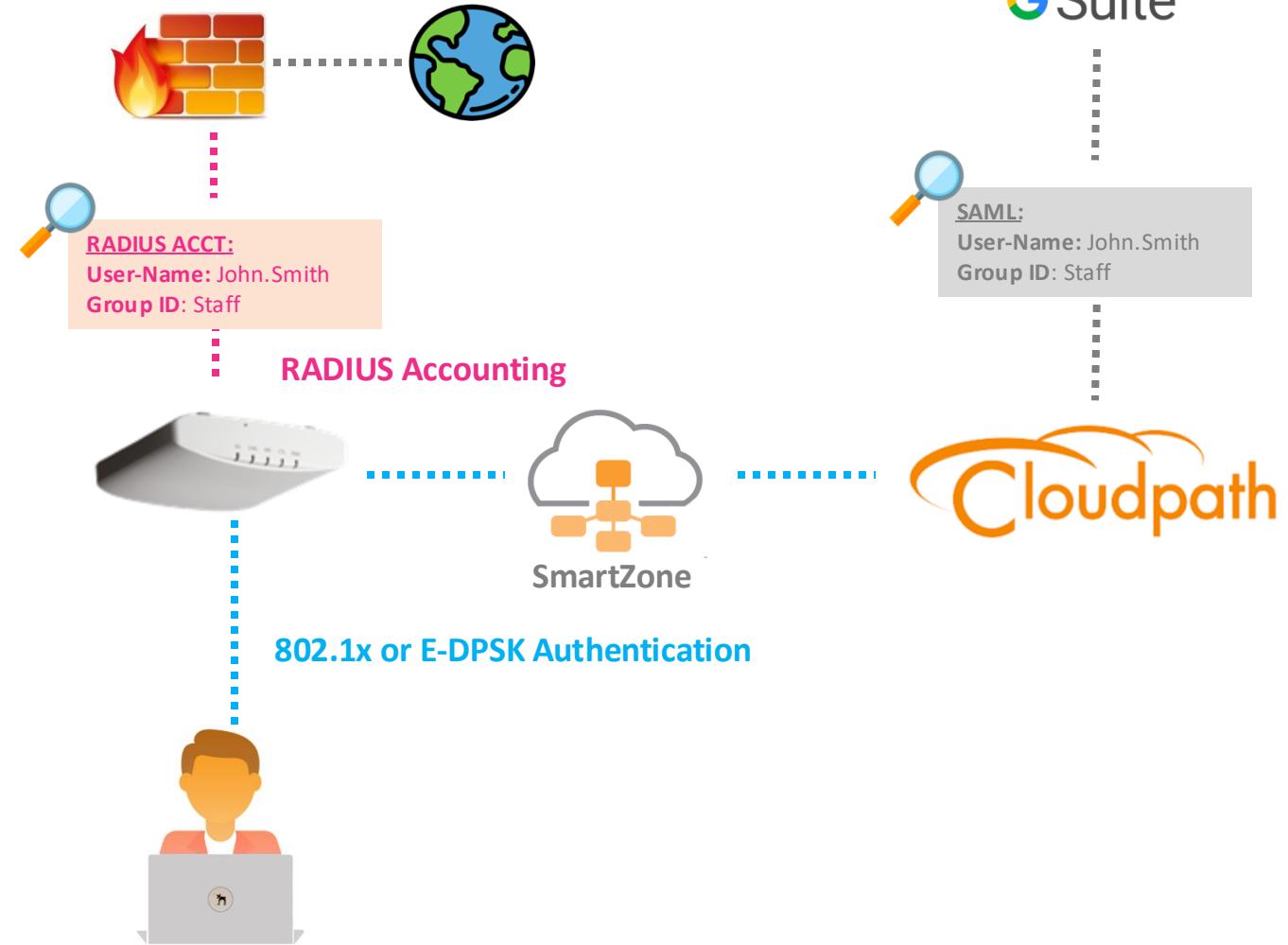
100 1 Mbps 500 Mbps

Max clients per radio:

100 1 512

# Integration With Network Reporting

- Wi-Fi Network passes the firewall RADIUS Accounting or API data including the Username and Group information.
- Content Filtering and Reporting based on the users identity.





**PURPOSE-DRIVEN**  
ENTERPRISE NETWORKS

# RUCKUS AI

## Self Optimising Networks



# WE ARE LIVING IN NEW ERA OF NETWORKING



AI Costs are  
Plummeting since  
2020

The Impact of  
Declining AI Training  
Costs - Leading to  
Mass Adoption

AI Everywhere

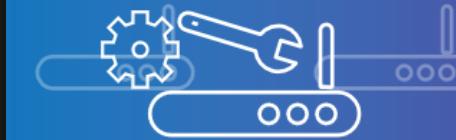
# WE ARE IN THE ERA OF AI DRIVEN NETWORKING!

Surface issues before  
they blow up



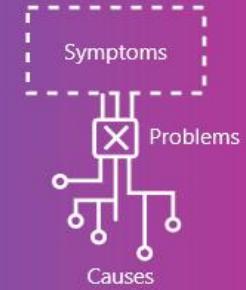
ML-driven incident and  
anomaly detection

Address the most  
urgent issues first



AI-driven prioritization

Fix them fast



ML-driven root cause  
and recommendations

Compare network KPIs  
before and after a  
change to analyze the  
impact



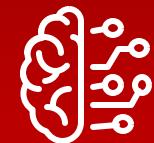
Config change analysis

Let the system make  
recommendations on  
changes to improve  
network performance



AI-recommendations

Let Cloud RRM  
drive down  
interference and  
maximize capacity  
every day.



AI-Driven Cloud RRM

# FRUSTRATIONS OF NETWORK TROUBLESHOOTING TODAY



Always reactive. **Can you catch the problem before it blows up?**



Too much data or too little data for troubleshooting. **Can technology help you cut through the noise?**



Difficult to produce relevant network reports for other stakeholders. **Is there a solution out there?**



No matter what, you are covered!



