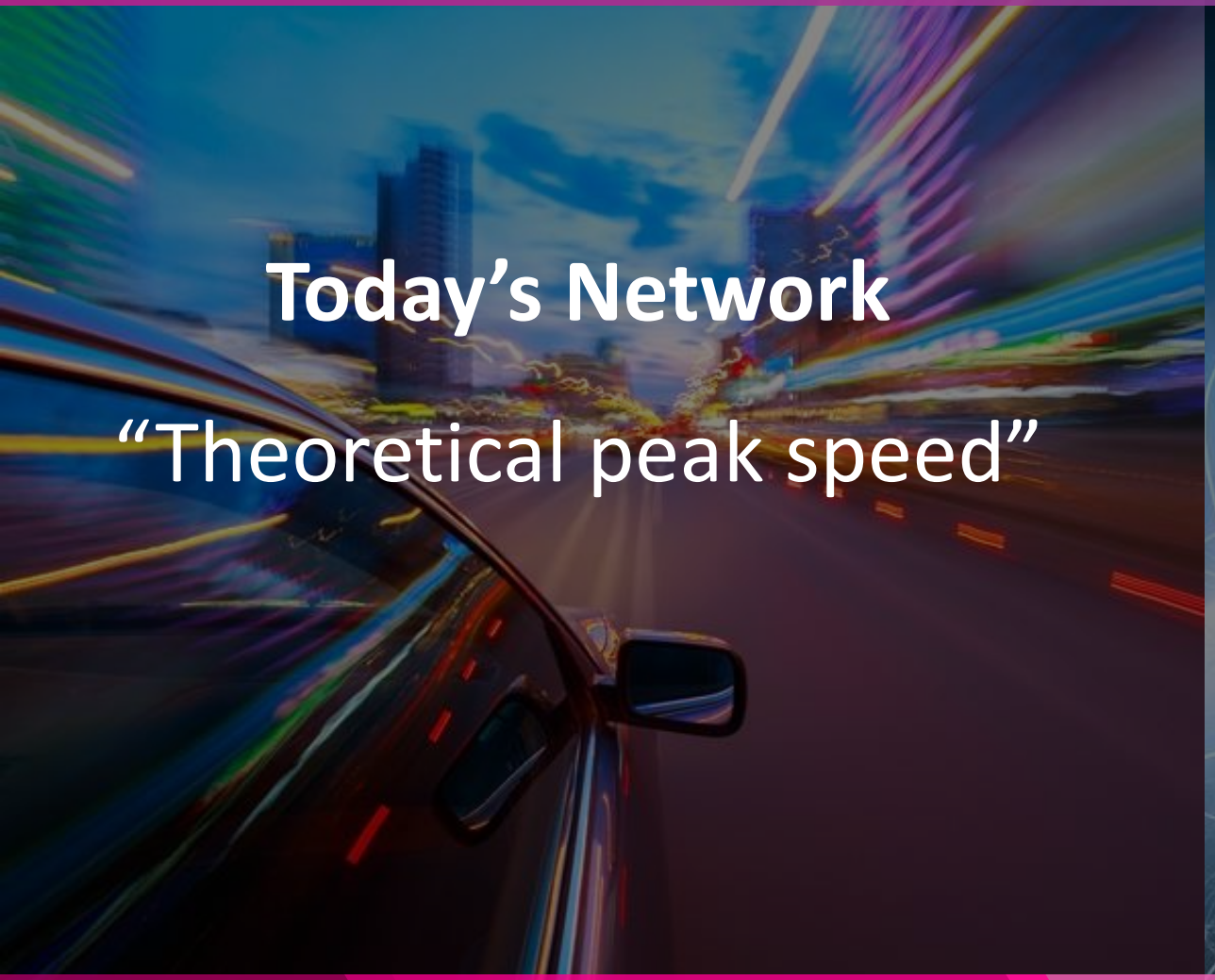
Wi-Fi 6無線安全應用及智慧管理

Kevin Su

Technical Consultant

無線演進過程



Today's Network

"Theoretical peak speed"

Tomorrow's Network

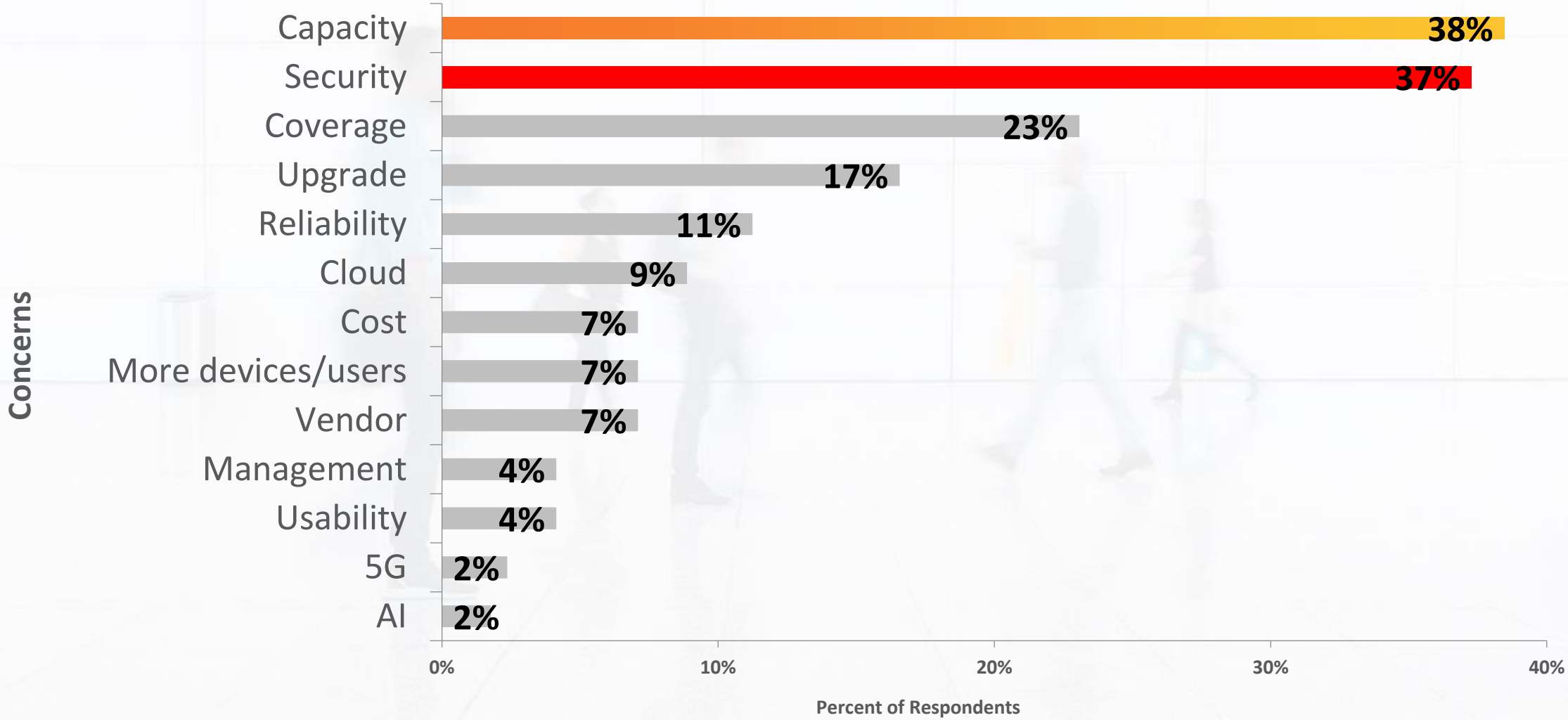
"Overall network capacity"

11a | 11b | 11g | 11n | Wi-Fi 5 (11 ac) | Wi-Fi 6 (11 ax)

僅使用Wi-Fi辦公的人越來越多

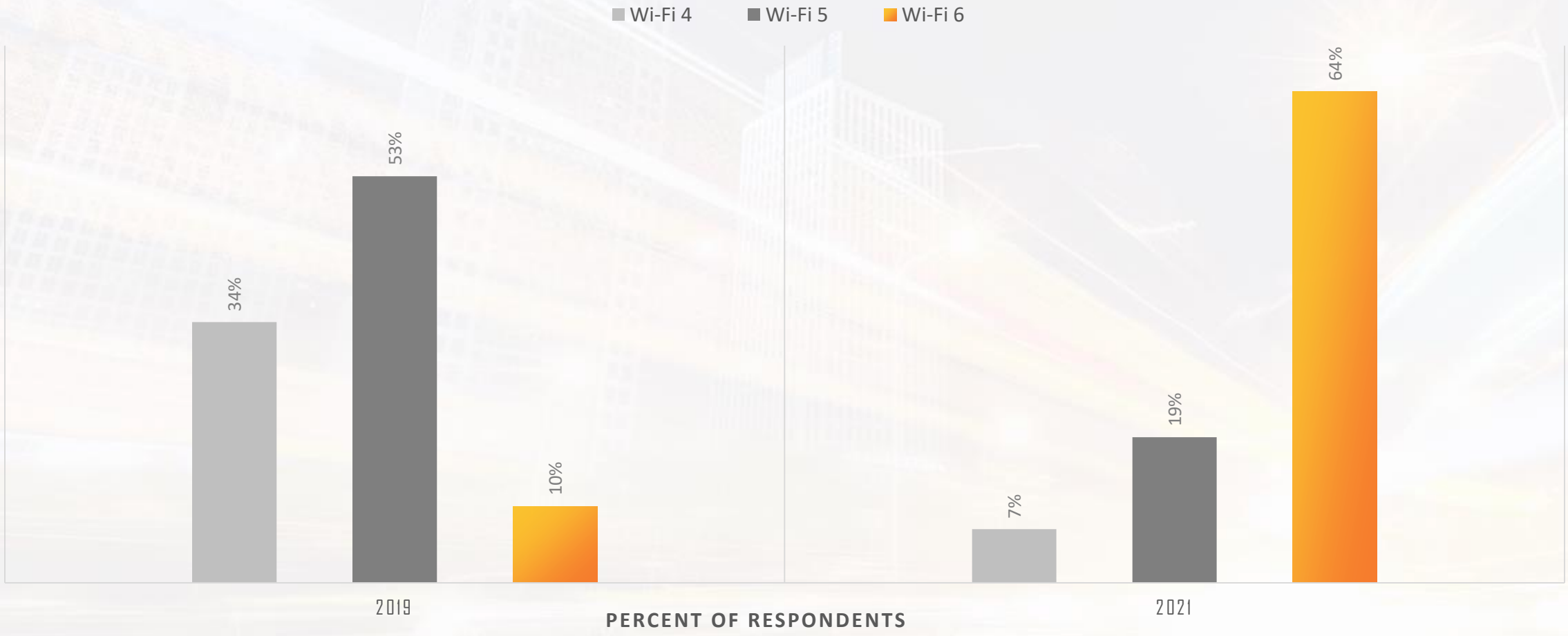
Source: IHS Markit WLAN strategies North American enterprise survey, August 2019

企業最在意的無線網路要素



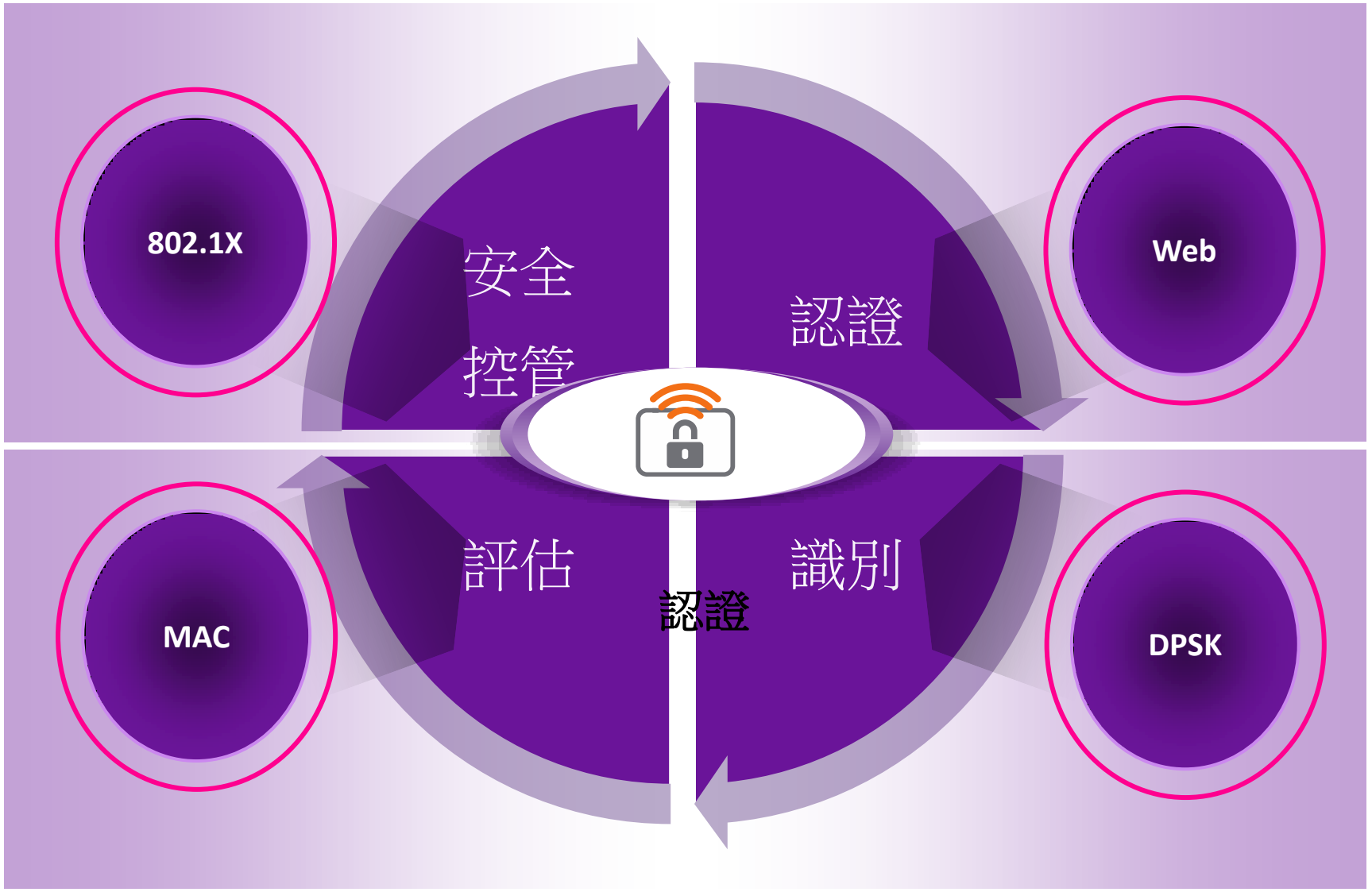
Source: IHS Markit | Technology, now part of Informa Tech, WLAN strategies North American enterprise survey, August 2019

企業加速轉移到Wi-Fi 6



Source: IHS Markit | WLAN strategies North American enterprise survey, August 2019

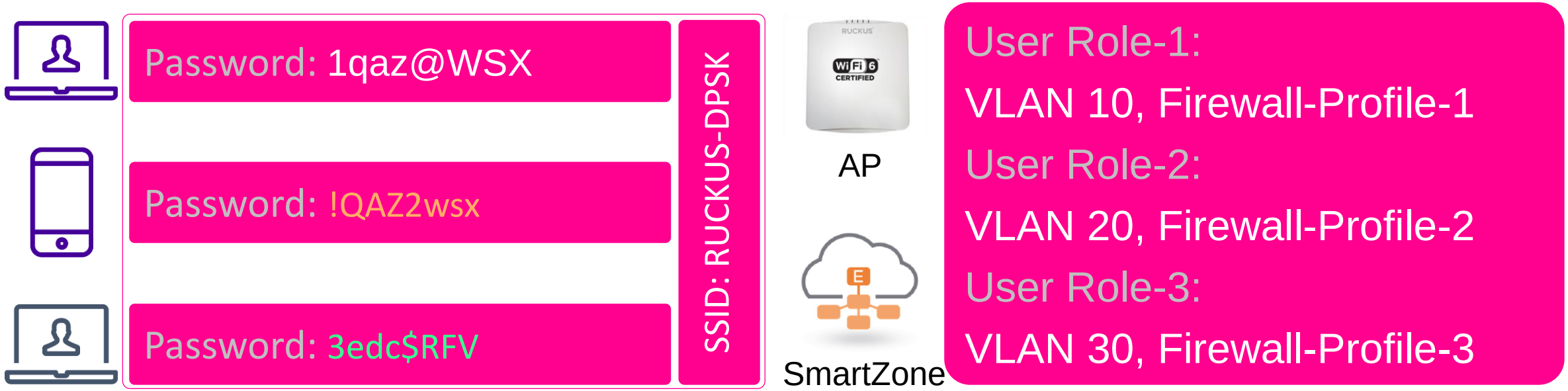
有線無線的端末安全性



認證功能的比較

項目	802.1X 認證	MAC地址認證	網頁認證	DPSK
適用情境	用戶集中且對資訊安全性要求極高的網路	適用於非用戶端裝置的認證，例如印表機和傳真機	訪客或協力廠商存取，並獲取其登入的身分資訊	對資訊安全性要求高的網路，且希望簡單配置
用戶端程式	需要	不需要	瀏覽器	不需要
優點	高安全性	容易設定、無須安裝終端	彈性佈署	容易設定、無須安裝終端和RADIUS
缺點	佈署不易	管理MAC地址麻煩，不適合大規模佈署，MAC地址容易偽冒	低安全性，如使用HTTPS因憑證因素有無法重導顯示認證網頁的問題	行動裝置如手機、平板等，需手動配置

DPSK – Dynamic Pre-Shared Key



- 每個使用者都有獨一無二的DPSK
- 當使用者離職或遺失裝置，可以隨時取消該DPSK
- 同一個SSID可以擁有多個User-Role
- DPSK可以用於一群裝置或是綁定特定的裝置MAC

COMMSCOPE®

MAC Randomization issues and how Ruckus solves it.

