

CISCO *Live!*

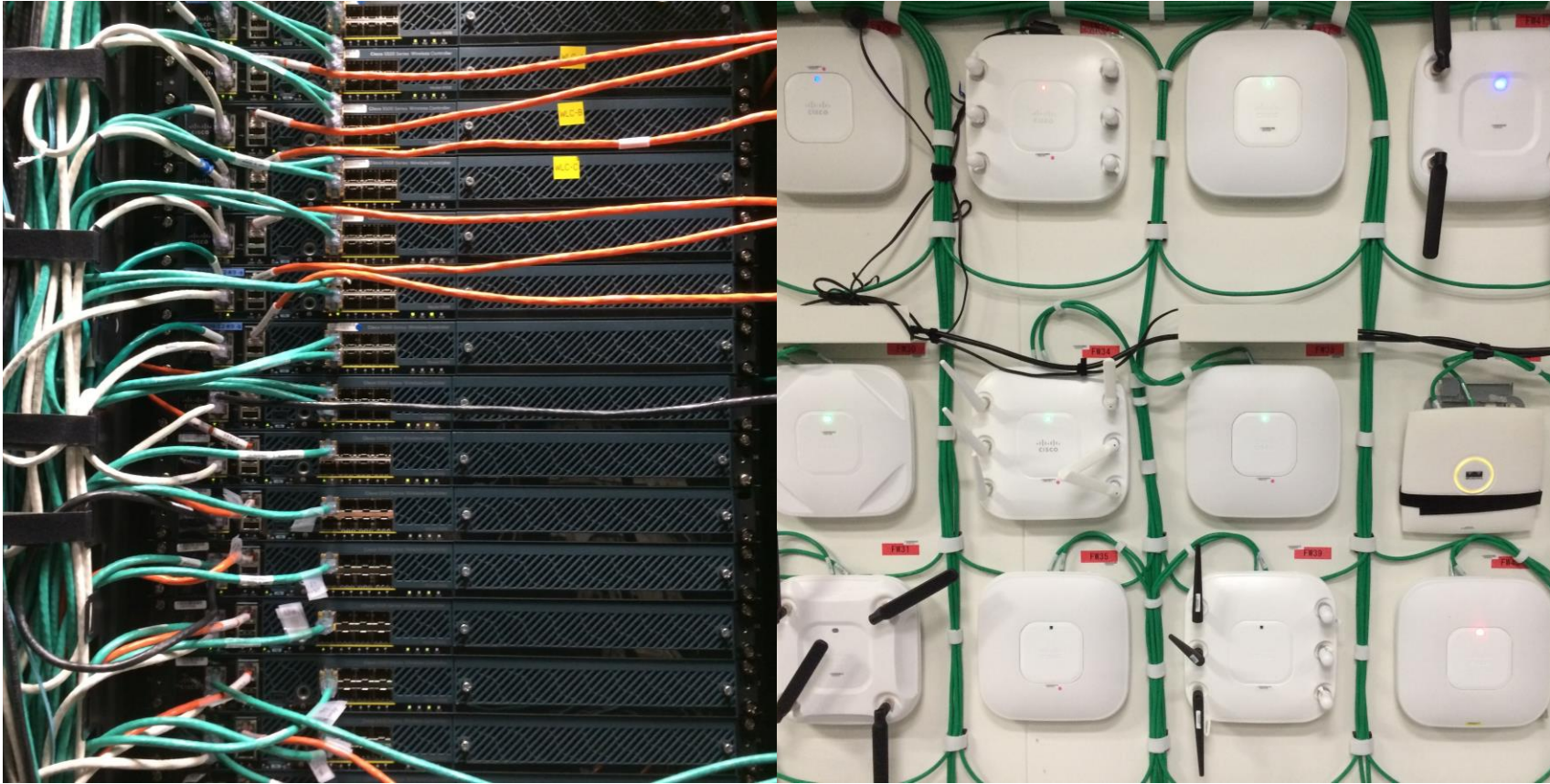
GO BEYOND

#CiscoLiveAPJC



A Spectrum of Wireless Designs with Cisco Meraki

Yuji Terada, Solutions Engineer
@terada_yuji
BRKEWN-1327



Documents



High Density Wi-Fi
Deployments



Wireless Layer 3 Roaming
Best Practices



MX Sizing Guide
& Principles



Wi-Fi 6E Frequently Asked
Questions



Adaptive Policy
Configuration Guide



[Internal docs...]