# AI-driven Network Assurance and Business Analytics



## Incidents/Insights

Root Cause and Recommendations, Network Health, Client Troubleshooting

## AIOps

Service Validation, Video call QoE, Webhook, Runbooks, Melissa

## Explainable AI

AI Recommendation, Auto Remediation, Configuration Analysis

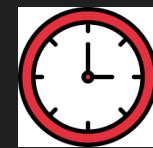
## Business Analytics

Brand 360, Data Studio

# RUCKUS AI is a Must-Have SOFTWARE



**657K** Priority1  
Incidents identified



**4.5** Man-Years of Tier-2/3  
Support cost saved

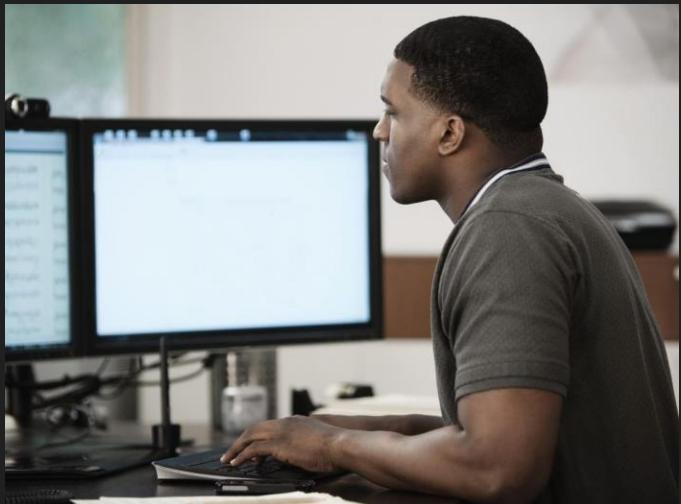


**20%** reduction in  
helpdesk tickets



# RUCKUS AI benefits all 3

**RUCKUS**<sup>®</sup>  
COMMSCOPE



IT



Helpdesk/Support



Line of business

# Benefits delivered by RUCKUS AI

Helps IT teams to prioritize

Eliminate IT tribal knowledge

Long term visibility and monitoring of network health

Service Assurance

Accelerate network and client troubleshooting

Reduce the number of service affecting incidents

Industry specific reports

Business Intelligence

Better planning and forecasting

# What is a Digital Twin?

# Wireless Digital Twin - AI-RRM & AIOps



- Harness AI power available in the cloud
- Make a digital copy of the physical RF network- 'Digital Twin'
- Run RRM simulations on the Digital Twin
- Leave the physical network unchanged
- Make new RF channel plan - ch, width, tx power - available
- Show improvements in the network visually
- Automate applying the configuration from the Digital twin to the physical network using AIOps tool
- Predict, Schedule, Monitor and Revert Options

**AI-Driven RRM** 5

There are 5 recommendations for 5 zones covering 379.2K possible RRM combinations. Currently, 0 zones are optimized.

- FR-AUDU  
13 interfering links can be optimized to 0
- FR-PLFI  
33 interfering links can be optimized to 0
- GCR-CHI  
16 interfering links can be optimized to 0
- HS-HOUSTON  
4 interfering links can be optimized to 0
- TESLA  
5 interfering links can be optimized to 0

**QuadrantA**

**Zone 888 Health:**  
Optimized

**Recommendation Details**

**Original Configuration:** Background scanning and 20 MHz for 2.4 GHz with static AP Tx Power

**Current Configuration:** AI-Driven RRM for channel and bandwidth plan with static and reduced AP Tx Power in 332 APs

**Zone:** QuadrantA is experiencing high co-channel interference in 2.4 GHz band due to suboptimal channel planning. The channel plan, and potentially channel bandwidth and AP transmit power can be optimized by enabling AI-Driven RRM. This will help to improve the Wi-Fi end user experience.

**Why this recommendation?**  
AI-Driven Cloud RRM will constantly monitor the network, and adjust the channel plan, bandwidth and AP transmit power when necessary to minimize co-channel interference. These changes, if any, will be indicated by the Key Performance Indicators. The number of interfering links may also fluctuate, depending on any changes in the network, configurations and/or rogue AP activities.

**Potential trade-off:**  
AI-Driven Cloud RRM will be applied at the zone level, and all configurations (including static configurations) for channel, channel bandwidth, Auto Channel Selection, Auto Cell Sizing and AP transmit power will potentially be overwritten. Do note that any unlicensed APs added to the zone after the AI-Driven Cloud RRM is applied will not be considered and thus no results in suboptimal channel planning in the zone.

**Key Performance Indications**

**Before**   
**Recommended** 

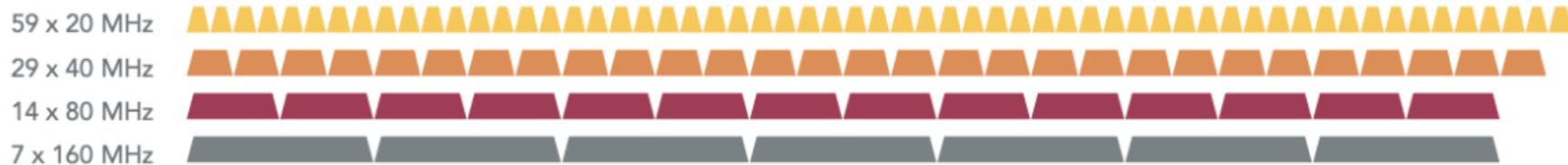
**Status Trail**

# RF Channel Management is VERY complex



## Comparative Channel schema

### 6 GHz Band – Total Spectrum 1200 MHz



### 5 GHz Band – Total Spectrum 500 MHz (180 MHz without DFS)



### 2.4 GHz Band – Total Spectrum 80 MHz



From: [litepoint.com](http://litepoint.com). Comparison of WiFi spectrum between 6GHz, 5GHz and 2.4GHz