Apple iOS 14 **Before and After**

Beta 3

- Random MAC for probing
- Random MAC enabled by default
- Random MAC for each network joined
- MAC addressed changed every 24 hours

Beta 4 & beyond

- Random MAC for probing
- Random MAC for each network joined
- Random MAC enabled by default
- MAC address used for each network doesn't change;
  - Network is forgotten
- Don't discount the timing change

Apple iOS 15 **Will Wreak Havok!**

COMMSCOPE®

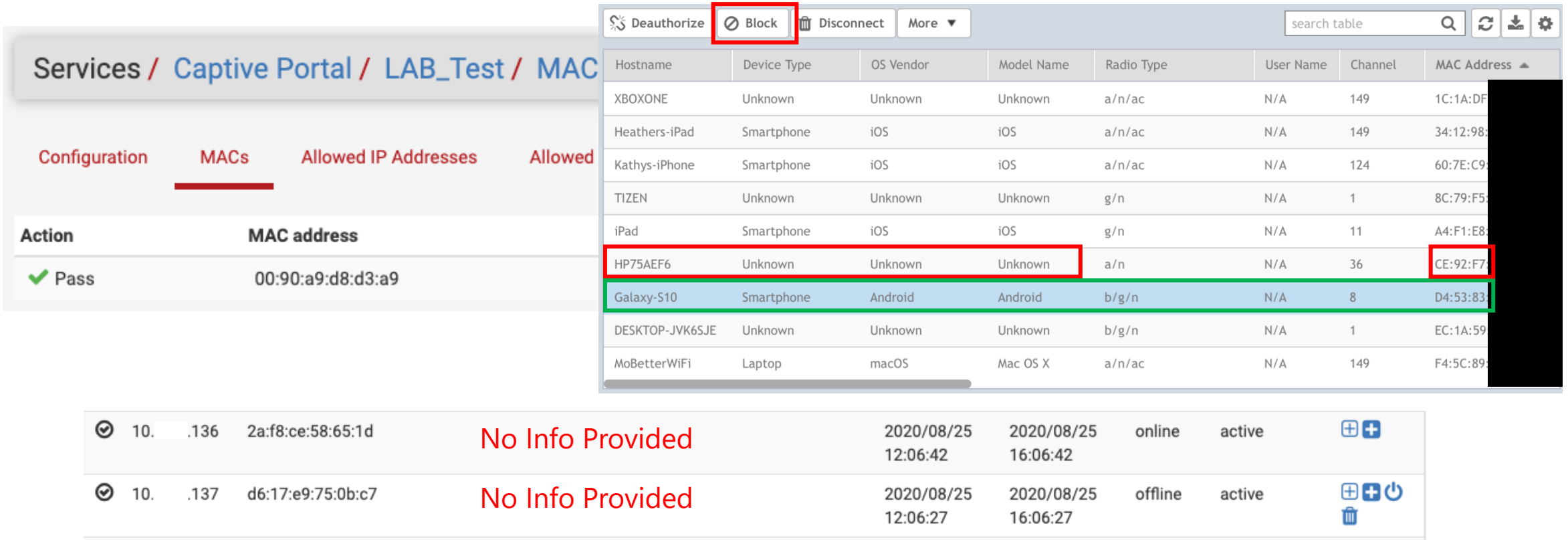
What & When

- Apple = Predictability
- Android = Uncertainty
- Expect mobile OS to go fully random soon
- Expect desktop OS to lag but get there
- Forgetting any network = Random MAC

Operating System	Supports MAC Randomization	Defualt Status	Network Based per SSID	Time Based. (24 hours)
Apple iOS 13	NO	N/A	N/A	N/A
Apple iPadOS 13	NO	N/A	N/A	N/A
Apple iOS 14	YES	ENABLED	ENABLED	NO**
Apple iPadOS14	YES	ENABLED	ENABLED	NO**
MacOS 10.15/10.16	NO	N/A	N/A	N/A
MacOS 11 Big Sur	NO	N/A	N/A	N/A
Android 9	YES	DISABLED	OPTIONAL	NO
Android 10	YES	Carrier / Vendor Specific	Carrier / Vendor Specific	NO
Android 11	YES	ENABLED ^	ENABLED ^	OPTIONAL
Windows 10	YES	DISABLED	OPTIONAL	OPTIONAL
ChromeOS	NO	N/A	N/A	N/A

** Beta 3 this was enabled, disabled in Beta 4, expect to see it enabled in iOS 15

^ Expect to see the same Vendor/Carrier specifics



Security Impact

- MAC Authentication
- Captive Portal
- Block List
- 802.1X
- DPSK

x2:xx:xx:xx:xx:xx

x6:xx:xx:xx:xx:xx

xA:xx:xx:xx:xx:xx

xE:xx:xx:xx:xx:xx

1 Device = Multiple IPs

1[redacted]20	00:1e:06:[redacted] (Wibrain)	homeassistant	Home Assistant Odroid Server	n/a	n/a	online	static	
1[redacted]32	00:90:a9:[redacted] (Western Digital)	mycloud	My Cloud NAS	n/a	n/a	online	static	
[redacted]	[redacted]	[redacted]	[redacted]	2020/08/25 12:06:27	2020/08/25 16:06:27	offline	active	

Reserved DHCP

IP Based ACL / Firewall

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
Servi	0 /0 B	IPv4 *	192.168.1.50	*	192.168.10.0/24	*	*	none		Allow MacBook Air Access to LAB subnet

Configuration | MACs | Allowed IP Addresses | Allowed Hostnames | Vouchers | File Manager

IP Addresses	Description	Actions
⇄ 1[redacted]1	Office ICX-7150	

→ = All connections to the address are allowed, ← = All connections from the address are allowed, ⇄ = All connections to or from are allowed

Allowed IP Addresses

DHCP Impact:

Unknown MAC means random IP

- Random IP breaks:
  - Reserved DHCP
  - Captive Portal Bypass
  - Layer 3 Firewall or ACLs
  - DHCP Pool Exhaustion

x2:xx:xx:xx:xx:xx

x6:xx:xx:xx:xx:xx

xA:xx:xx:xx:xx:xx

xE:xx:xx:xx:xx:xx

COMMSCOPE®

Troubleshooting

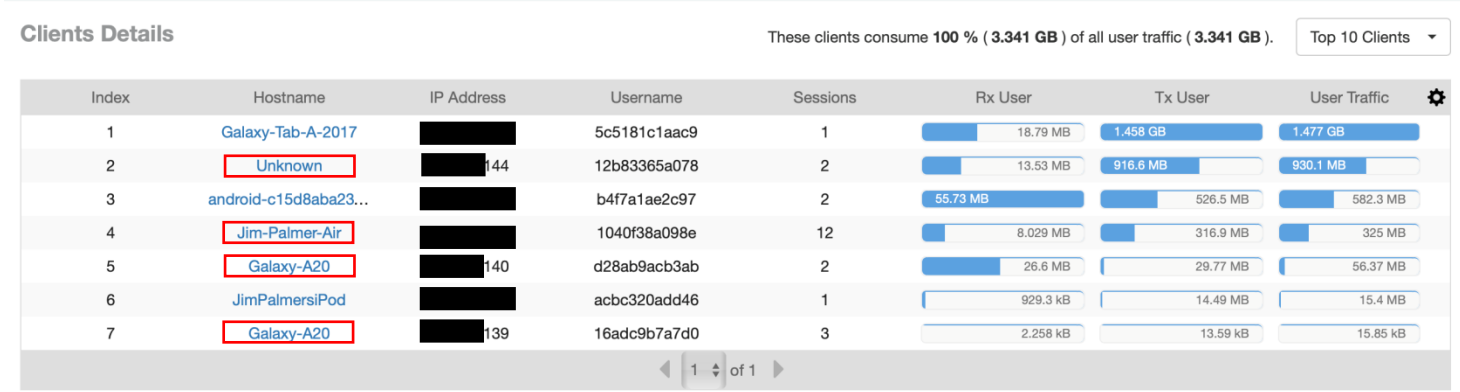
- Identify Clients?
- RUCKUS Analytics
- Client Operation
  - Band Steering?
  - Band Balancing?

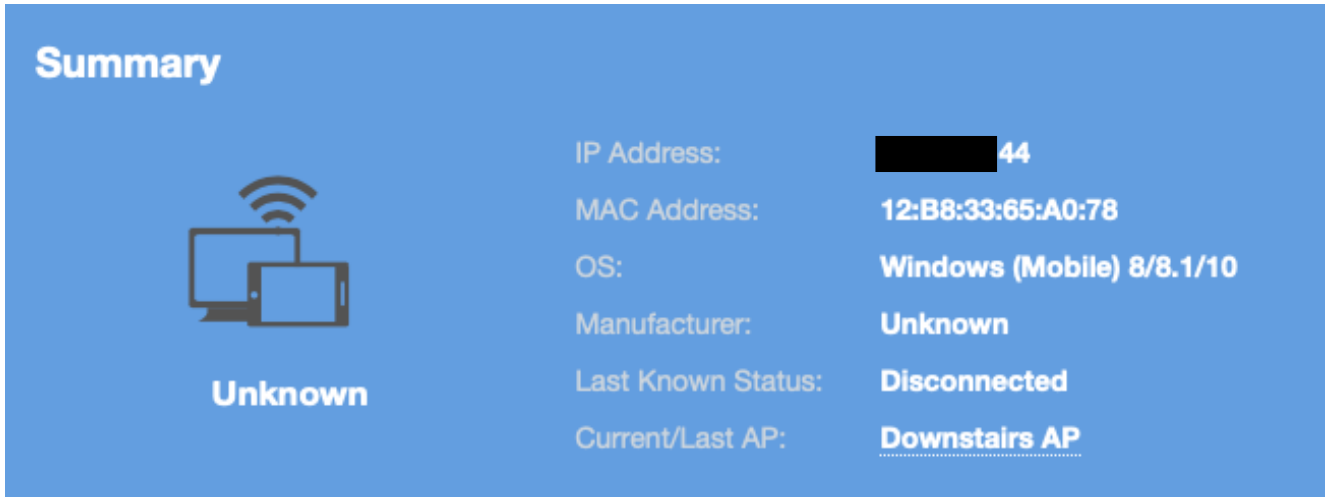
x2:xx:xx:xx:xx:xx

x6:xx:xx:xx:xx:xx

xA:xx:xx:xx:xx:xx

xE:xx:xx:xx:xx:xx





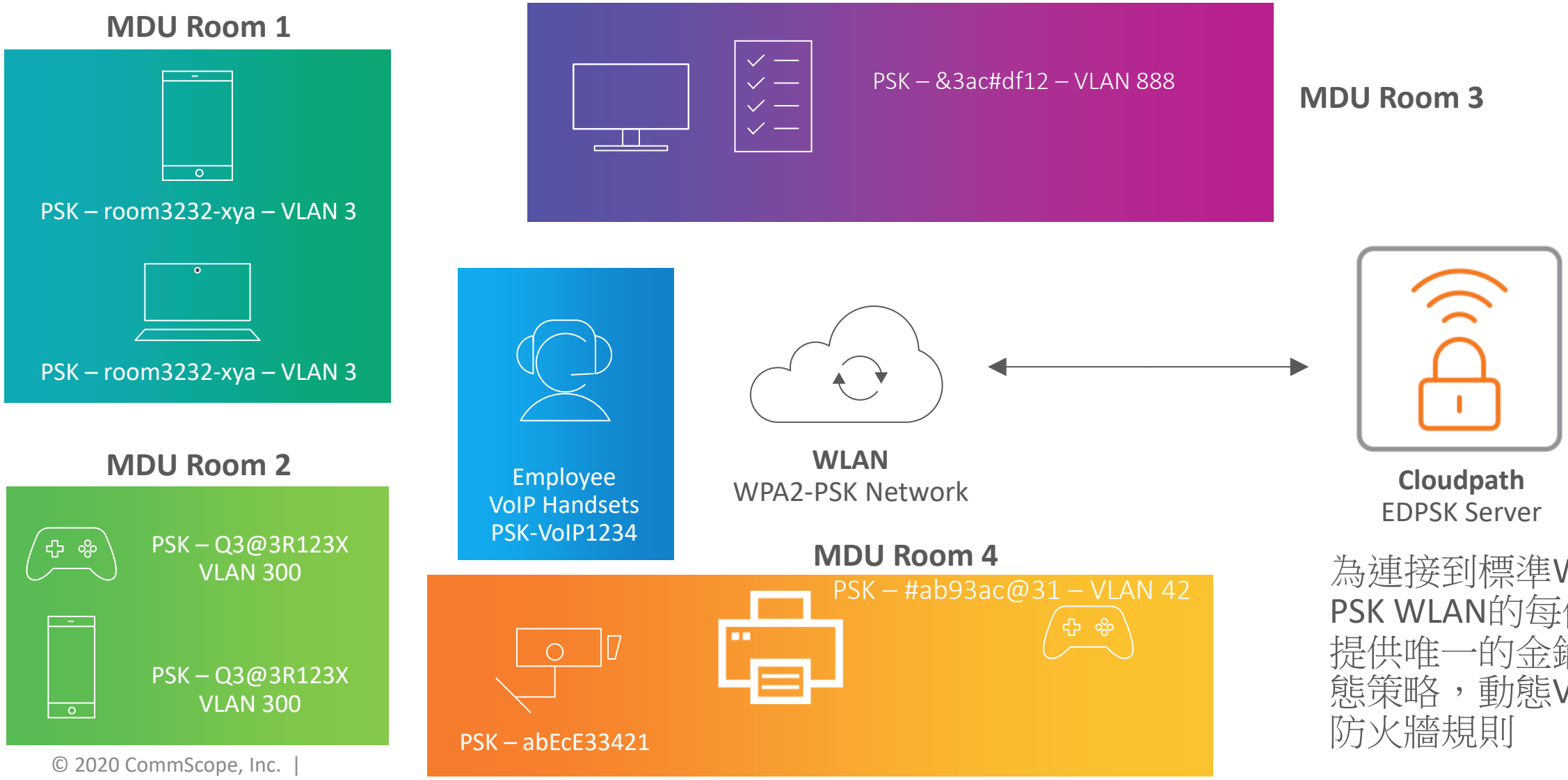
如何解決MAC Randomization帶來的問題

- 連線前停用MAC專用位址/隨機化MAC
- 使用802.1x認證
- 使用eDPSK/Group DPSK

eDPSK概觀

- Ruckus是動態預先共享金鑰技術的先驅，並且是第一個開發OTA配置的廠商。
- 與共享的PSK相比，DPSK顯著增強了Wi-Fi安全性和可管理性。
- DPSK可以與RBAC（VLAN，速率限制，L3-L7策略）綁定在一起，以提供完整的設備策略管理。
- 儘管不像802.1X身份驗證那樣完全基於標準，但由於它利用WPA2（目前），因此可以與更多的設備相容。
- DPSK的使用是一個很大的成長領域：包括MDU，學生住宿，飯店，可管理的商業辦公室，醫療保健，物聯網設備等。
- 無線控制器對可管理的DPSK數量上有限制，而eDPSK是透過RADIUS，因此理論上沒有限制