About me

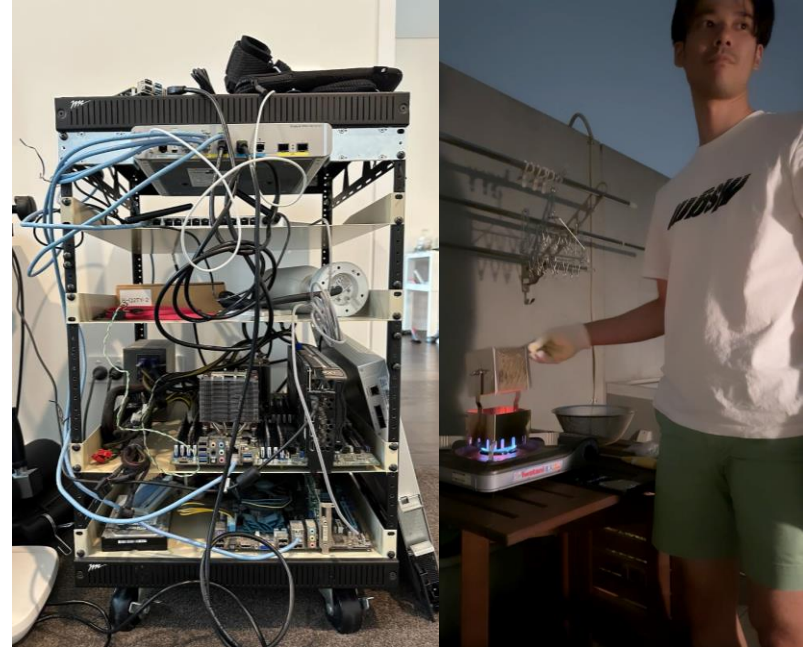
Yuji Terada

Career

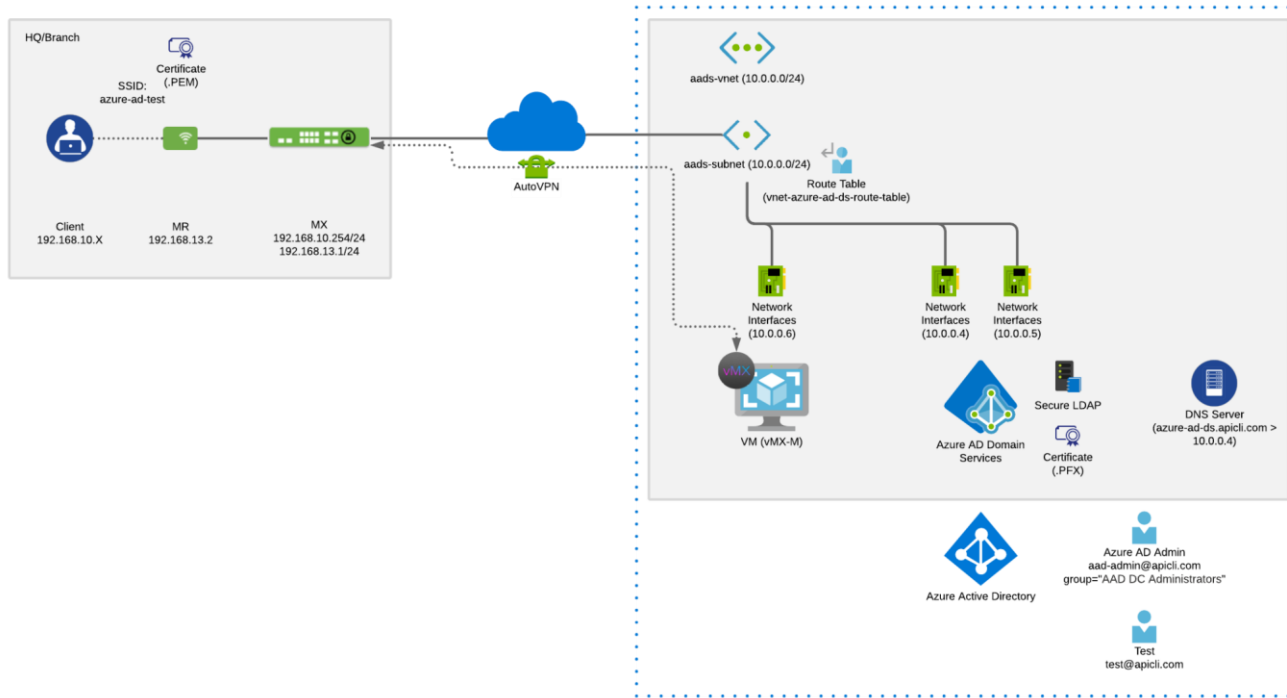
Apr 2014 Support Engineer @TAC
Feb 2018 Solutions Engineer @Meraki
Meraki APJC API Ninja
Meraki APJC Ninja Geo Lead