# AI-Driven Cloud RRM delivers:



**Greater AP  
Capacity**

**Higher** client  
throughput

**Lower** Airtime  
Utilization

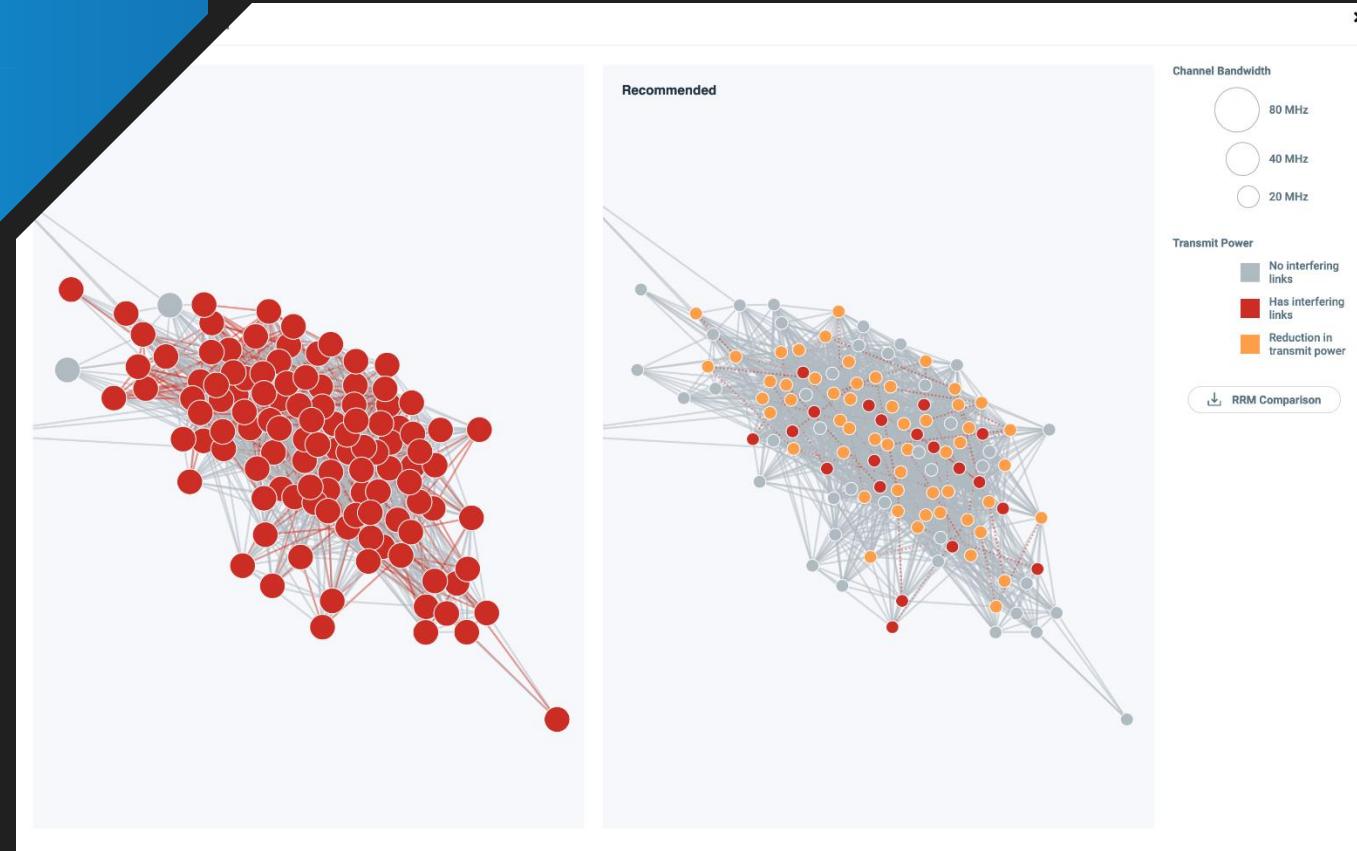
**Higher**  
Reliability

Operate APs at  
**MAX** capability

**Proactive**, Network  
Performance Optimization

**Biggest** advancement in Radio  
Management since BeamFlex!

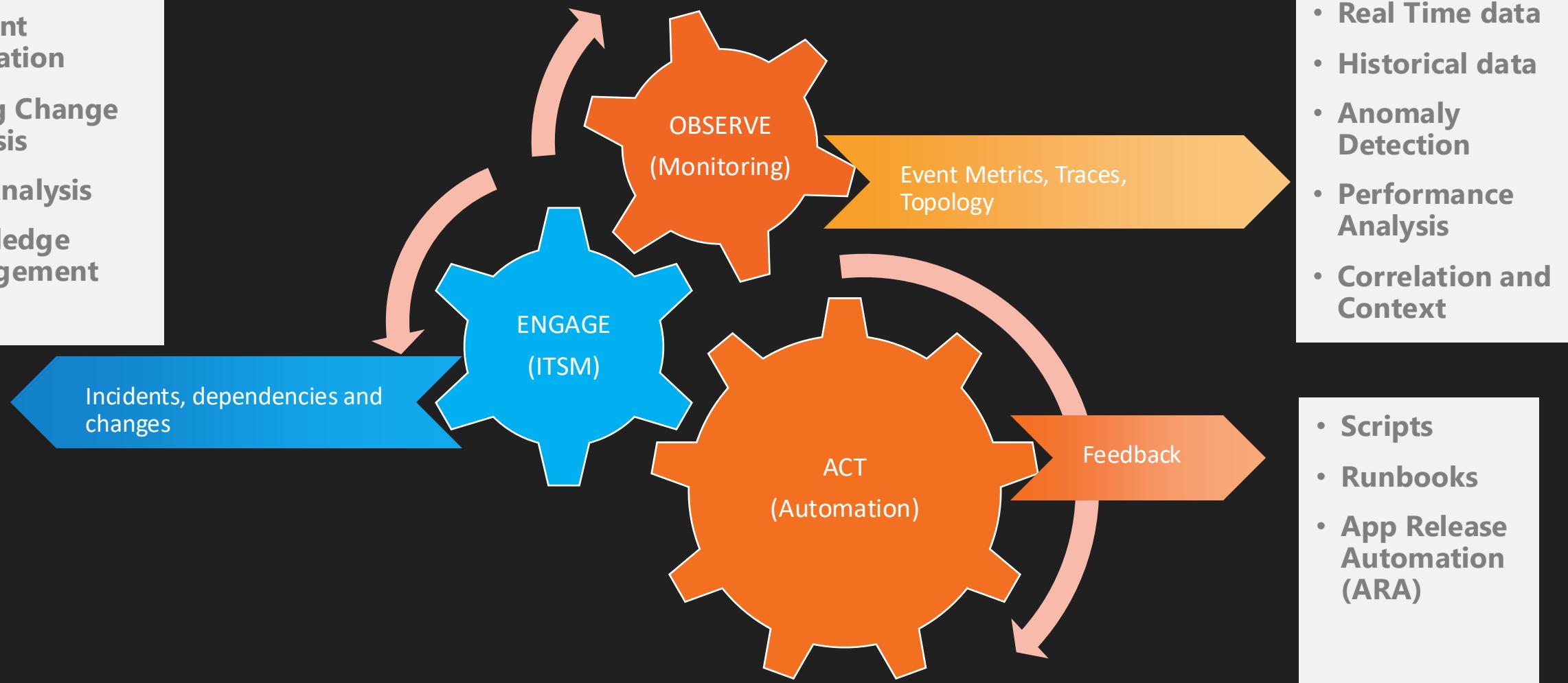
# AI-Driven Cloud RRM delivers:



**Proactive, Tx Power  
Management**

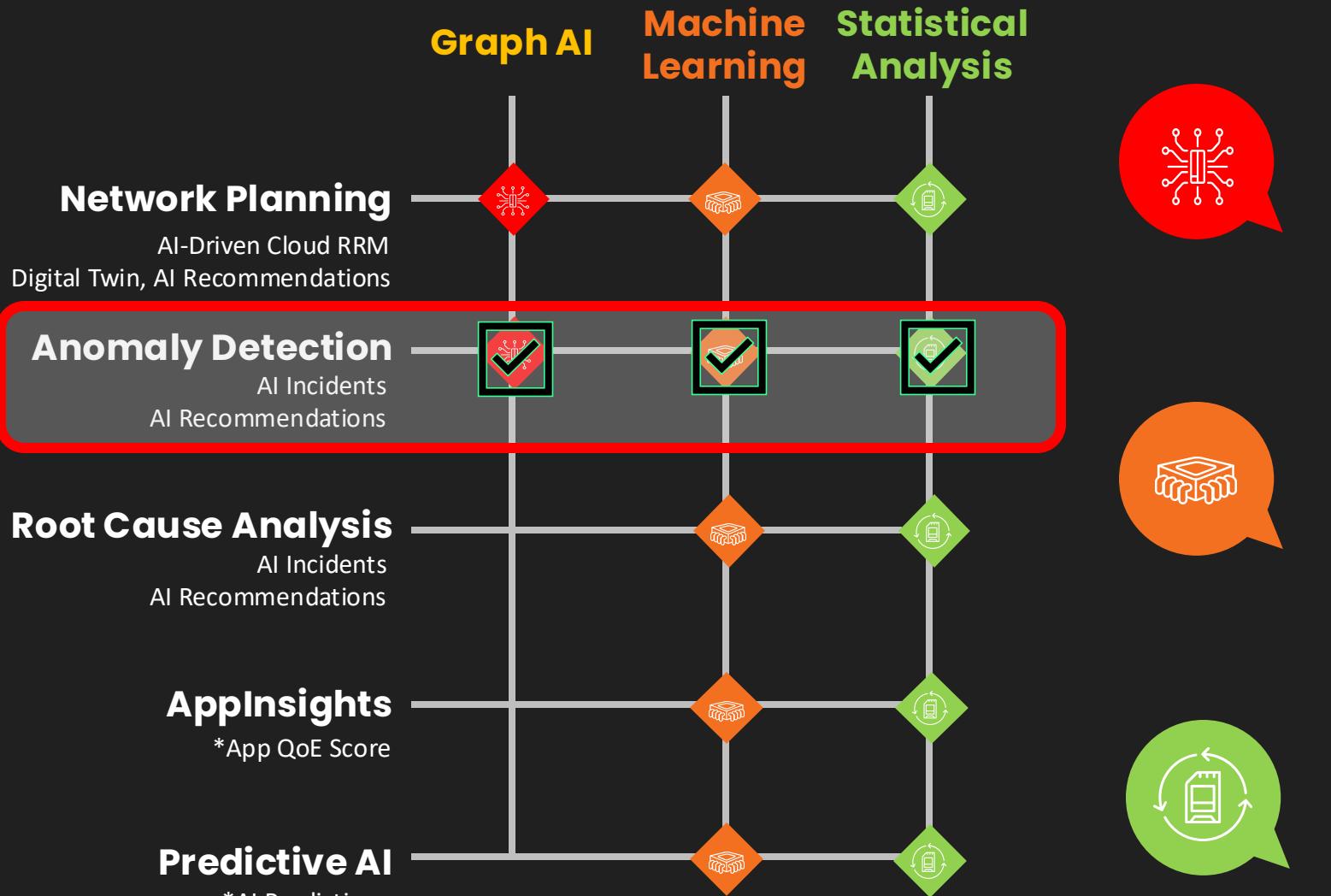
**Optimized, Network  
Performance**

- Incident generation
- Config Change Analysis
- Risk Analysis
- Knowledge Management



## AIOPs – COMBINE AI AND BIG DATA TO AUTOMATE IT PROCESSES

# RUCKUS AI: Delivering Purpose Driven Networks



## Graph AI

Personalized Pagerank, Label Propagation, Louvain Clustering, Betweenness Centrality, Graph Embedding, Weakly Connected Components

## Machine Learning

Decision Tree, Reinforcement Learning, Hybrid Federated Learning, Jenks Optimization, Logistic Regression, Local & Isotonic Regression, Dimension Reduction, Mean Shift Clustering

## Statistical Analysis

Maximum Likelihood Estimation, Seasonality decomposition, Bayesian Inference, Event Density Analysis, Complex Event Processing

# Configuration Change Analysis



Analytics US Search... Clients Network rajiv iyer | RUCKUS NETWORKS INC ? ? Aug 10 2021 12:09 to Aug 17 2021 12:09

Window width is fixed at 24 hrs

Change can be filtered over 7 days or a month

Color of config dots represent SZ config hierarchy

KPI color

Red is degradation, Green is improvement, grey is not significant. Important to understand that this is correlation and not causation.