External DPSK帶給使用者的好處



為連接到標準WPA2-PSK WLAN的每個裝置提供唯一的金鑰，動態策略，動態VLAN，防火牆規則

Cloudpath Key Features

Onboarding Portal

Self-service portal automatically provisions devices for the Wired and Wireless networks

802.1X Based

PKI policy-enabled certificates tie User, Device & Policy together PEAP/MSChapV2

Enrollment Record

Tracks who, what, & when is onboarded and authenticated

Policy Controls

eDPSK, auto-VLANs, ACLs, Policies based On User/Groups, Devices & Browser/OS, Policy Engine

Broad Device Support

iOS, Android, ChromeOS, Mac OS X, Windows & Linux

Reliability

Eliminate password-related disconnects, support costs, and security problems

MDU Portal – Use Case

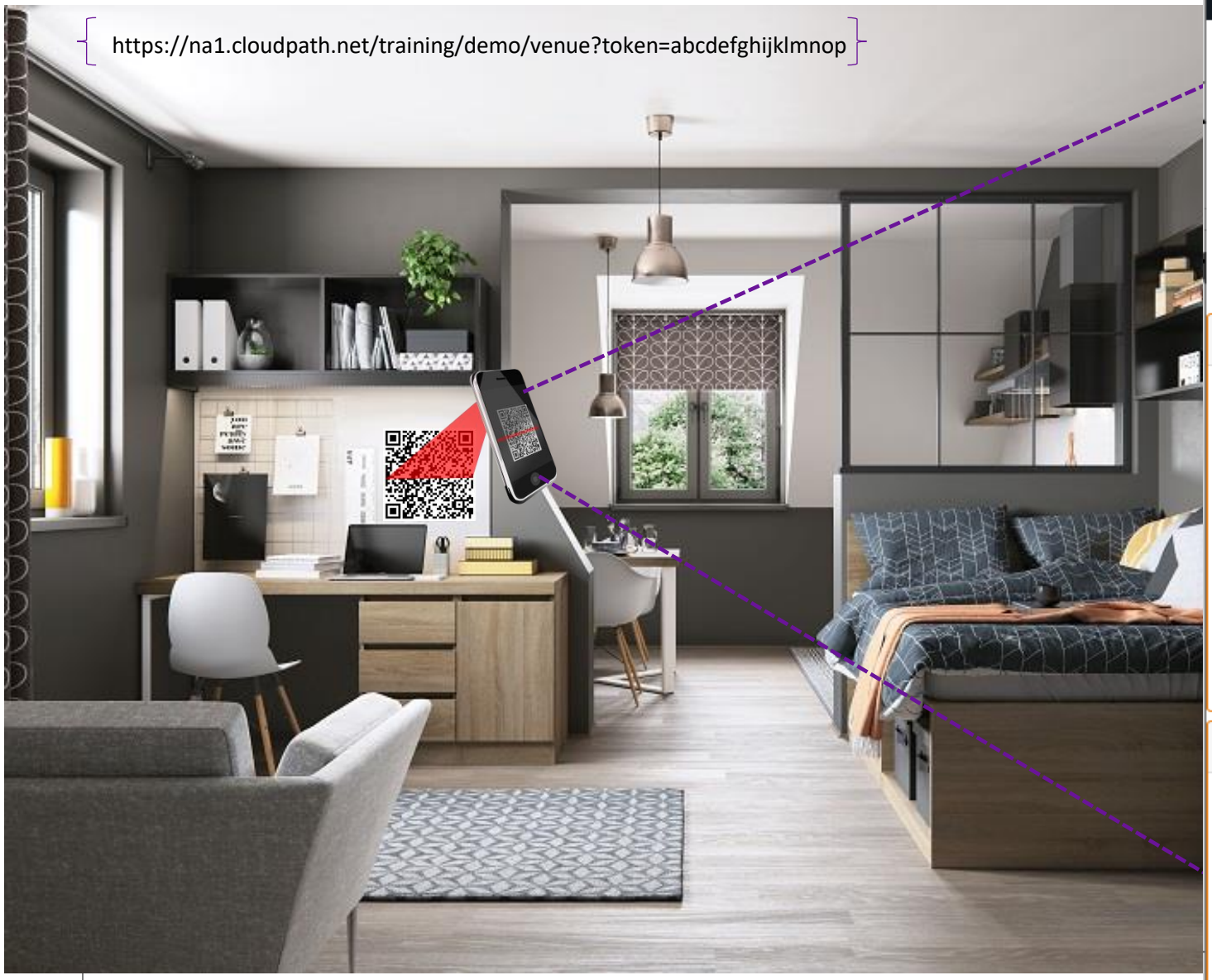
MDU Device Examples:

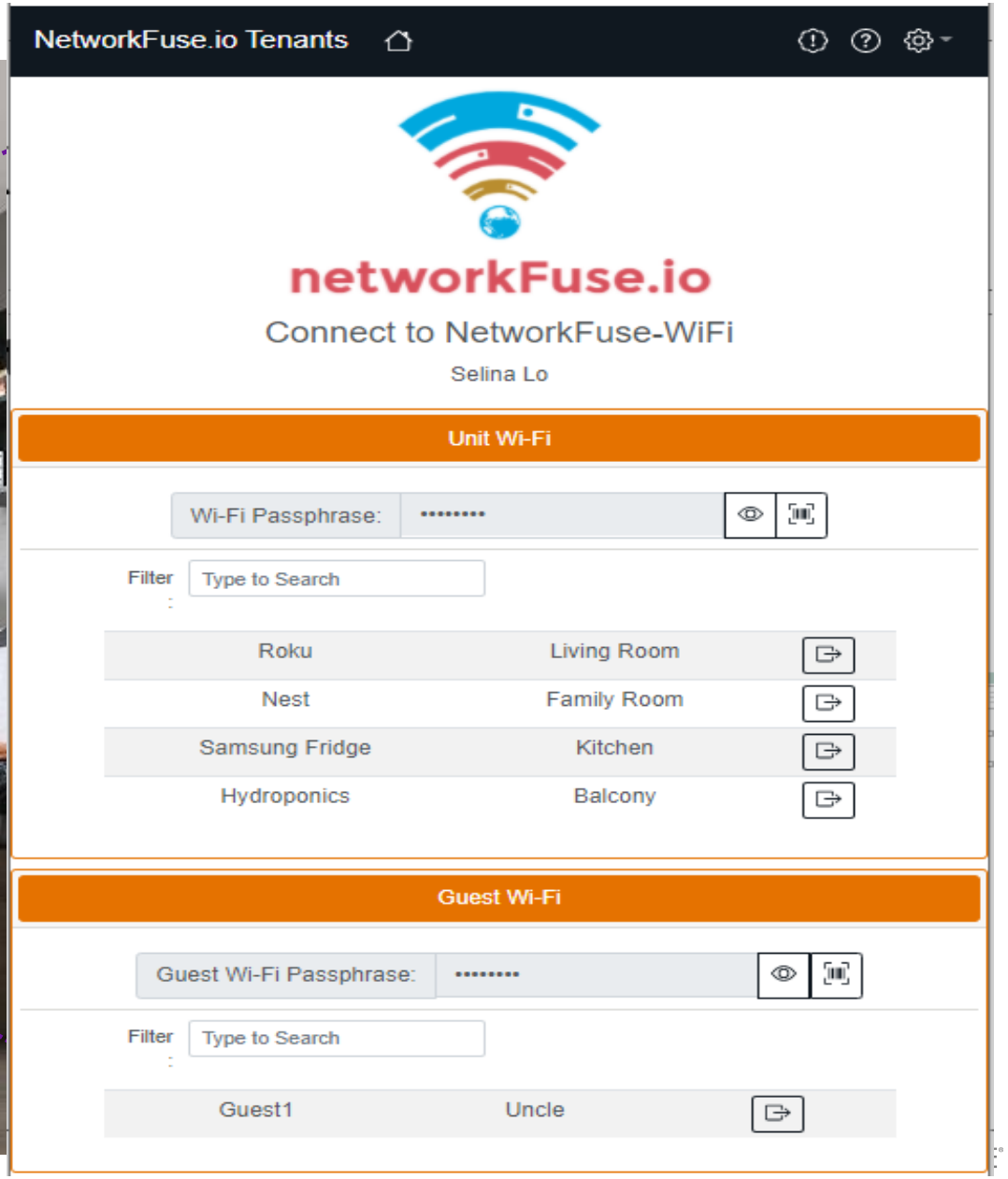
1. Phones
2. Tablets
3. Lighting
4. Gaming Machines
5. Desktops
6. Speakers
7. Printers
8. Laptops
9. Thermostat
10. **Hydroponics**
11. Smart plugs
12. Cameras

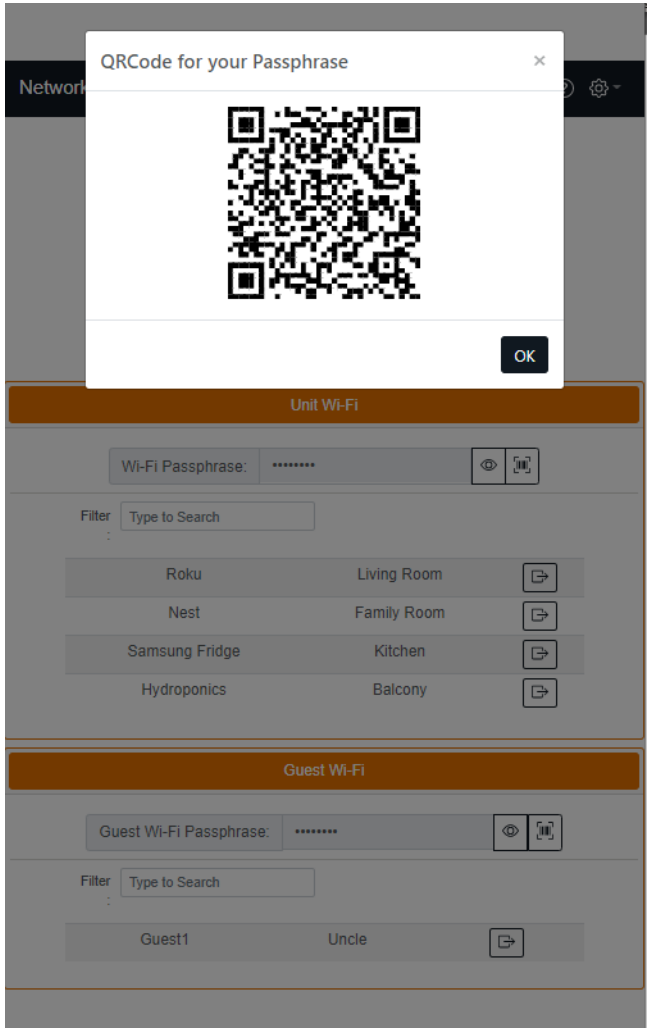
How do we connect these devices, give them a secure network and ensure communication between these devices?

How do we solve headless devices?

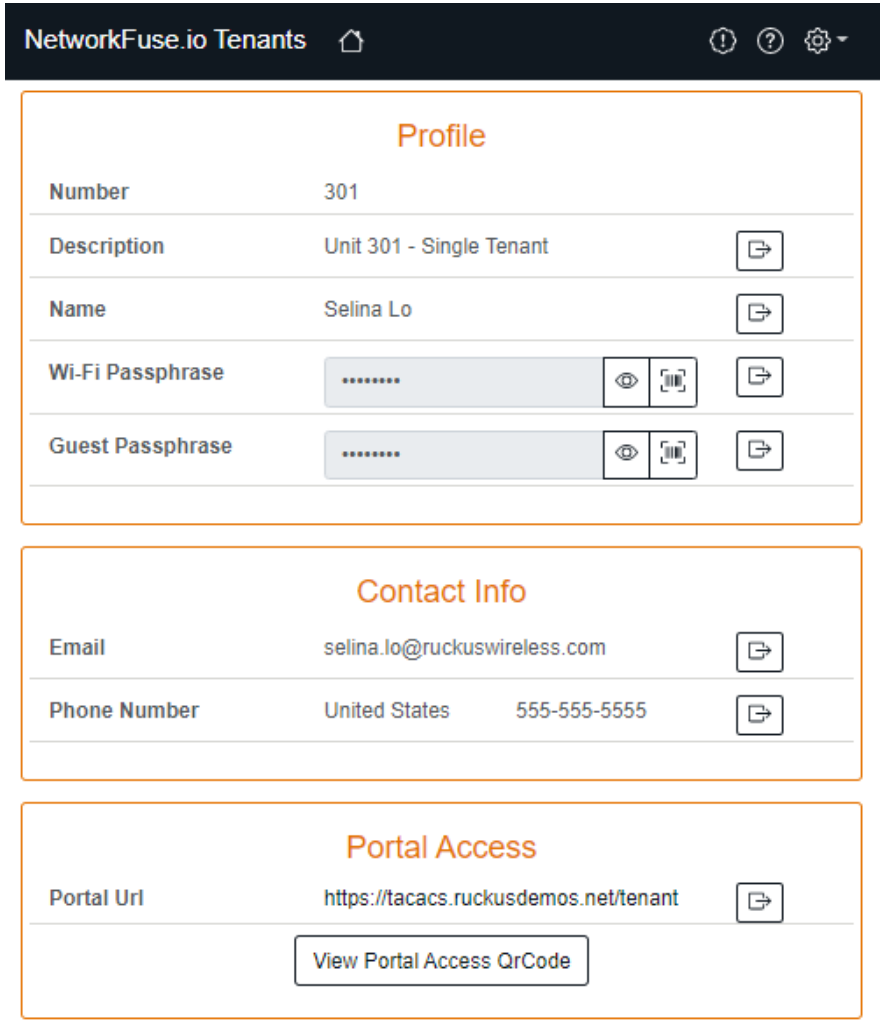
Customer Experience: Access Tenant Portal Via QR Code/URL/App