Certifications

CCIE R&S, Wireless
CCNP DevNet



Author of MR 802.1X with Azure Active Directory



<https://apicli.com/2021/12/13/meraki-mr-802-1x-with-azure-active-directory/>

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

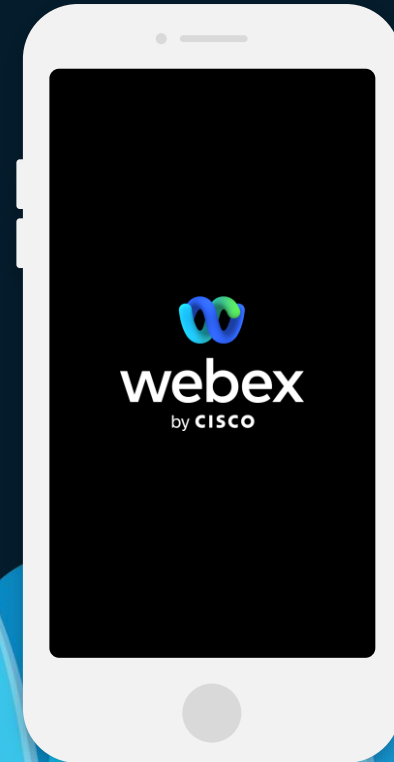
How

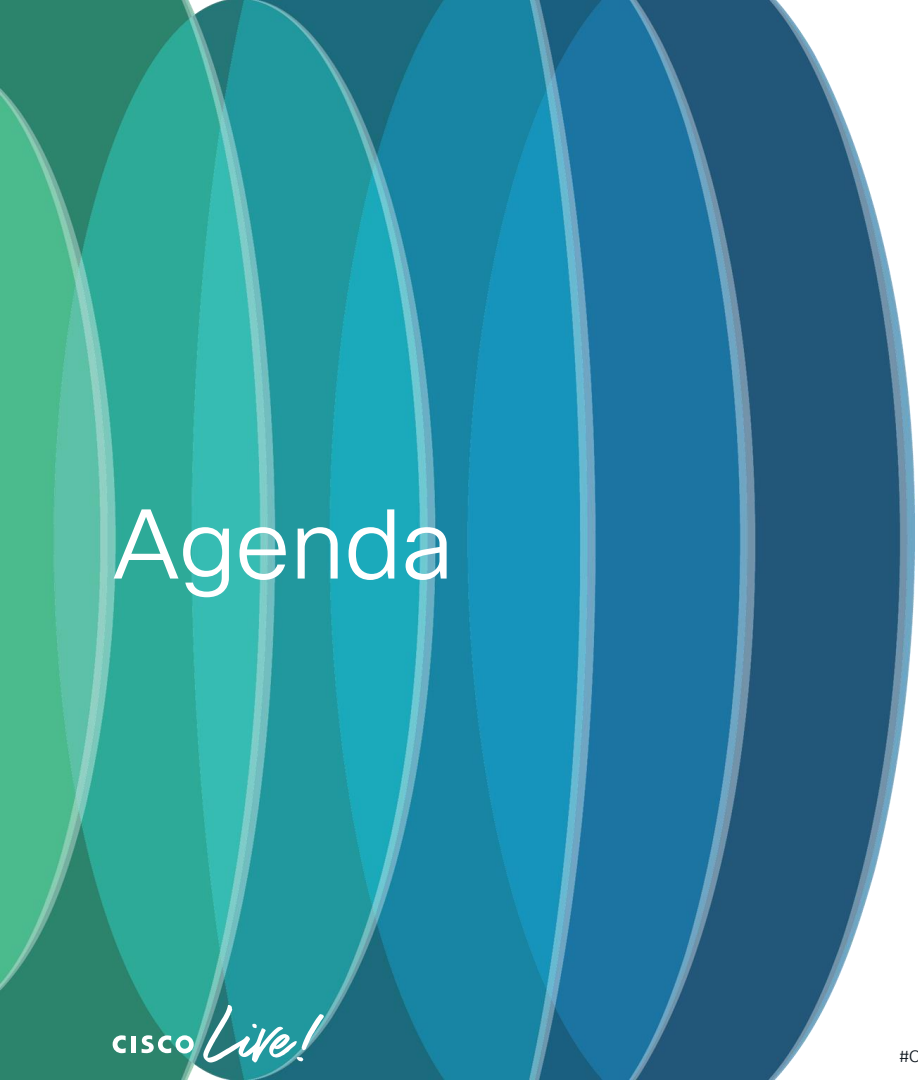
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-1327>