KPIs across connection, performance, infrastructure

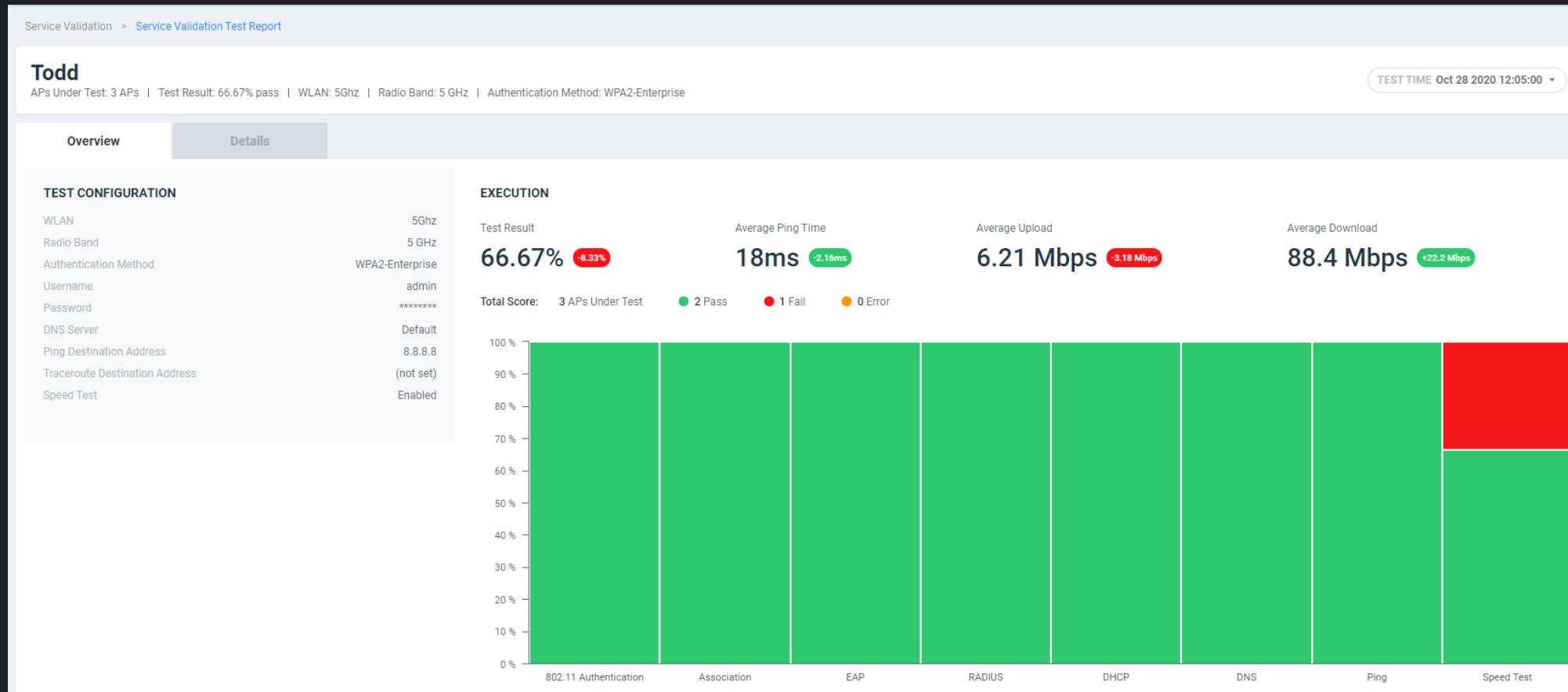
Configuration Change Listing

Timestamp	Entity Type	Entity Name	Configuration
Aug 17 2021 11:08	Zone	RuckusDEMO-01	Recovery SSID: Custom
Aug 17 2021 11:08	Zone	RuckusDEMO-01	AP Admin Password
Aug 17 2021 11:05	Zone	Oyster Pointe	Restricted AP Access Point
Aug 17 2021 11:05	Zone	Oyster Pointe	Historical Connection

Configuration Change Listing

Timestamp	Entity Type	Entity Name	Configuration
Jul 11 2022 15:19	WLAN	LBO	
Jul 11 2022 15:18	WLAN	LBO	
Jul 11 2022 12:28	WLAN	new8021x	
Jul 11 2022 12:22	WLAN	new8021x	

# What is Service Validation?



- Conveniently orchestrate network tests from cloud
- No extra hardware sensor or test equipment needed
- Test WLAN, LAN and WAN connectivity
- Test EAP, RADIUS, DHCP, DNS, Ping, Traceroute, Speed Test (upload/download)

# Service Validation – Video Call QoE



Test Report

PTest8 | Start Time: May 21 2021 08:57:22 | End Time: May 21 2021 09:09:40 | Duration: 12m 18s

**Test participants**

Participant	Client MAC	IP	Network Type	Join Time	Leave Time	AP	AP MAC	SSID	Radio	Wi-Fi Connection Quality
Jpero	B8:08:CF:45:... ↪	76.9.88.170	Wi-Fi	08:57	09:09	R510_Office	EC:58:EA:09:80:B0	RA_vSZ_Network	2.4 GHz	Good
JP4BetterWiFi	B0:35:9F:07:... ↪	76.9.88.170	Wi-Fi	08:59	09:09	R510_Office	EC:58:EA:09:80:B0	RA_vSZ_Network	5 GHz	Good

**Overall Zoom call quality**

**Zoom stats – Jitter, latency, packet loss, video frame rate**

**Latency**

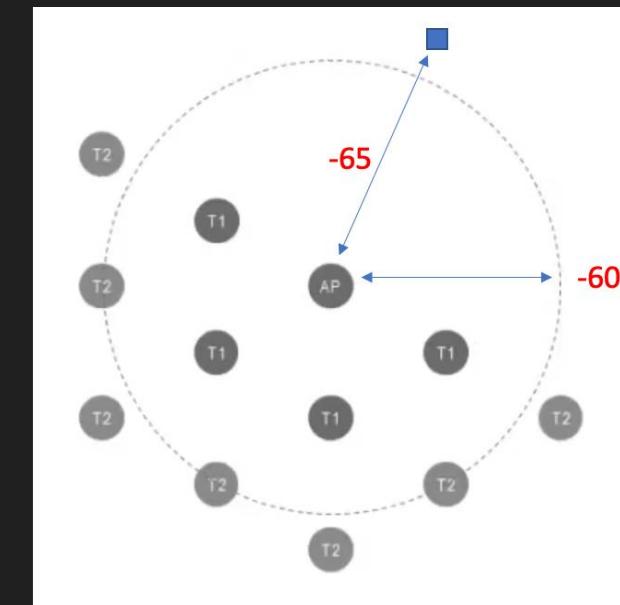
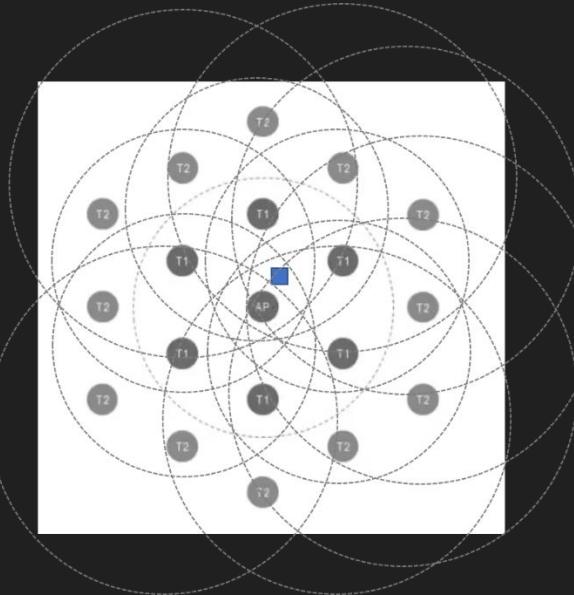
**Wi-Fi quality**