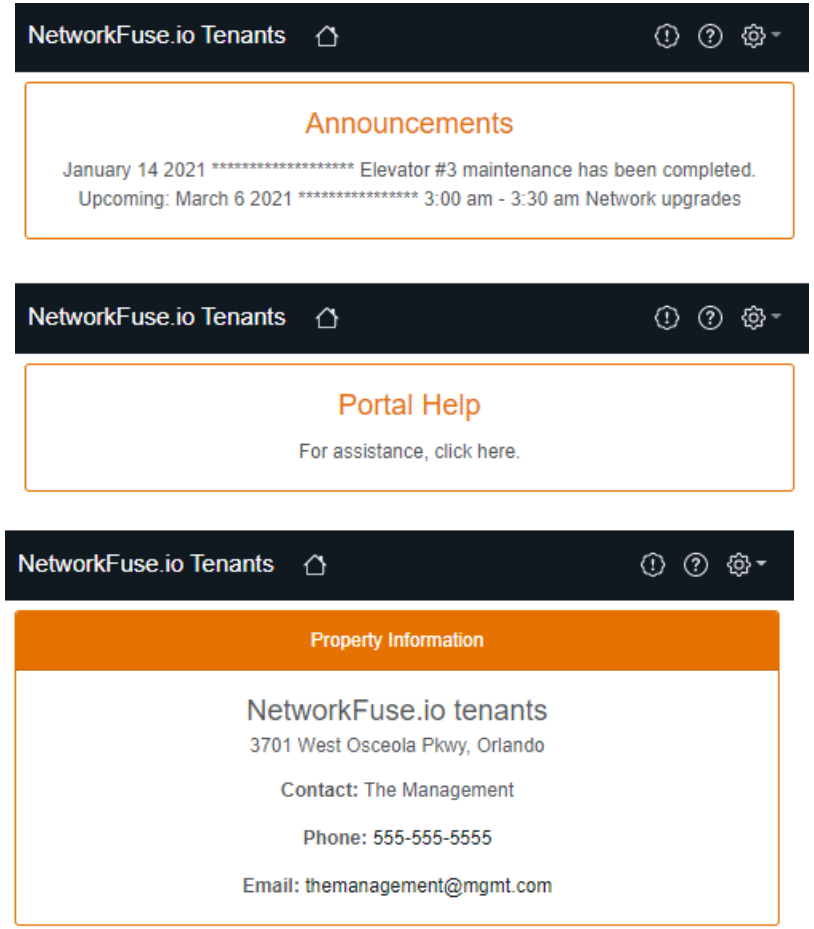




- Customer self service
- Modern UI, scalable for any device
- View DPSK in a QR code for easily onboarding devices

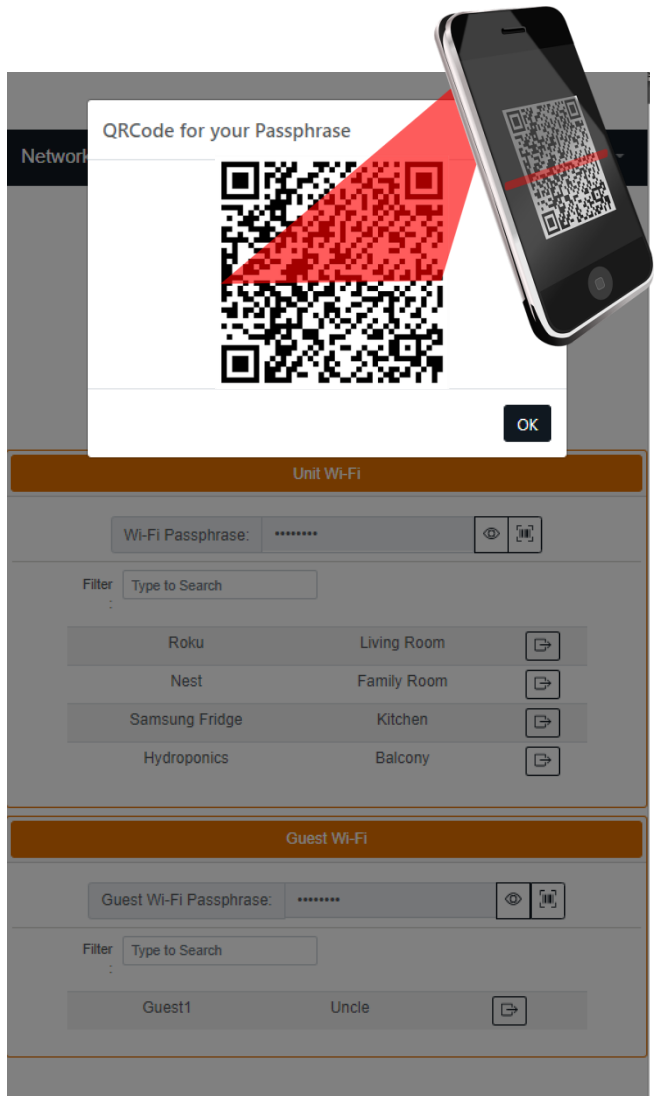


- Customers can self Manage their own portal
- Change DPSK passphrases, email, phone numbers
- Download a QR code for portal access
- Change their secret token



- See announcements
- portal assistance
- property information
- Auto logs out after idle time

Scan From Screen or Print it off

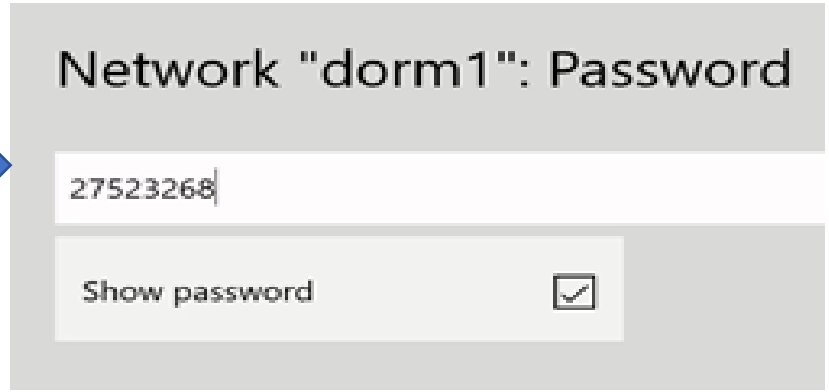


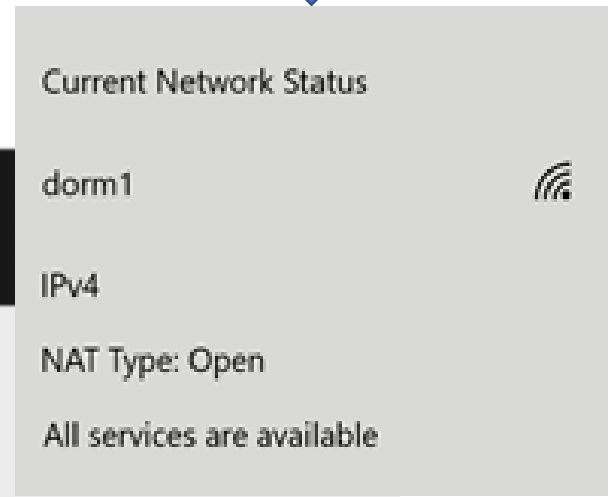
Use iPhone/Android device to take a picture of the QR code.

Once scanned, this prompts the user to join the network.

The QR Code already contains the WLAN profile, including SSID, Security, and DPSK!

Device Joins the Network, no need to configure the WLAN on the end device!





COMMSCOPE® RUCKUS®

Cloudpath Enrollment System

- Dashboard
- Welcome
- **Connections**
- Enrollments
- DPSKs

Show: Connections | Disconnects | **All**

Controls	Status	IP Address	MAC Address	Username	SSID	Duration
					dorm1	
	Connected	192.168.10.111	CE:7E:4E:A1:54:FB	KS-Building-01_601	dorm1	15 seconds ago
	Connected	192.168.10.110	86:95:C9:EC:39:C4	KS-Building-01_501	dorm1	48 seconds ago

Results 1 - 2 of 2. 15

Property Information

KS-Building-01

Contact: Kevin Su

Phone: +886975725

Email: kevinsu@gmail.com

今天 下午 8:18

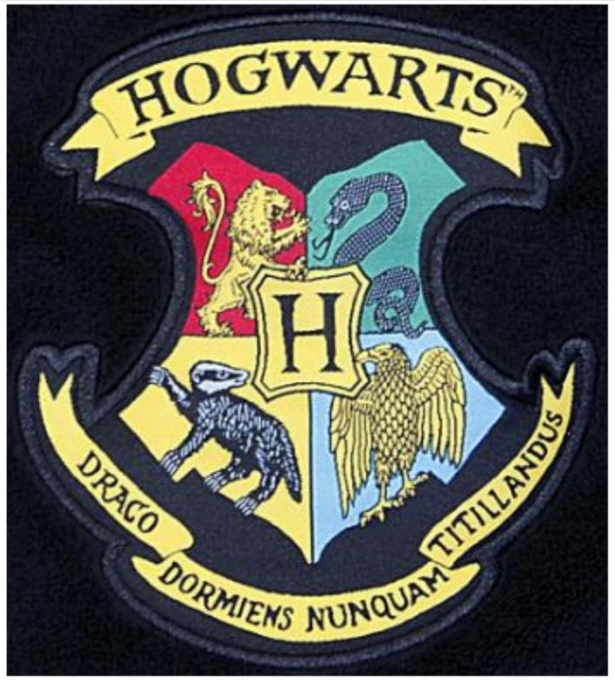
A Unit at KS-Building-01 has been assigned to you. Wi-Fi Passphrase: xatbuymz. Guest Wi-Fi Passphrase: jxhcztbc. Portal may be accessed at: https://ruckus.seclub.tw/tenant?&auth=CPNENCv2%3ABC%7C4377DA9C-3303-4469-90FF-69EB8FA749DF%7CUfv5OIVPhxShYxE4LTOPZg%3D%3D%3AXWpxv3fBdoXzKzQJCU4euQ%3D%3D&property=Property-34654423-9471-461b-8784-ab3837b1bbf1&api=BQ2NJbAmAi6p Sent on behalf of Ruckus Wireless

訊息

8:50

◀ 訊息

ruckus.seclub.tw



Kevin Su

Wi-Fi

Wi-Fi Passphrase: ••••••••

Filter:

Type to Search

a2c9d8a8af73

Guest Wi-Fi

8:50

◀ 訊息

大小 ruckus.seclub.tw

QRCode for your Passphrase

OK

Kevin Su

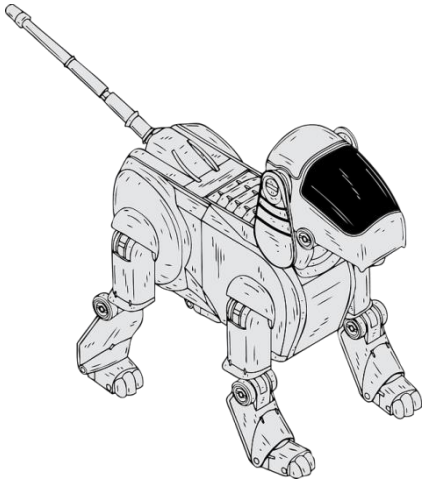
View Your Wi-Fi passphrase QRCode

Wi-Fi Passphrase: ••••••••

Filter:

Type to Search

整合第三方與自動化



Partner Systems

GUI is accessible via API calls:

- Create/Edit/Delete a Property
- Create/Edit/Delete/Suspend a DPSK
- Create/Edit/Delete/Suspend a Unit
- Bulk upload Units
- Create/Edit/Delete a DPSK pool
- Create/Edit/Delete Policies

Cloudpath Customer Reference

Key Metrics:

- 800,000+ End Users
- 2500 Sites
- 38,000 Access Points
- 10,000 ICX Switches
- Completion December 2024 (5 Year Roll Out)

Ministry of Education of New Zealand + Follow ···
27,417 followers
4d •

We are pleased to announce **Exeed NZ** have been awarded the contract for replacing school network hardware as part of the Te Mana Tūhono work programme.

Exeed is a New Zealand IT distributor focused on supplying a range of top technology brands, including **CommScope**'s Ruckus.

Schools will receive new hardware from Ruckus that enables the wireless network to handle multiple simultaneous connections more efficiently using the Wi-Fi 6 technology. Our continued focus is ensuring schools have access to high-speed internet that's reliable, resilient, and safe. **Network for Learning (N4L)** will be upgrading schools with the new hardware.

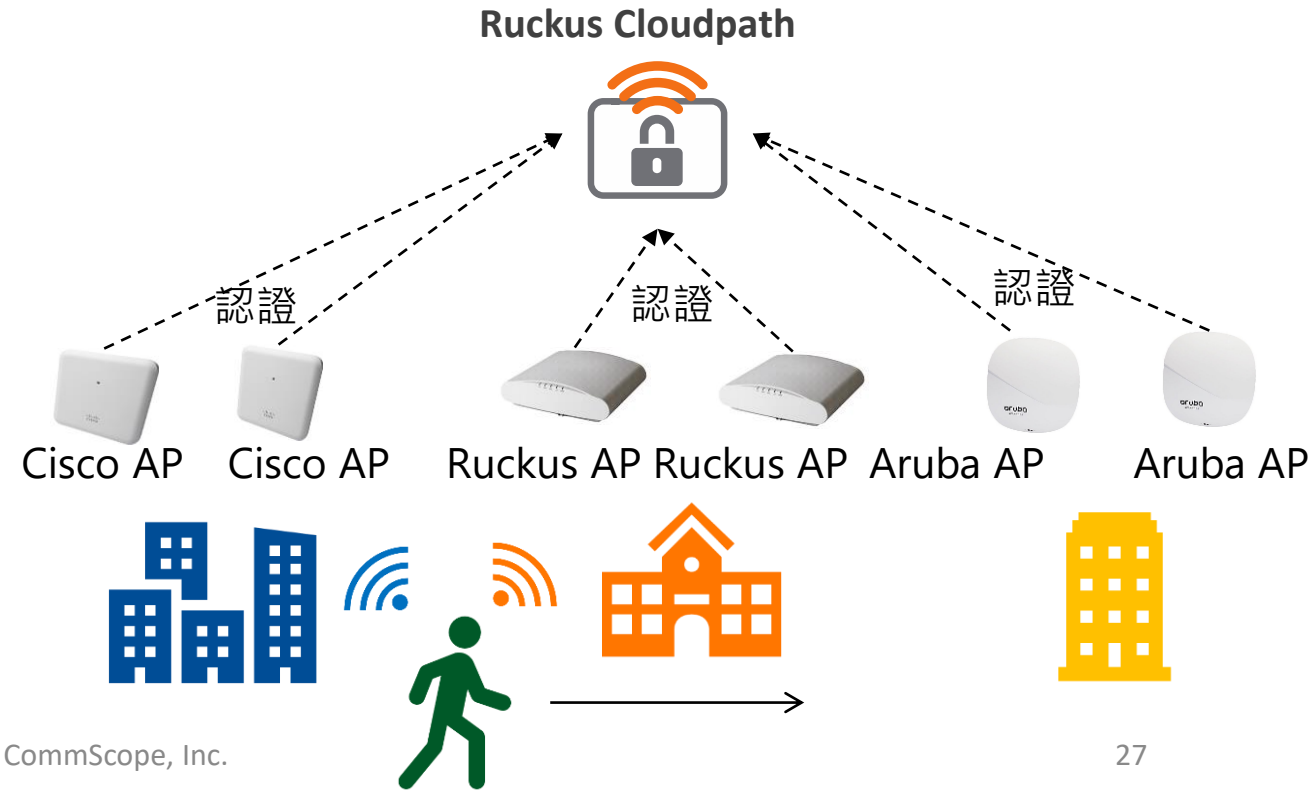
📷: N4L

某大學無線汰換及擴充

- 即有無線網路
  - Cisco AP x 170
  - Aruba AP x 28
- 需求與挑戰
  - 使用都完成認證後,漫遊連接至即有不同廠牌AP,不需重新認證
  - 教職員每三個月才需重新認證
  - 學生每日只需認證一次
- 競爭對手
  - Aruba
  - Cisco
- Why Ruckus
  - Ruckus具較佳的無線效能及涵蓋率
  - Ruckus Cloudpath具簡單認證管理及較低的總持有成本 (by User)

Ruckus Solutions:

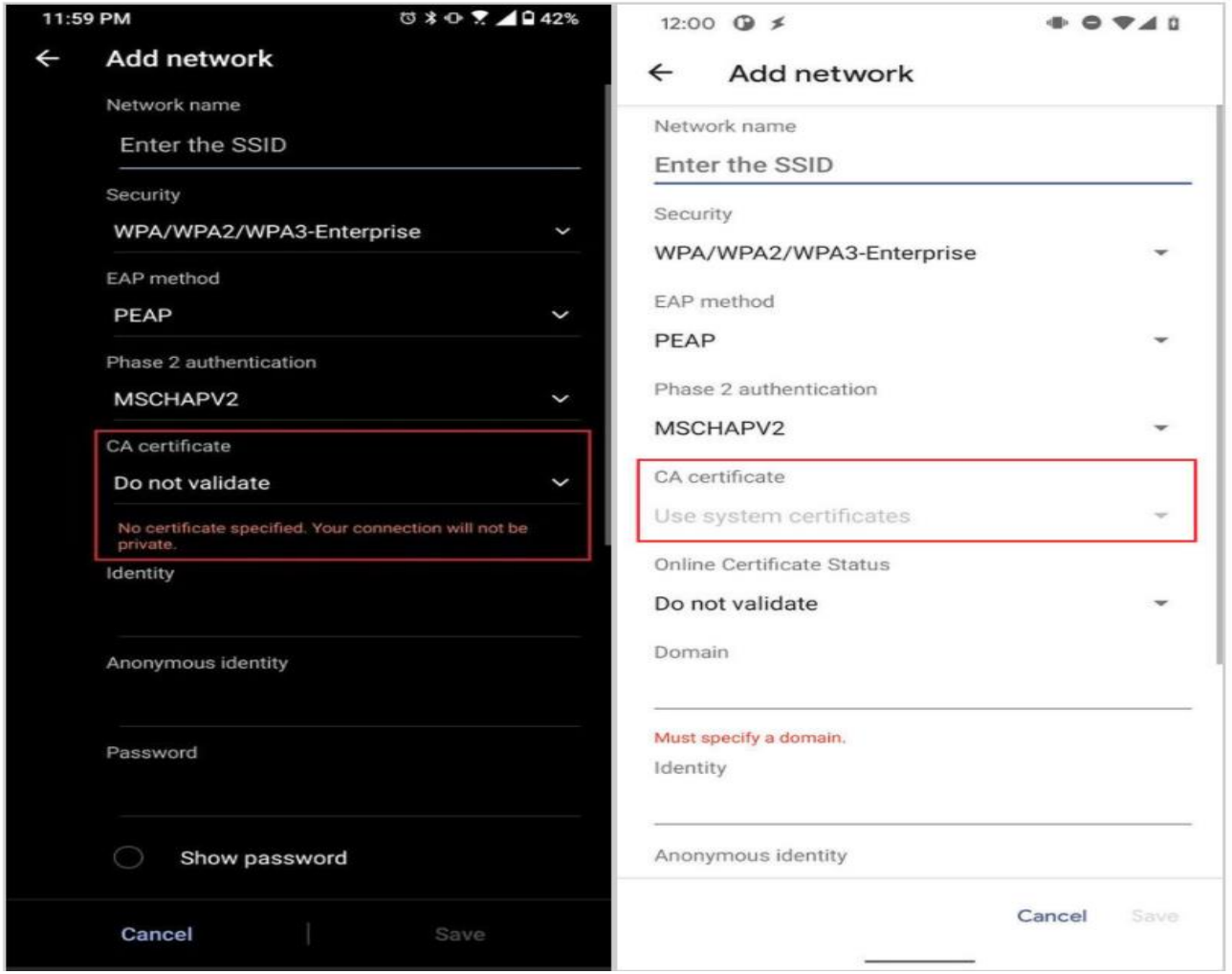
- 第一期汰換擴充
  - Cloudpath 5,000u
  - R720 x20, T610 x9
  - SCI
- 宿舍無線
  - H510 AP x260
- 第二期擴充
  - R730 (8x8 WiFi6) x 3, R720 x 19, T610 x 3



COMMSCOPE®

Android 11 Security Update affects EAP authentication

Android 11 break enterprise Wi-Fi connection

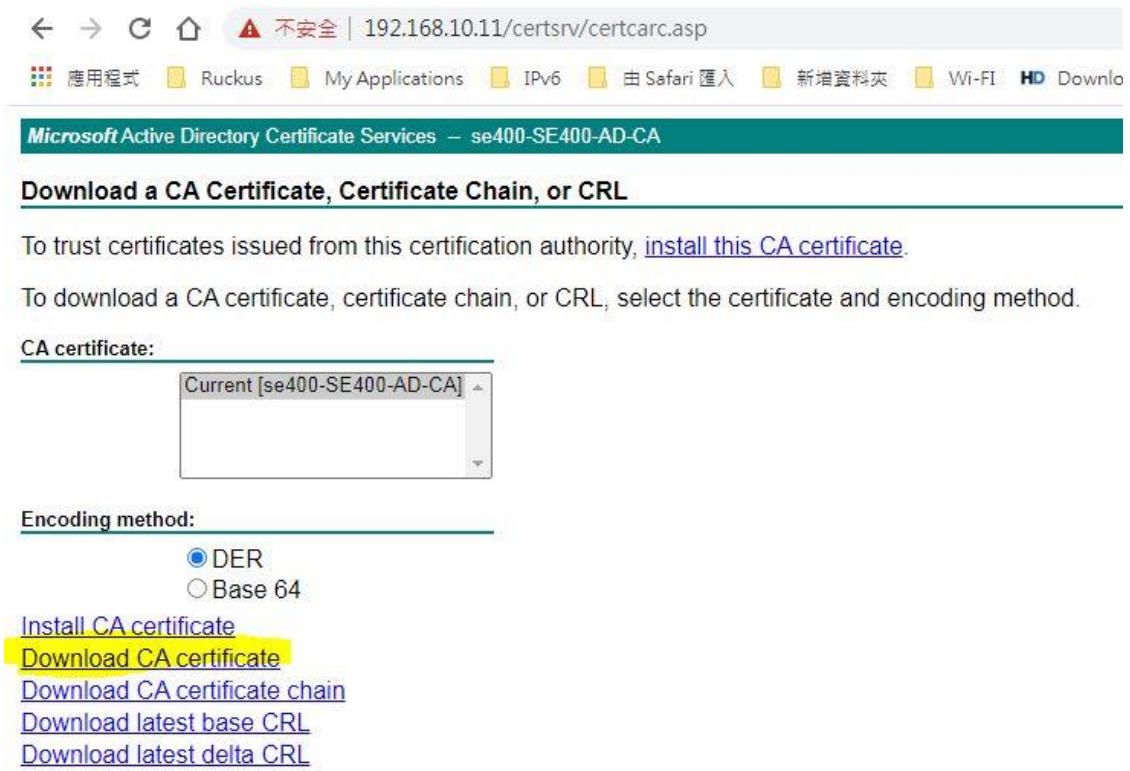


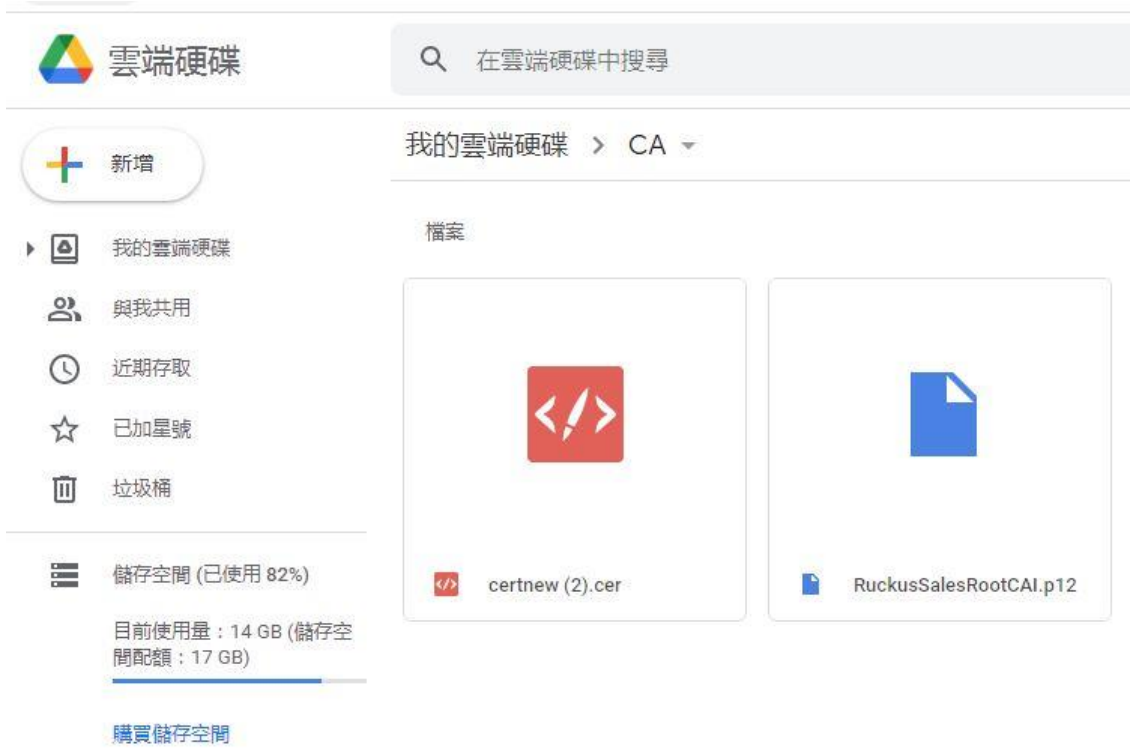
https://www.xda-developers.com/android-11-break-enterprise-wifi-connection/

如何解決

- 不更新Android
- 網路管理員指導用戶如何安裝根CA證書及如何配置服務器域名
- 網路管理員創建一個應用程式，該應用程式使用Android的WiFi建議API為用戶自動配置
- 使用Passpoint (hotspot 2.0)
- 使用EAP-TLS