Agenda

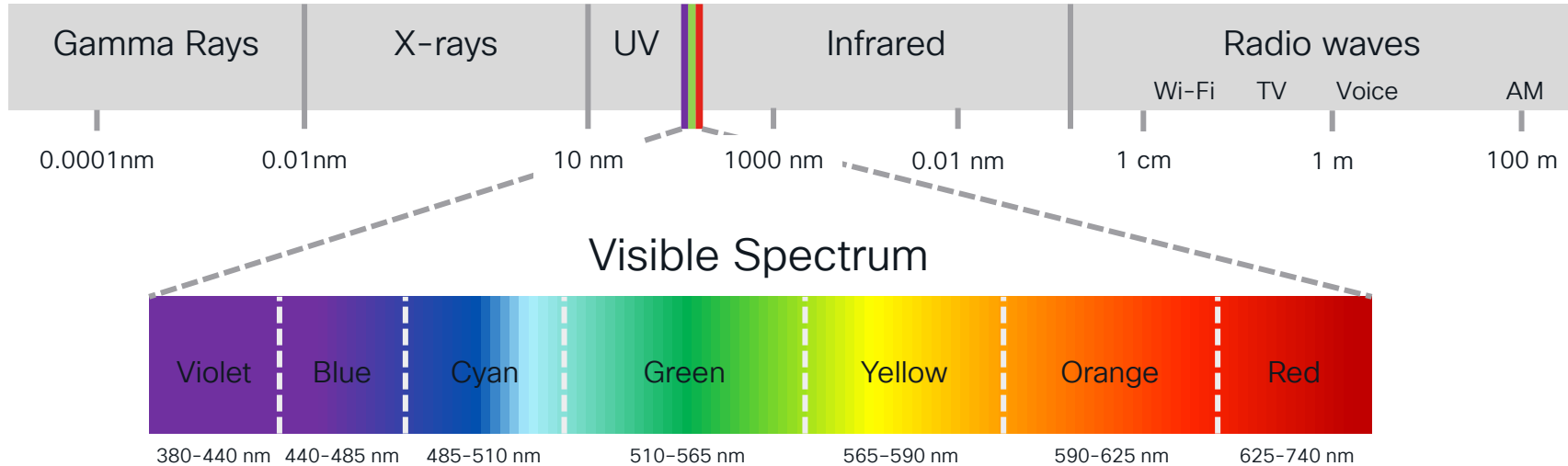
- Radio wave basics
- RF Profile
- 6 GHz
- Design
- Segmentation
- Architecture

Radio wave basics



Electromagnetic spectrum

Waves share common features. Human voices have a wavelength of 1.3 – 4 meters. Wi-Fi 2.4 GHz is 12.5 cm, and 5 GHz is 6 cm.