**Packet Loss**

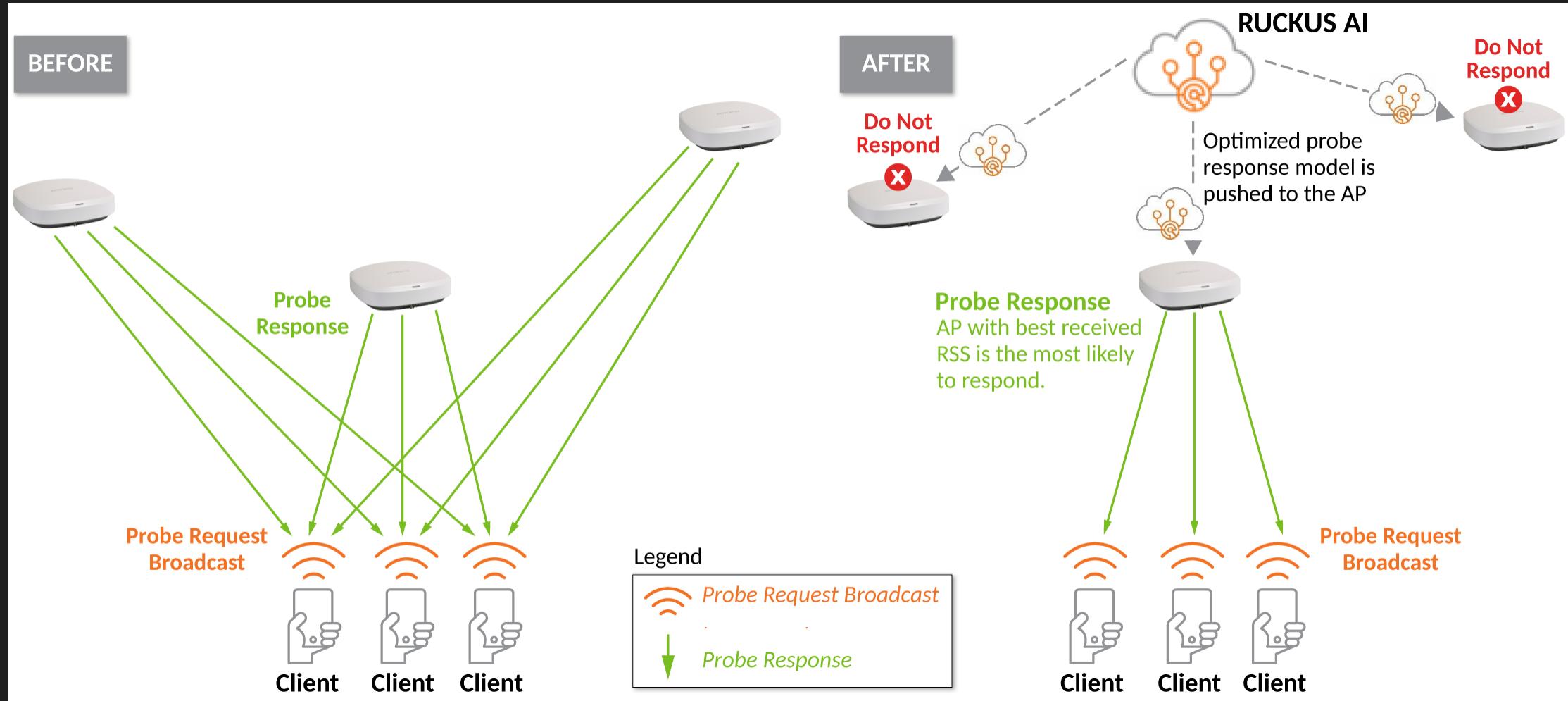
**Video Frame Rate**

# Introducing EquiFlex

*RUCKUS APs are now equipped with unique AI capabilities to adapt to RF network needs.*



# EquiFlex- An Example of Hybrid Federated Machine Learning (HFML)



# RAI Switch Insights – How do they help?

## Network Topology

Gain a powerful interactive view into their wired/wireless network along with useful information such as switch version etc.

## VLAN Mismatch Insight

Automatically identify costly misconfigurations and proactively prevent network outages

## High Memory Utilization Insight

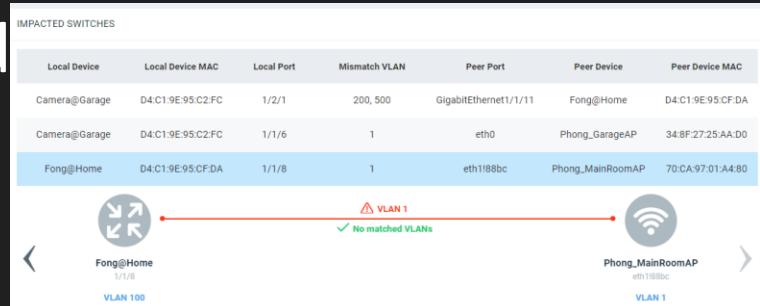
Proactively identify possible switch memory leak and prevent costly network downtime. Incidents rise in severity based on time to failure.

## PoE Insight

Automatically identify PoE exhaustion issues which could require adding more power capacity or replacing failed units saving time and network downtime

# VLAN Mismatch Insight

- VLAN mismatch - Automatic classification as P1 incident
- Impacted switches and VLANs listed
- Drill down at port and connection level
- Port, mismatched VLAN number, peer port, peer device name, peer device MAC displayed



## INSIGHTS

### ROOT CAUSE ANALYSIS

System has detected VLAN mismatches in your network. This is usually caused by misses during the VLAN configuration process.

### RECOMMENDED ACTION

Check and configure missing VLAN, or ensure type (untagged/tagged) match on both ends of the connection.

### INCIDENT INFO

Incident Category	Infrastructure
Incident Sub-Category	VLAN Mismatch
Type	Switch Group
Scope	Fong@Home
Duration	2h
Event Start Time	Feb 10 2021 09:00
Event End Time	Feb 10 2021 11:00

# VLAN mismatch Insight DETAILS

Incidents > Incident Details

**Incident Details** P1 | VLAN mismatch found in Switch Group: Density

**DETAILS**

<b>3</b> east-icxstack-density west-density-7650-stack ICX7150-C12-Switch	<b>1</b> VLAN 1
<b>Impacted switches</b> Out of 4 switches	<b>Impacted VLANs</b> Out of 6 VLANs