Download CA and Upload to Google Disk



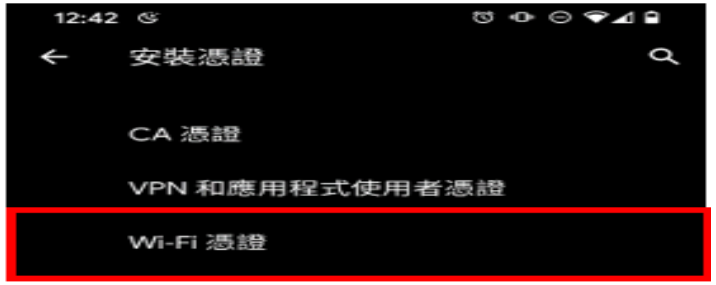


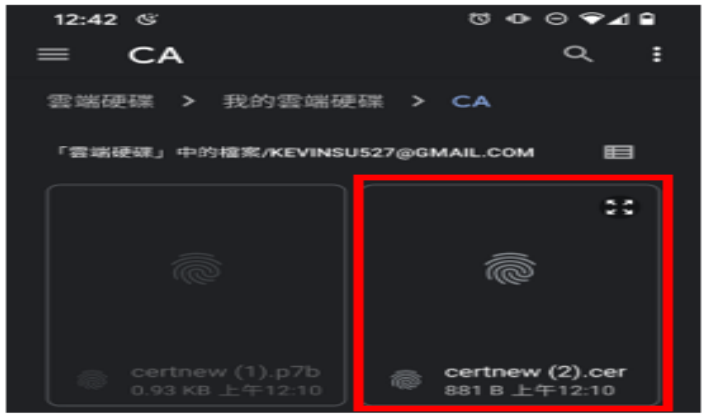
COMMSCOPE

Install CA

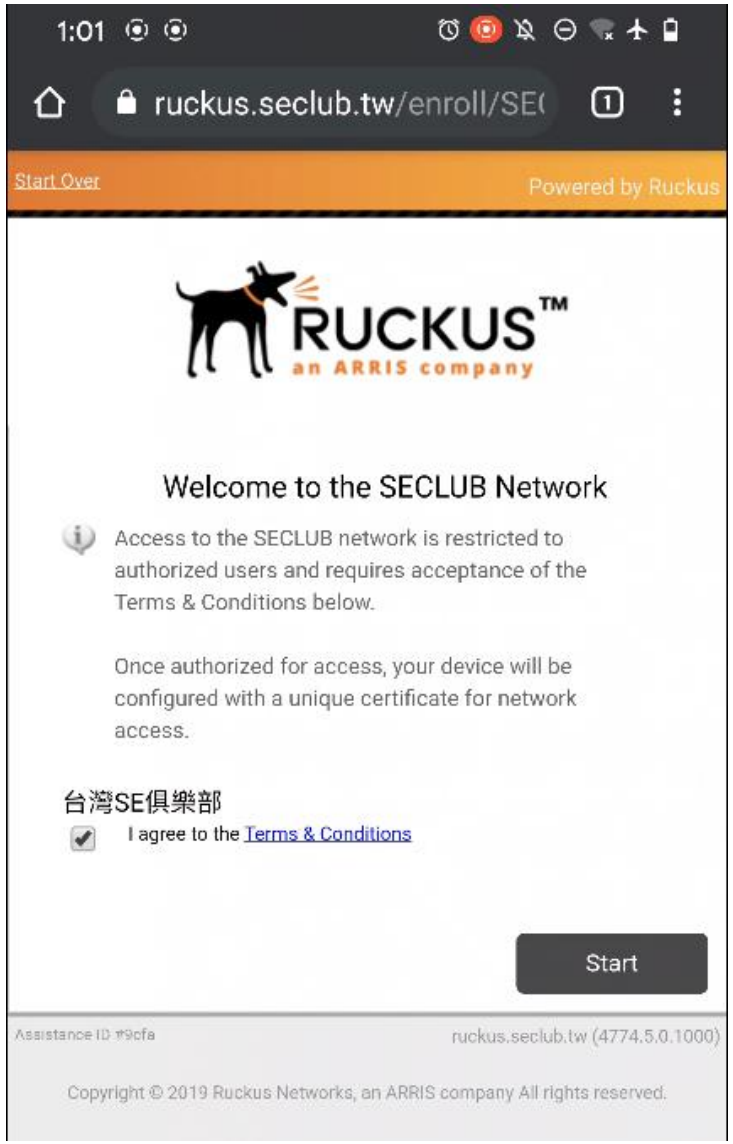
COMMSCOPE®

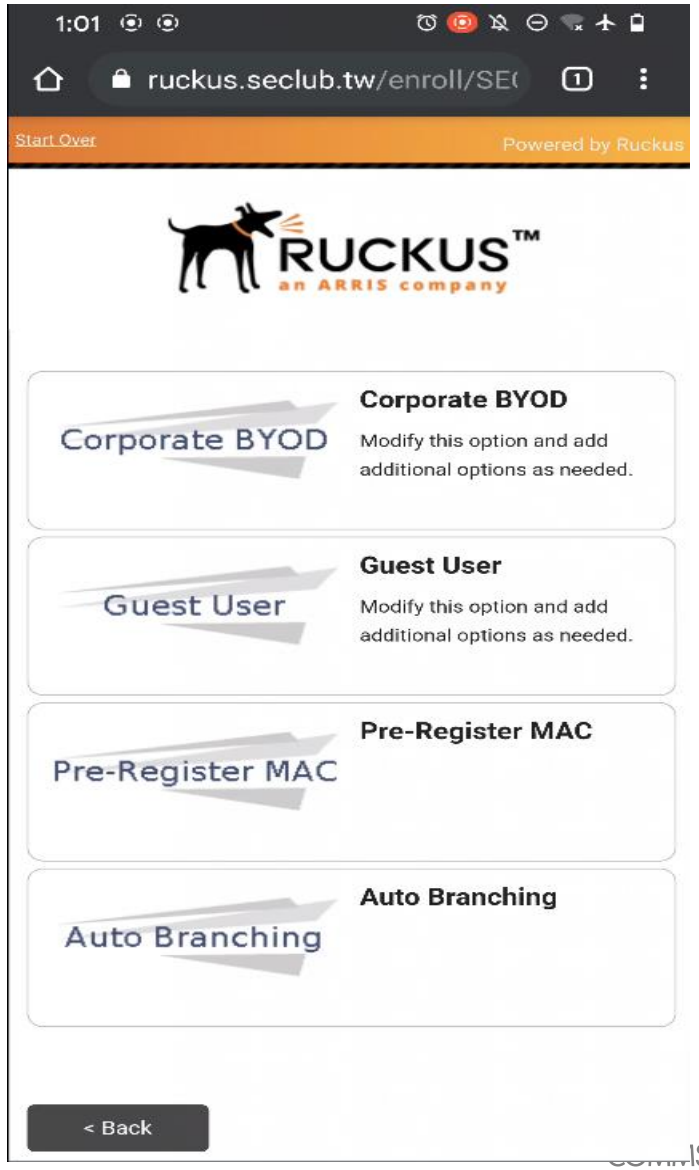
Re-configure 802.1x Authentication



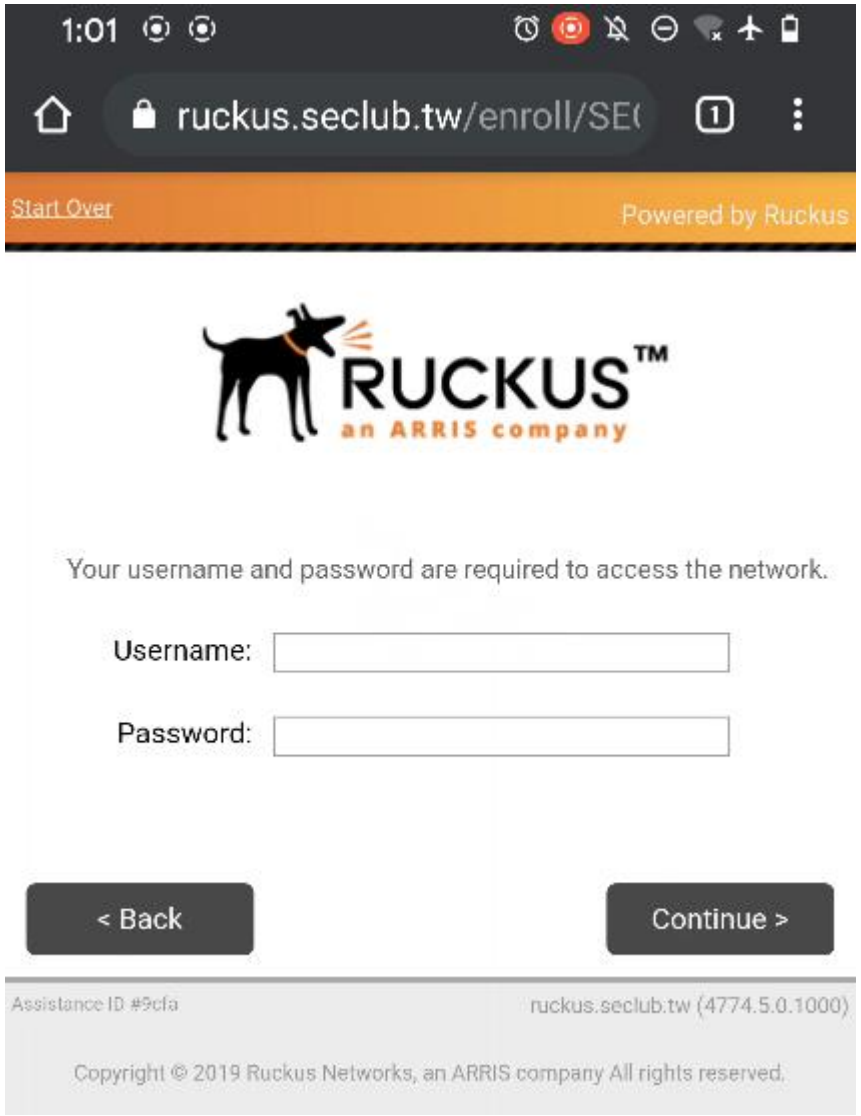


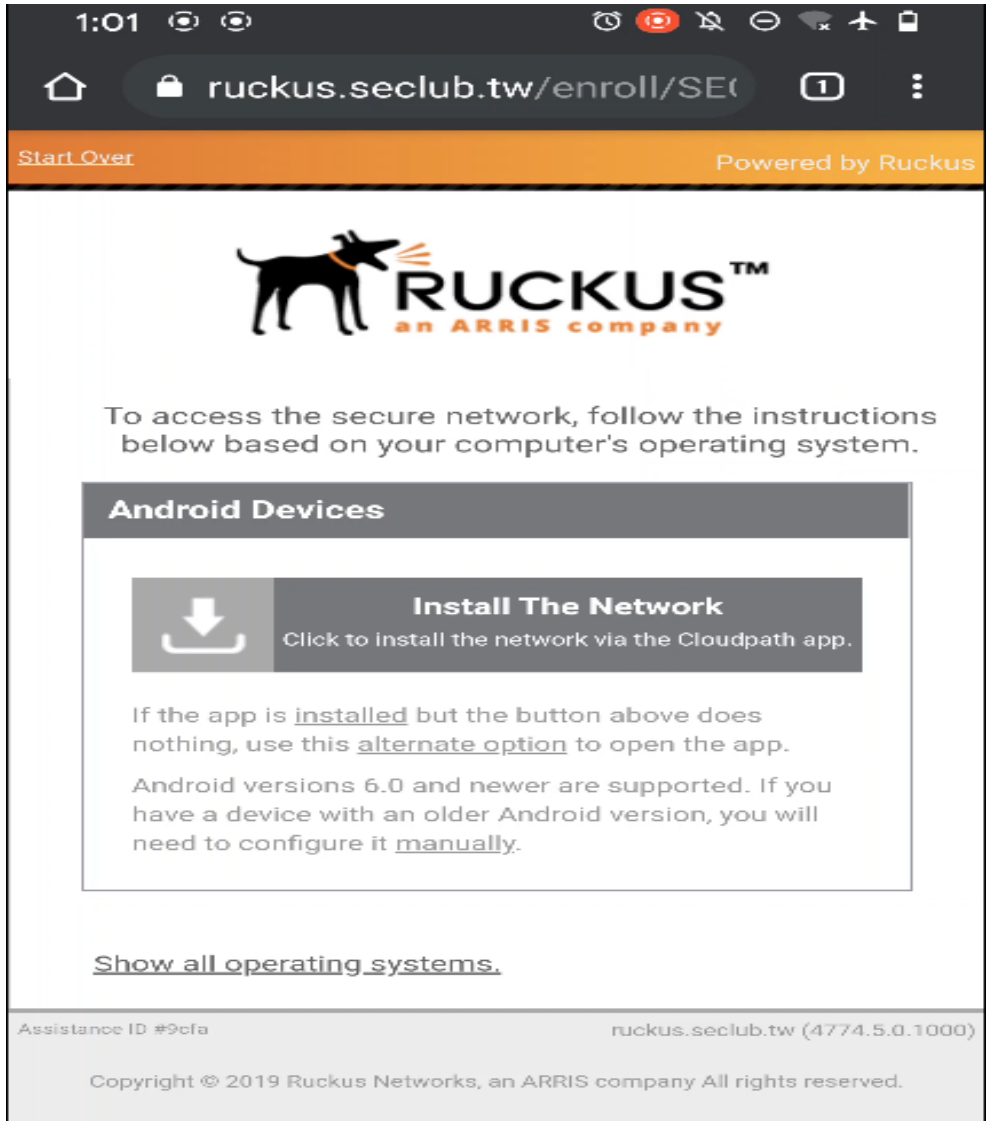
Cloudpath EAP-TLS Procedure for Android 11



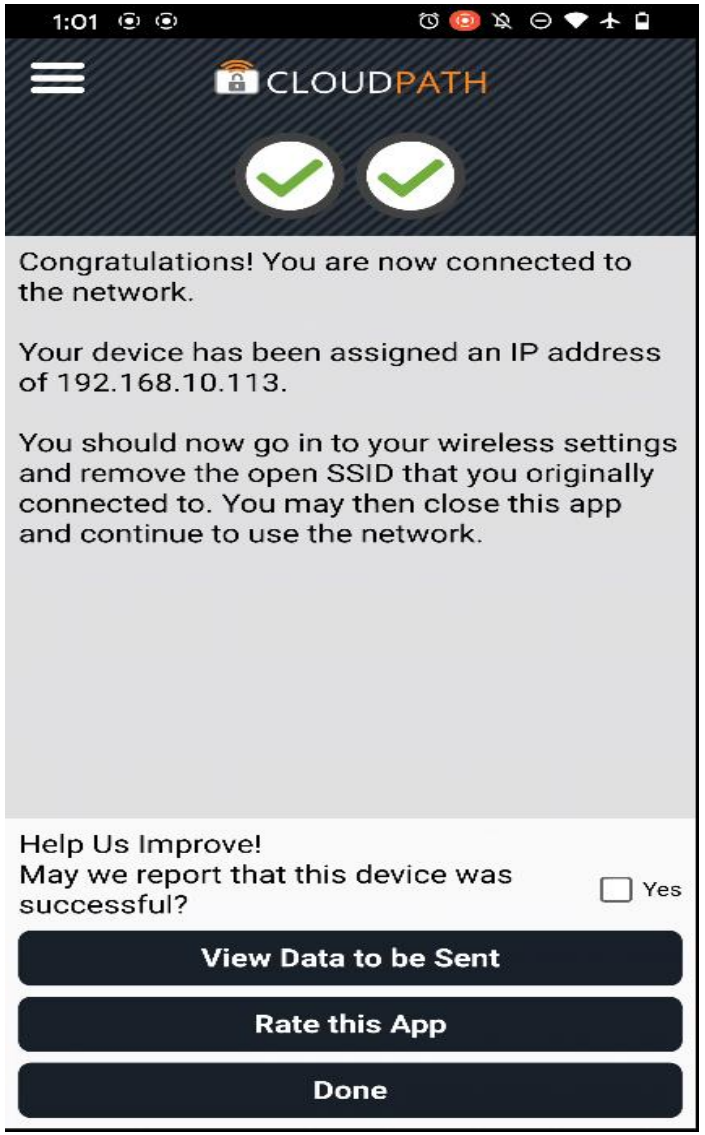


Cloudpath EAP-TLS Procedure for Android 11





Cloudpath EAP-TLS Procedure for Android 11



COMMSCOPE®

網路智慧管理

Ruckus™ Analytics

1 深度事件檢測

架構於機器學習之上的人工智慧優先序事件偵測

2 用戶故障排除

用一個視窗幫助您把所有的詳細用戶端事件紀錄

3 網路健康儀表板

提供專屬頁面為您監控網路的所有健康度跟效能

4 深度數據領航

提供彈性的資料瀏覽儀表板，只需要輕鬆的拖拉所需

5 全方位的報表

全面，精心策劃的報告可滿足您的所有報告需求

效益

提供網路運作全方位的可視性

加快對網路及用戶端的故障排除

幫助IT團隊改善用戶體驗

事件偵測情境

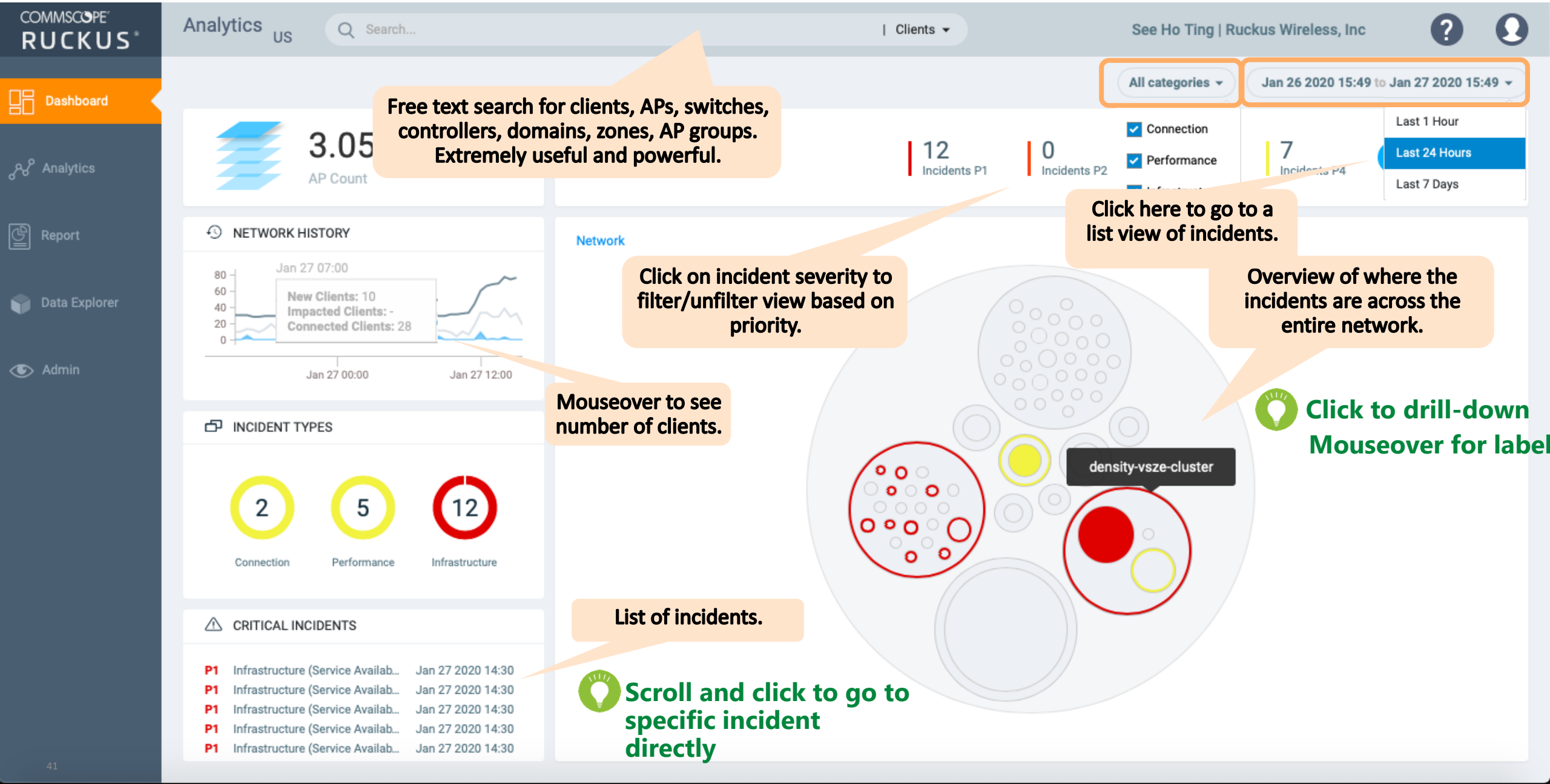
資訊處組長一早8點進到辦公室。

.