<https://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob30dg/Voice.pdf>

Characteristics of our voice



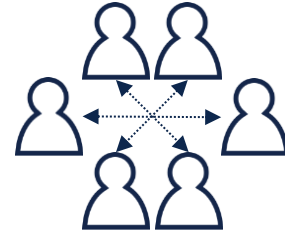
Distance

You can speak faster when close but need to slow down or increase your voice when far apart.
H E L L O ~



Obstruction

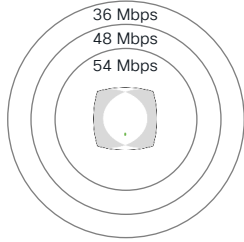
If an object exists between the two, communication becomes difficult



Noisiness

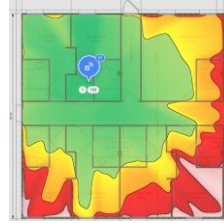
In a noisy area, you'll have to speak louder or move to a quiet location

Wi-Fi is similar



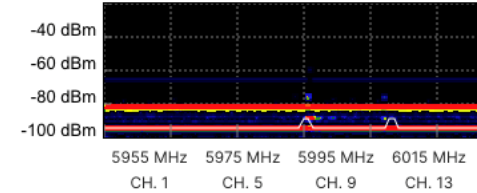
Distance

- AP decreases data rate for farther client



Obstruction

- Limits radiation

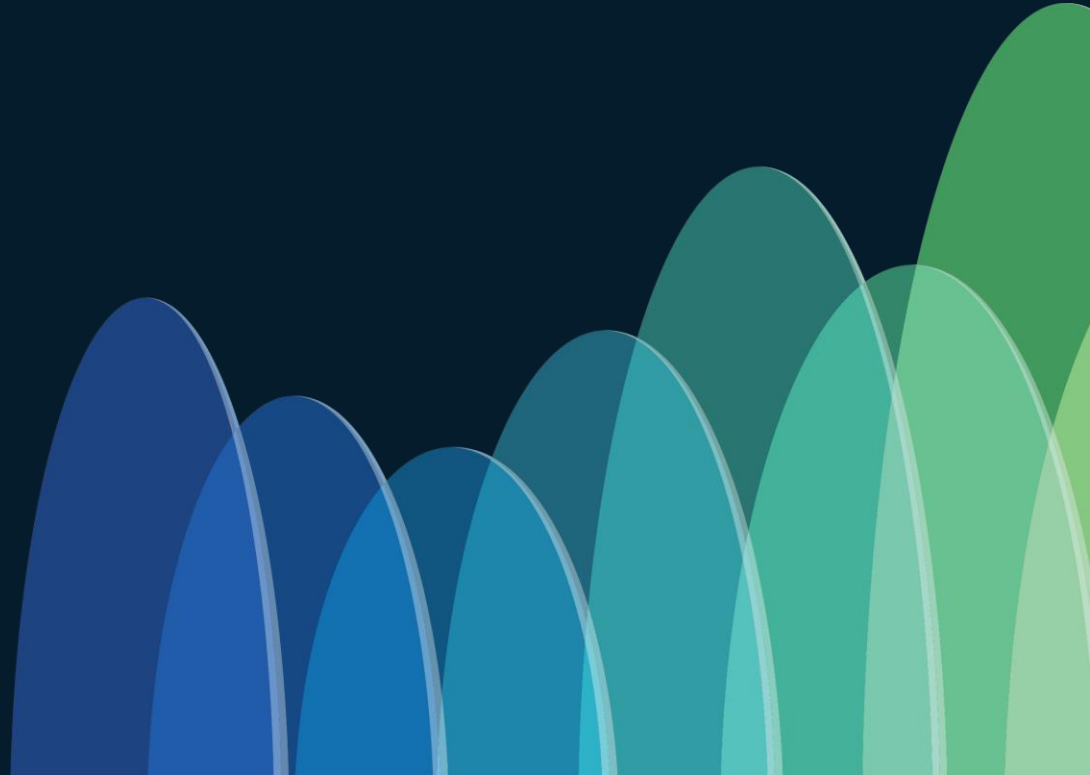


Noisiness

- AP changes channels
- AP changes channel width

Where should I place a MX67W? How many clients per AP?