**IMPACTED SWITCHES**

Local Device	Local Device MAC	Local Port	Mismatch VLAN	Peer Port	Peer Device	Peer Device MAC
east-icxstack-density	60:9C:9F:FE:56:42	1/1/8	1	eth1!88bc	E03-R750_EastOfFoxhound	1C:3A:60:3B:DD:70
west-density-7650-stack	60:9C:9F:52:C9:86	1/1/29	1	eth1	W06-R650-Chihuahua	20:58:69:3B:CB:70
west-density-7650-stack	60:9C:9F:52:C9:86	2/1/18	1	eth1!88bc	W03-R550-Terrier	B4:79:C8:3E:87:20
ICX7150-C12-Switch	78:A6:E1:2E:CF:FE	1/1/1	1	eth1!88bc	W04-05_Nextto_Amrit_T75...	28:B3:71:05:14:30

**east-icxstack-density** VLAN 1001 → **VLAN 1** ⚠️ No matched VLANs → **E03-R750\_EastOfFoxhound** VLAN 1

P1 Incident, Identifies switch group, IT can act

**INCIDENT INFO**

Incident Category	Infrastructure
Incident Sub-Category	VLAN Mismatch
Type	Switch Group
Scope	Density
Duration	15m
Event Start Time	Feb 02 2021 16:45
Event End Time	Feb 02 2021 17:00

Insight is evaluated every 2hrs (15 mins is used for internal testing)

No matched VLANs found

# High Switch Memory Utilization Insight

Incidents > Incident Details

**Incident Details** P1

High memory utilization detected in Switch: D52\_RACK\_ICX755048ZP\_Standalone (28:B3:71:29:8C:B6)

P1 Incident, High memory utilization identified, IT can take action



Anomalous memory utilization detected. Time to 50% threshold mem projected

**INCIDENT INFO**

Incident Category	Performance
Incident Sub-Category	Memory
Type	Switch
Scope	D52_RACK_ICX755048ZP_Standalone (28:B3:71:29:8C:B6)
Duration	1h
Event Start Time	Feb 01 2021 21:00
Event End Time	Feb 01 2021 22:00

Scope, Duration, Event, Start and End Time.  
Start Time: Event Detected  
End Time: Memory will Exceed 90% threshold

# Memory Leak - Proactive and Advance Notice

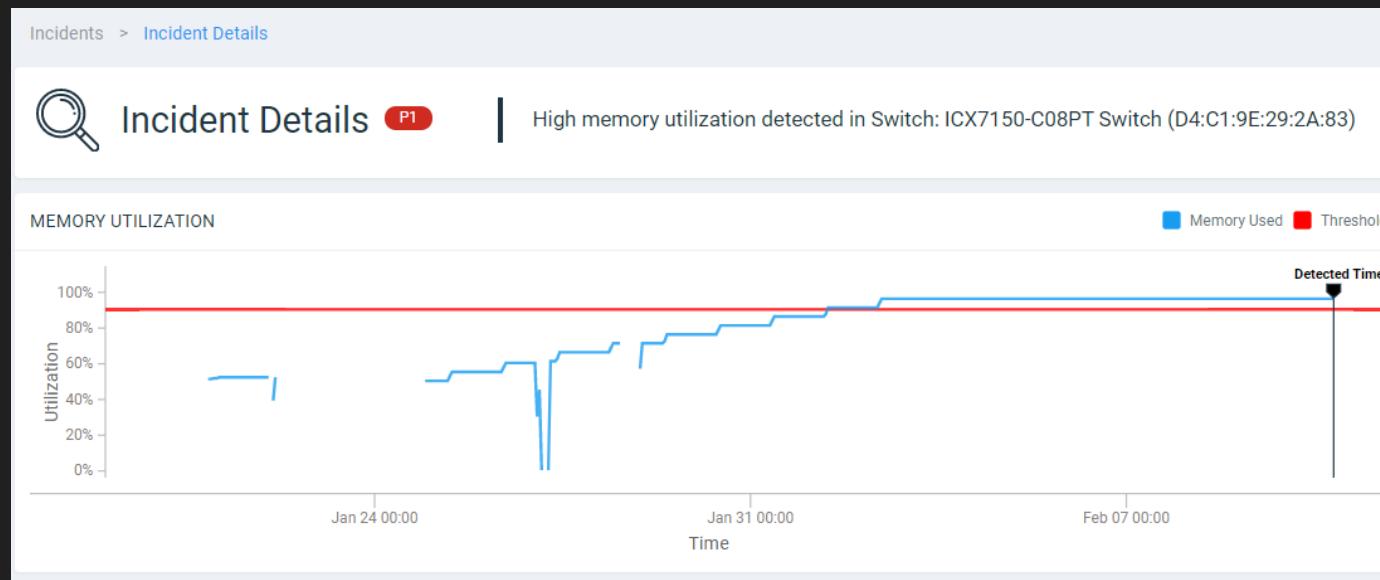
- Controller reads ICX switch memory utilization for every managed switch
- Using telemetry architecture described earlier, this information is passed to RA
- RA has algorithms to measure baseline memory usage of every switch and compute a worst case upper bound for memory utilization
- Here is an example of maximum memory utilization at 50%



- Actual memory utilization is continuously tracked and compared to the upper bound using moving window regression analysis
- In case of increasing memory usage, based on the rate of increase of memory utilization a projection is made about when worst case upper bound will be reached and insight generated

# High Switch Memory Utilization

- Automatic classification and rising priority based on time to failure
- This insight can be P1, P2 or P3 depending on time to failure. P3 with 10 days, P2 with 7 days, P1 with 3 days to failure



 **INSIGHTS**

**ROOT CAUSE ANALYSIS**

System has detected abnormally high memory utilization in the switch. At the current rate, the switch will reach threshold limit\* soon, as indicated in the graph.

Switch might run out of memory if the memory usage rate continues. This is typically indicative of a memory leak in the switch.

\*Note: Threshold limit is auto-calculated by the system.