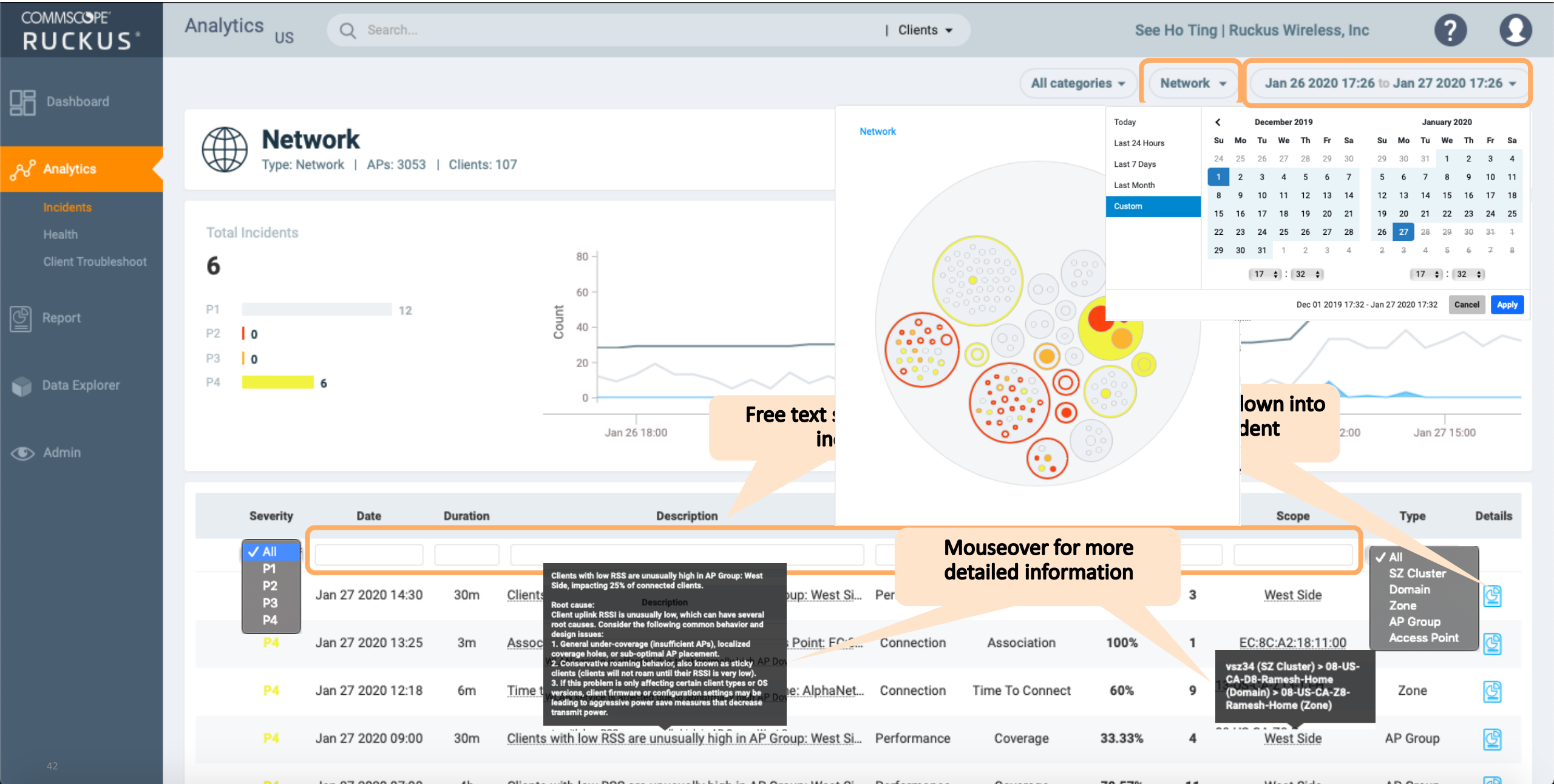
組長想知道校園網路中是否發生任何問題？ 希望在問題爆發之前就可以解決掉該問題。

網路中總會發生問題。組長希望對事件進行優先處理，因此他需要知道優先要排除的問題。

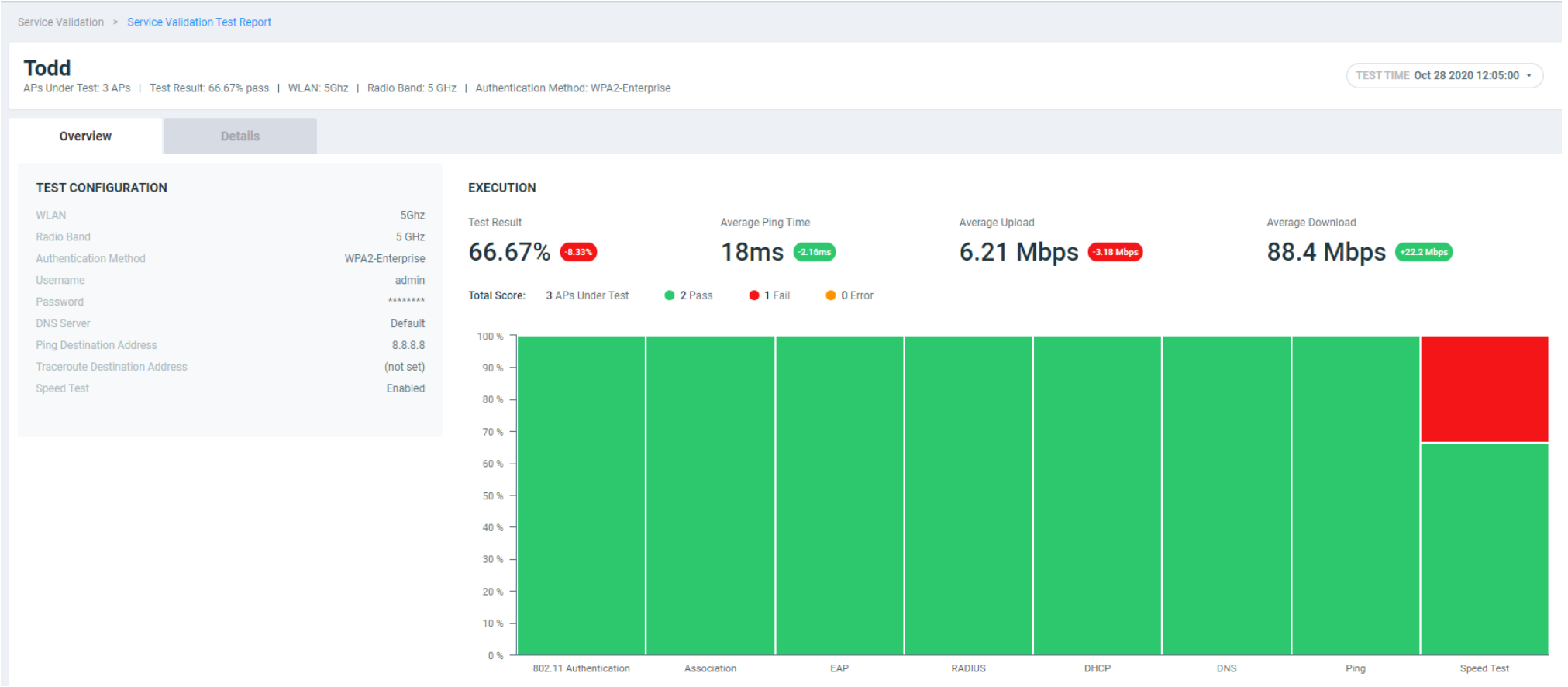
Incident Detection - Dashboard



Incident Detection – Incidents List



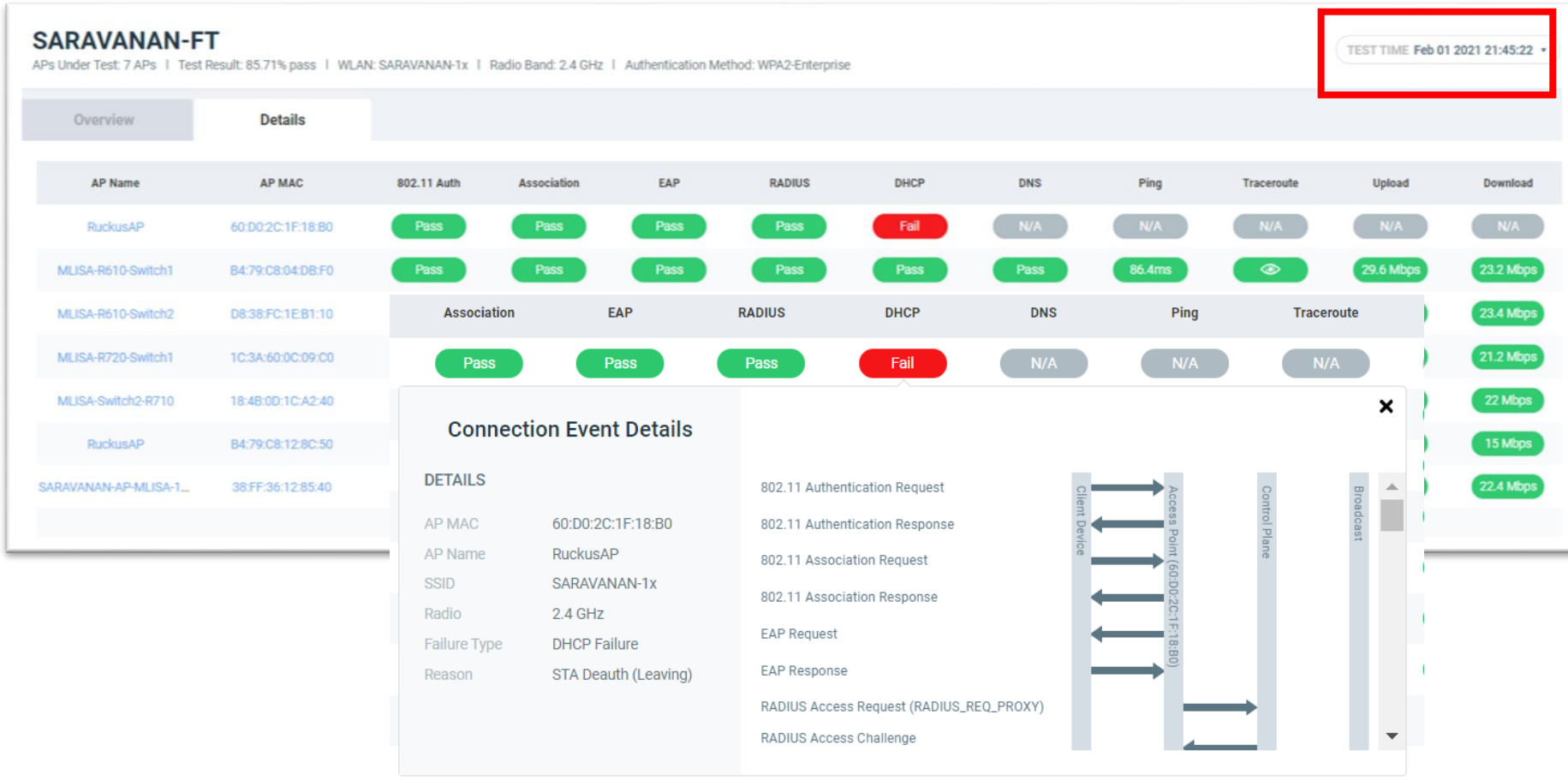
What is Service Validation?



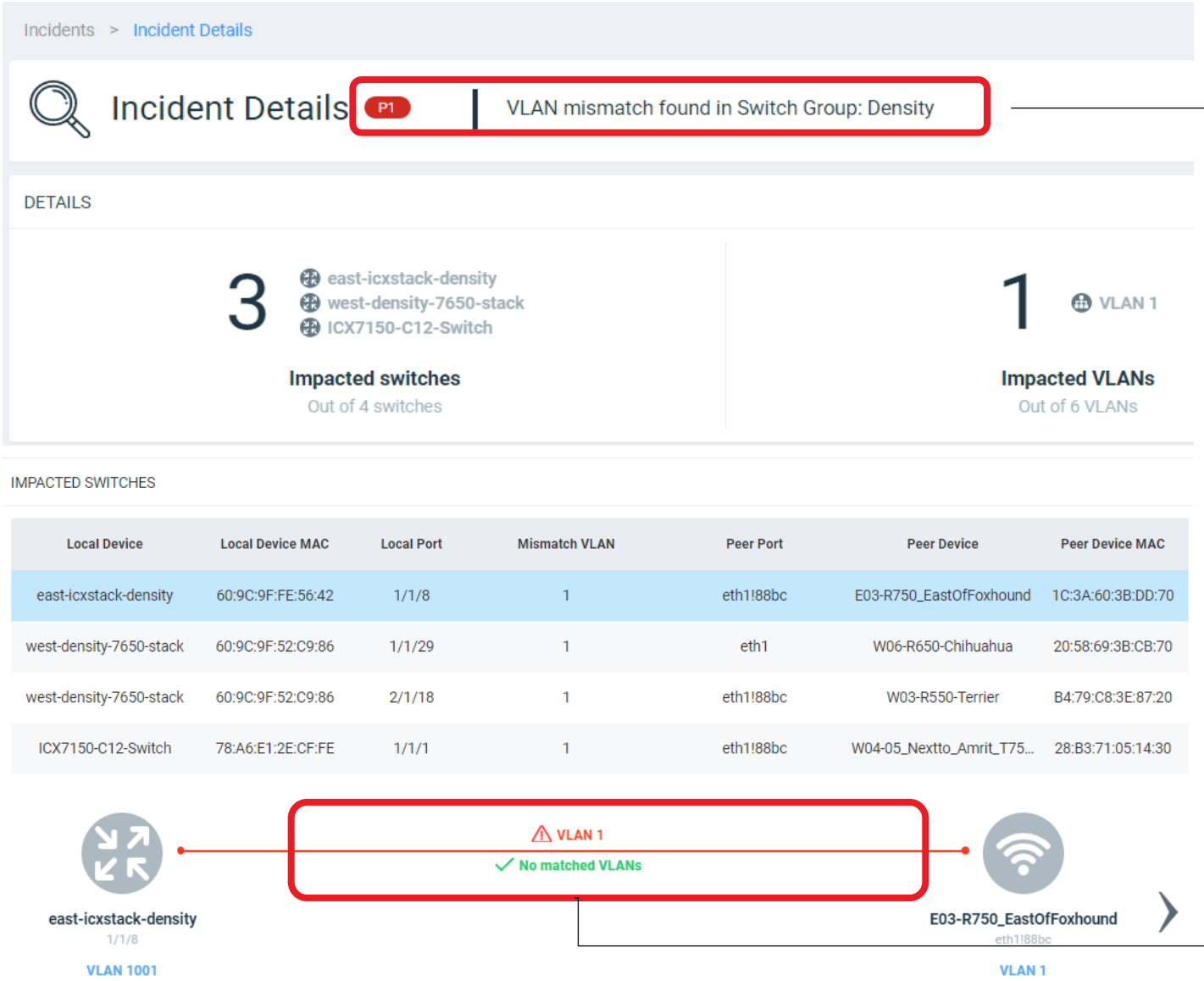
- Conveniently orchestrate network tests from cloud
- No extra hardware sensor or test equipment needed
- Test WLAN, LAN and WAN connectivity
- Test EAP, RADIUS, DHCP, DNS, Ping, Traceroute, Speed Test (upload/download)
- Service Validation is available for both Cloud and SZ customers

SV Test Details

- In Details page test result for each AP in every stage is shown
- At the top right in the test time widget, admins can see when the test was run.
- Click on failure to see details of where the test failed
- If a test was run multiple times, prior test results are available from here.