RF Profile



Band selection

Disable 2.4 GHz where possible and encourage devices to connect on 5 GHz

General

Band selection

All SSIDs

Per SSID

Name	2.4 GHz	5 GHz	6 GHz	Band steering ⓘ
terada-house	☐	☒	☒	☐
terada-house-jpn	☐	☒	☒	☐
terada-house-legacy	☒	☒	☐	☐

[Show disabled SSIDs](#)

Monitor client capable Wi-Fi standards

Status, type, OS Connected to VLAN Policy 22 results

☐	Status	Description	IPv4 address	MAC address	Last seen (UTC+11)	Usage	Client type, OS	Capable Wi-Fi standards	Policy	Cap. char. width
☐	Wireless	Yujis-iPhone-6s	192.168.9.157	e6:63:da:7f:15:79	Nov 1 2024 06:56	132.27 MB	Other	802.11ac - 2.4 and 5 GHz, Fastlane capable	Normal	80 M
☐	Wireless	raspberrypi	172.16.100.10	e4:5f:01:2b:b4:bb	Nov 5 2024 15:32	1.44 GB	Raspberry Pi Trading	—	Normal	—
☐	Wireless	Watch	192.168.10.217	d6:73:ca:e7:ae:84	Nov 5 2024 13:13	3.15 MB	Other	802.11n - 2.4 and 5 GHz, Fastlane capable	Normal	40 M
☐	Wireless	10:ae:60:94:9b:04	192.168.9.137	10:ae:60:94:9b:04	Nov 4 2024 23:06	7.08 MB	Apple iPhone	802.11n - 2.4 GHz	Normal	40 M
☐	Wireless	WICED IP	192.168.9.134	2c:4c:c6:1d:42:58	Nov 5 2024 15:08	1.01 MB	Murata Manufacturing	802.11n - 2.4 GHz	Normal	20 M
☐	Wireless	YUJTERAD-M-HC5K	192.168.10.231	b8:ab:61:e4:1b:06	Nov 5 2024 15:32	557.9 MB	Meraki OS	—	Normal	—
☐	Wireless	teradaisagowanoiPhone	192.168.9.140	da:58:a9:ef:89:ae	Nov 5 2024 15:31	1.16 GB	Other	802.11ac - 2.4 and 5 GHz, Fastlane capable	Normal	80 M
☐	Wired	mbc3340463800	1.1.1.1	bc:33:40:46:38:00	Nov 5 2024 11:23	39.35 MB	Cisco Meraki	—	Normal	—
☐	Wireless	192-168-9-130	192.168.9.130	90:39:5f:88:c1:1c	Nov 5 2024 15:31	6.6 GB	Android	802.11ax - 2.4, 5 and 6 GHz	Normal	80 M
☐	Wireless	0c:8d:db:83:0a:2f	—	0c:8d:db:83:0a:2f	Nov 5 2024 15:30	—	Meraki	—	Normal	—
☐	Wireless	58:2f:40:ce:2f:cb	192.168.9.152	58:2f:40:ce:2f:cb	Nov 5 2024 15:31	506.49 MB	Nokia	802.11ac - 2.4 and 5 GHz	Normal	80 M
☐	Wireless	Watch	192.168.9.169	9a:42:85:0c:3b:0d	Nov 5 2024 11:19	371.46 MB	Other	802.11n - 2.4 and 5 GHz, Fastlane capable	Normal	40 M
☐	Wireless	Sawas-MacBook-Pro	192.168.9.112	b8:e8:56:48:10:da	Nov 5 2024 15:31	557.04 MB	Apple	802.11ac - 2.4 and 5 GHz, Fastlane capable	Normal	80 M
☐	Wireless	d7758312-a4da-43e2-bdd3-f09c1d25bea3	192.168.9.168	f6:7e:a2:b6:69:38	Nov 5 2024 10:33	1.14 GB	Apple iPhone 15 Pro, iOS 17 A 1	802.11ax - 2.4, 5 and 6 GHz, Fastlane capable	Normal	160

Select columns

Check to add, drag columns to reorder.