**RECOMMENDED ACTION**

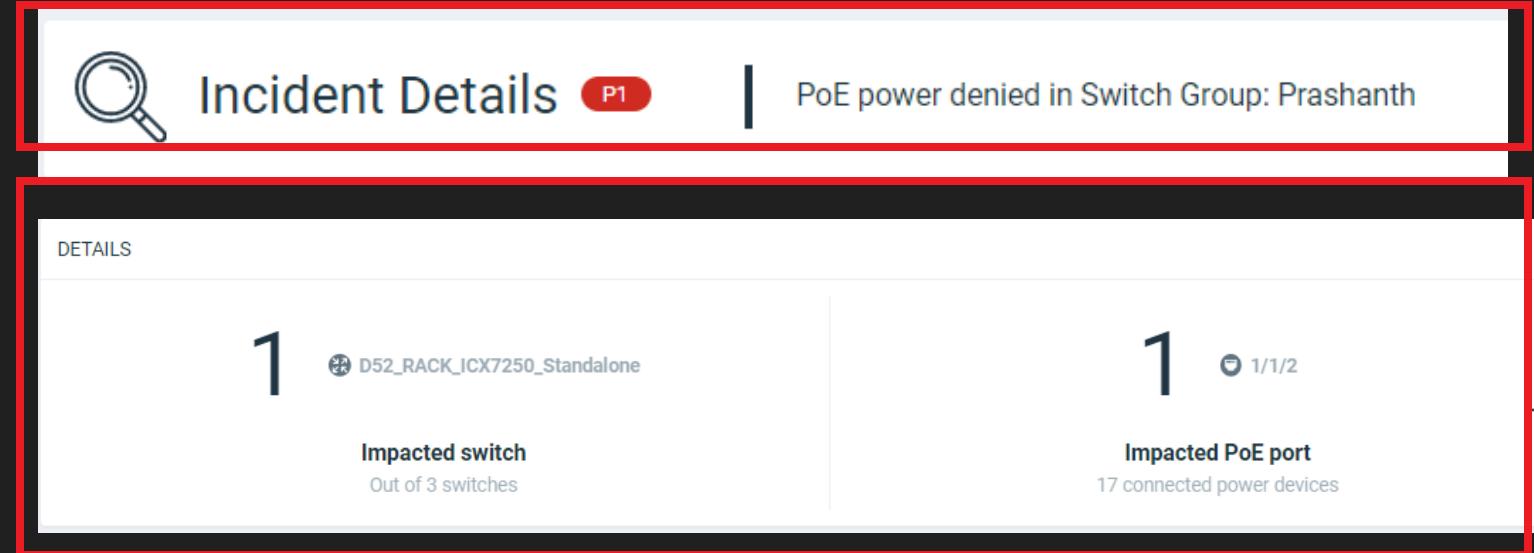
P3 - Contact RUCKUS Support.  
 P2 - Schedule a maintenance window and reboot the switch if the memory utilization continues to increase. Contact RUCKUS Support.  
 P1 - Schedule a maintenance window and reboot the switch if the memory utilization continues to increase. Contact RUCKUS Support.

**INCIDENT INFO**

Incident Category	Performance
Incident Sub-Category	Memory
Type	Switch
Scope	ICX7150-C08PT Switch (D4:C1:9E:29:2A:83)
Duration	12d 21h
Event Start Time	Jan 29 2021 00:00
Event End Time	Feb 10 2021 21:00



# PoE Insight – PoE power denied in Switch Group



**Incident Details** P1

PoE power denied in Switch Group: Prashanth

**DETAILS**

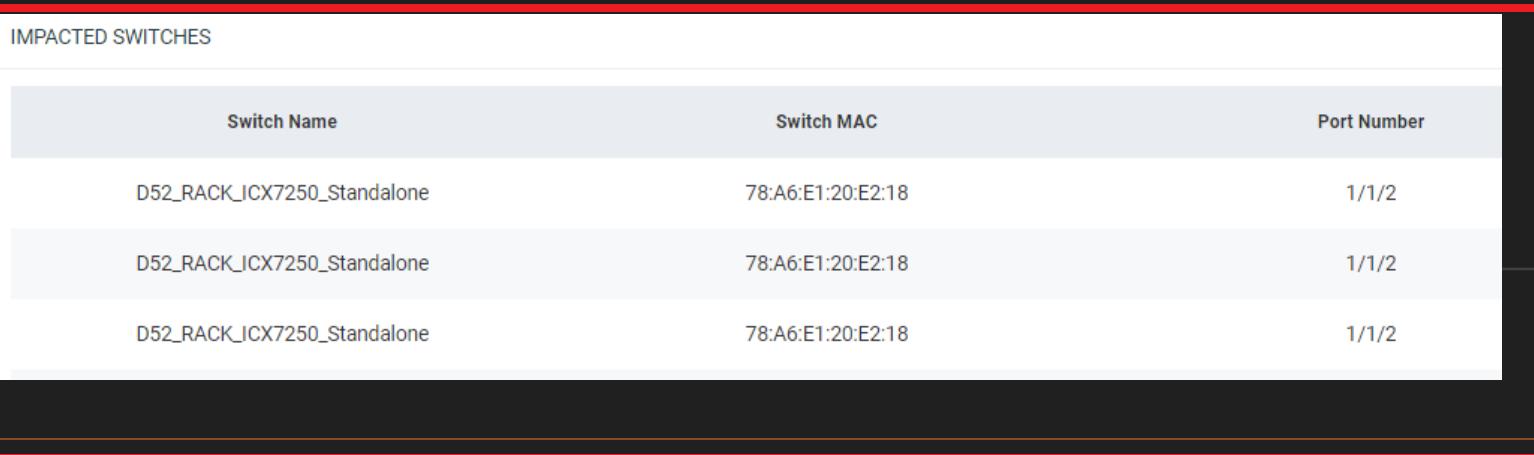
1	D52_RACK_ICX7250_Standalone
Impacted switch Out of 3 switches	

1	1/1/2
Impacted PoE port 17 connected power devices	

P1 Incident, PoE power denied in Switch Group, IT can take action

Impacted Switch name and count

Impacted Port count



Switch Name	Switch MAC	Port Number
D52_RACK_ICX7250_Standalone	78:A6:E1:20:E2:18	1/1/2
D52_RACK_ICX7250_Standalone	78:A6:E1:20:E2:18	1/1/2
D52_RACK_ICX7250_Standalone	78:A6:E1:20:E2:18	1/1/2

Each row represents impacted port number.  
Port Number format:  
**Stack Unit Number / Module / Port Number**

# PoE Insight – Root cause and Recommendations

- RAI shows switch, port number and reason for why power has been disabled at the port
- RAI lists all impacted Stack Units, modules and port numbers
- Root cause and recommendation is displayed along with the insight

A circular icon containing a white lightbulb with a brain-like shape inside, set against a dark background.

## INSIGHTS

### ROOT CAUSE ANALYSIS

PoE power has been denied due to power exhaustion or because another high priority device is plugged in.

### RECOMMENDED ACTION

Increase power capacity by adding a second power supply or add additional switches if the switch doesn't have pluggable power supply. If the switch is part of a stack, connect the device to a different switch in the stack based on proximity.

1. If there is no more room for adding power supplies either due to the switch type or all the power supply slots are used, increase power capacity by adding additional switches because there is no room to add more power supplies.
2. If the switch has room for more power supplies, increase power capacity by adding a second power supply.



**PURPOSE-DRIVEN**  
ENTERPRISE NETWORKS