VLAN mismatch Insight



P1 Incident, Identifies switch group, IT can take action

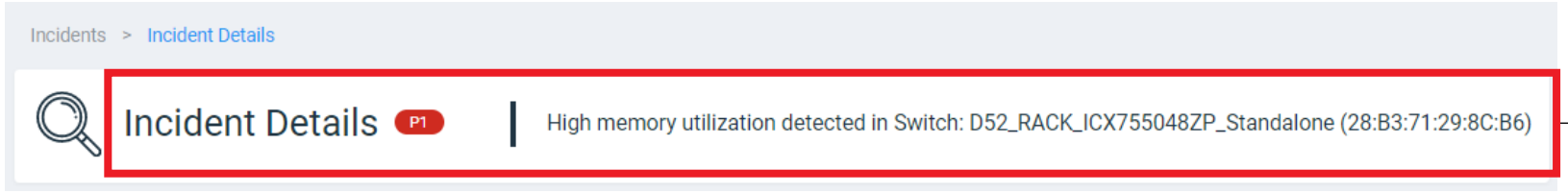
INCIDENT INFO

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)

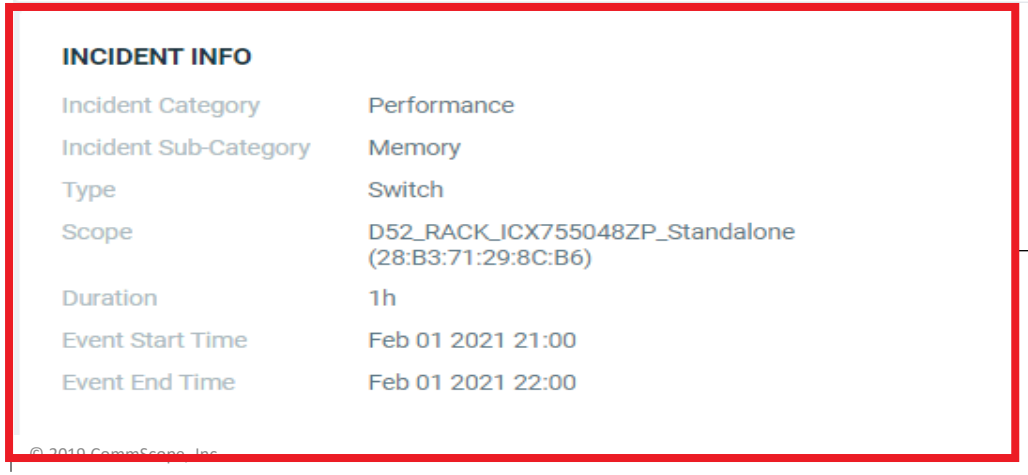
No matched VLANs found

High Switch Memory Utilization Insight



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

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

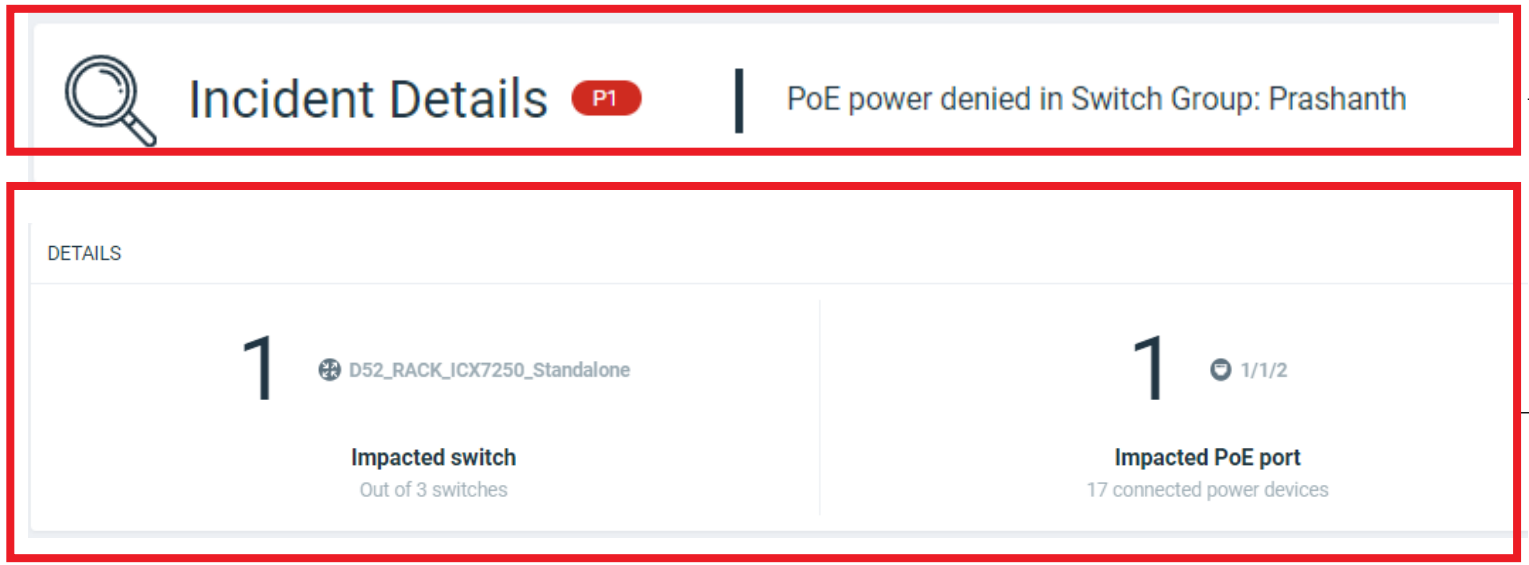


Scope, Duration, Event, Start and End Time.

Start Time: Event Detected

End Time: Memory will Exceed 90% threshold

PoE Insight – PoE power denied in Switch Group



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

Impacted Switch name and count

Impacted Port count

IMPACTED SWITCHES

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**

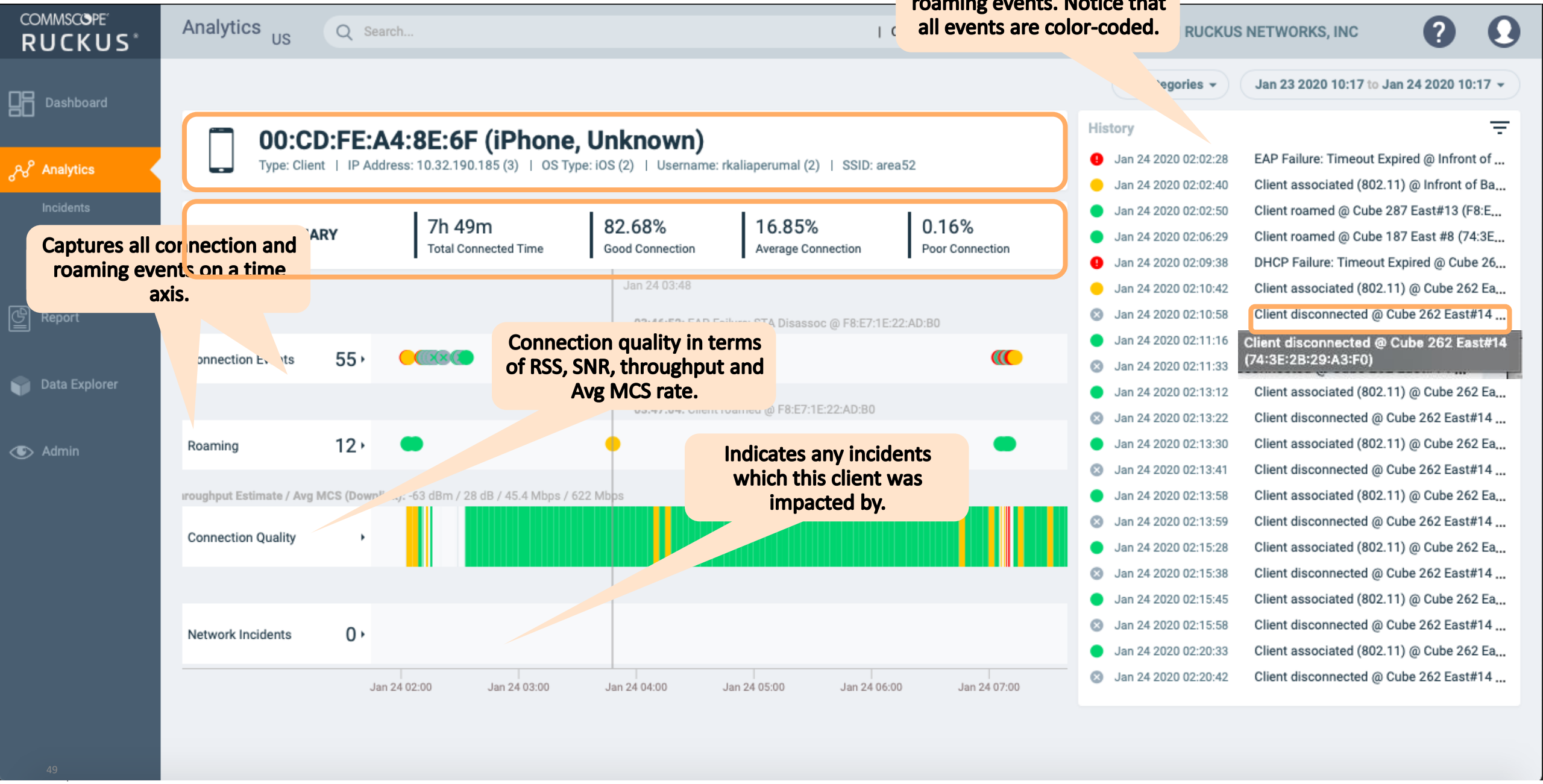
用戶端故障排除情境

資訊處組長一早8點進到辦公室

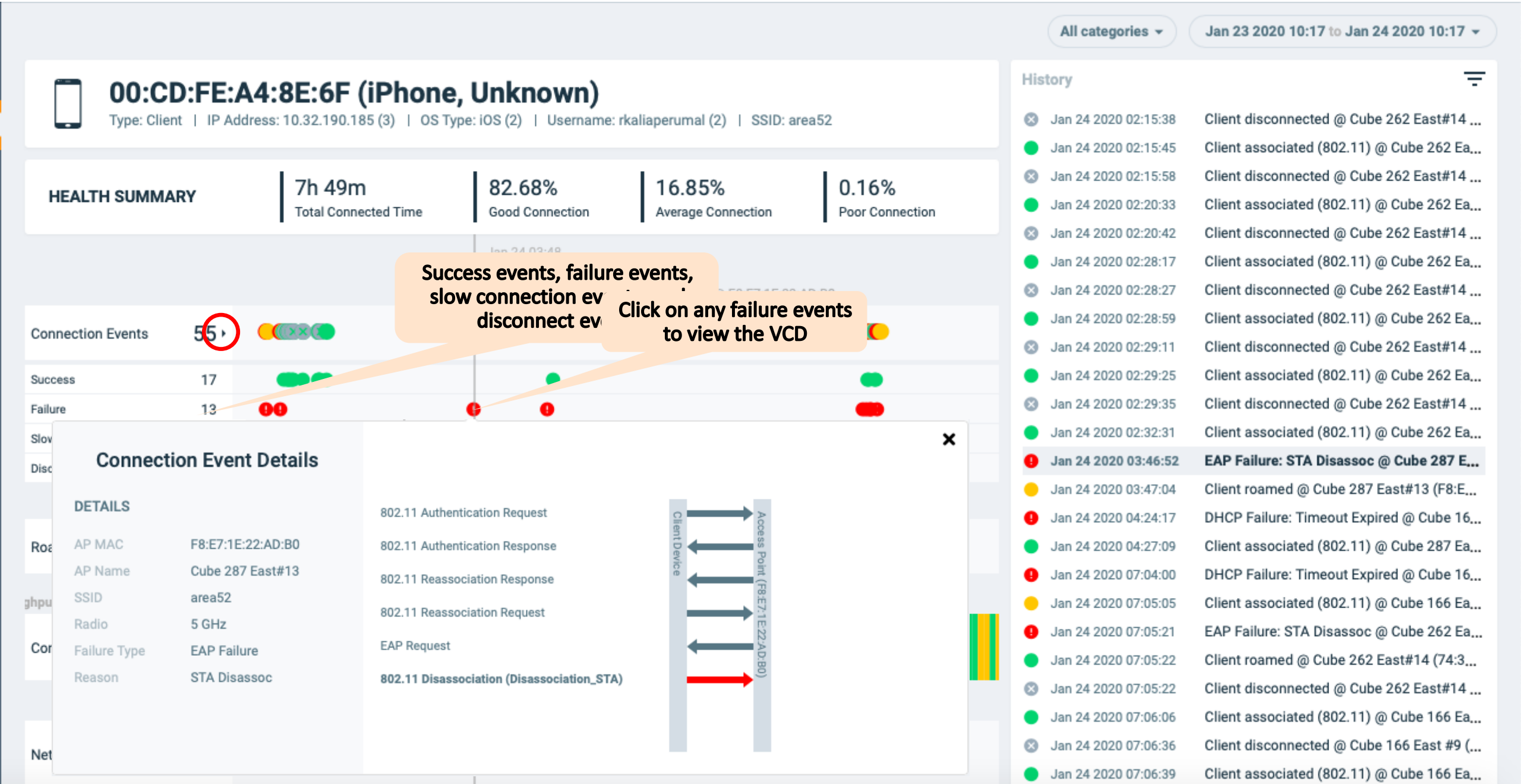
看到主任發給他的email，問他為什麼昨天下午開會時無法連接到WiFi。傳統組長必須針對個別WiFi用戶端進入故障排除模式，方能了解問題。

組長希望使用一個簡單的管理介面來了解主任在昨天所發生的狀況。

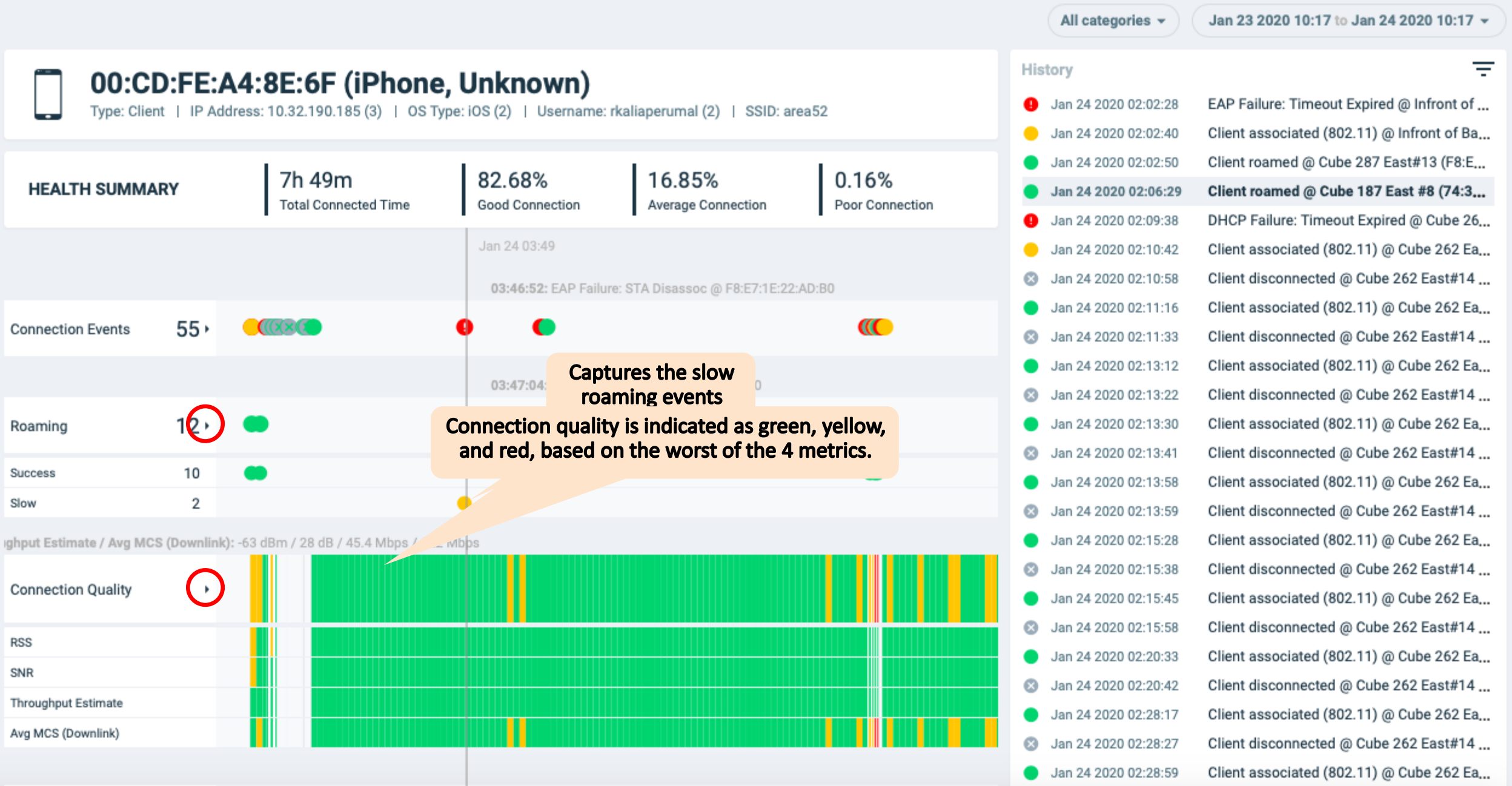
Client Troubleshooting



Client Troubleshooting – Visual Connection Diagnostics



Client Troubleshooting – Roaming & Connection Quality



總結

COMMSCOPE®

Thank You

Q&A

Kevin Su

Technical Consultant