- ☐ Adaptive policy group
- ☐ Named VLAN
- ☒ Capable Wi-Fi standards
- ☐ 802.1X policy
- ☐ CDP/LLDP
- ☒ IPv4 address
- ☐ IPv6 address
- ☐ IPv6 address (link local)
- ☒ Manufacturer
- ☒ MAC address
- ☒ Usage
- ☒ Client type, OS
- ☐ iPSK Name
- ☒ First seen (UTC+11)
- ☒ Last seen (UTC+11)
- ☒ Capable channel width
- ☐ Systems Manager
- ☐ Performance ⓘ
- ☐ Onboarding ⓘ
- ☒ Policy

Cancel Apply

Beacons consume airtime

Channel utilization when minimum data rate is **802.11b 1 Mbps**, beacon frame size is 380 bytes, and beacon interval is 102.4 ms

Number of APs on channel	Number of SSIDs							
	1	2	3	4	5	6	7	8
1	3.22%	6.45%	9.87%	12.90%	16.12%	19.35%	22.57%	25.80%
2	6.45%	12.90%	19.35%	25.80%	32.25%	36.70%	45.14%	51.59%
3	9.67%	19.35%	29.02%	38.70%	48.37%	58.04%	67.72%	77.39%
4	12.90%	25.80%	38.70%	51.59%	64.49%	77.39%	90.29%	100.00%
5	16.12%	32.25%	48.37%	64.49%	80.62%	96.74%	100.00%	100.00%

<https://revolutionwifi.blogspot.com/p/ssid-overhead-calculator.html>

Pushing data rate up

Channel utilization when minimum data rate is **802.11b 11 Mbps**, beacon frame size is 380 bytes, and beacon interval is 102.4 ms

Number of APs on channel	Number of SSIDs							
	1	2	3	4	5	6	7	8
1	0.43%	0.86%	1.30%	1.73%	2.16%	2.59%	3.02%	3.46%
2	0.86%	1.73%	2.59%	3.46%	4.32%	5.18%	6.05%	6.91%
3	1.30%	2.59%	3.89%	5.18%	6.48%	7.78%	9.07%	10.37%
4	1.73%	3.46%	5.18%	6.91%	8.64%	10.37%	12.10%	13.82%
5	2.16%	4.32%	6.48%	8.64%	10.80%	12.96%	15.12%	17.28%

<https://revolutionwifi.blogspot.com/p/ssid-overhead-calculator.html>

Data rate

Minimum data rate (bitrate) can be changed to solve management frames consuming airtime. Increasing data rate will cause a decrease in range

Minimum bitrate configuration

☐ Per band

Set the minimum bitrates for the 2.4 & 5 GHz radios separately below.

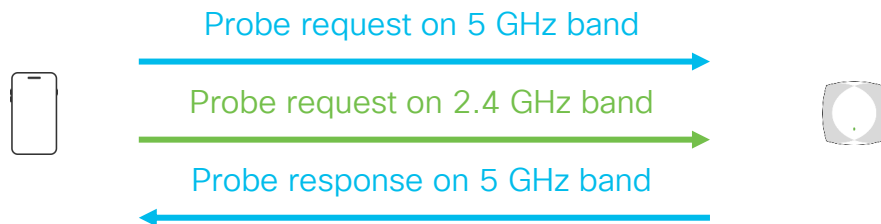
☒ Per SSID

Set the minimum bitrates per SSID

SSID name	Min bitrate	
terada-house	12	
terada-house-jpn	12	
terada-house-legacy	11	

Band steering

Disable unless you have legacy clients that can't determine the ideal AP



If you want clients to connect by 5 GHz, disable 2.4 GHz

https://documentation.meraki.com/MR/Radio_Settings/Band_Steering

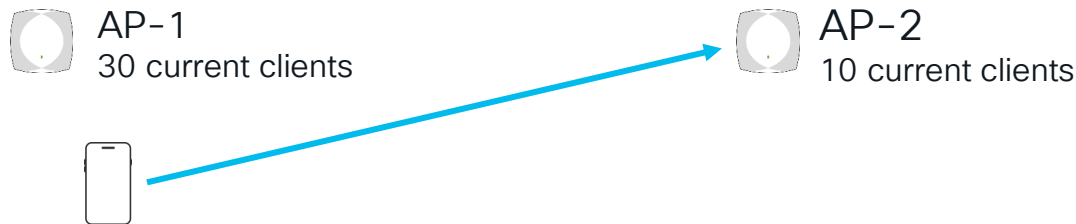
AP view and client view



In Wi-Fi, client makes the decision on how to connect

Client balancing

Disable unless most clients initially connect to the same AP

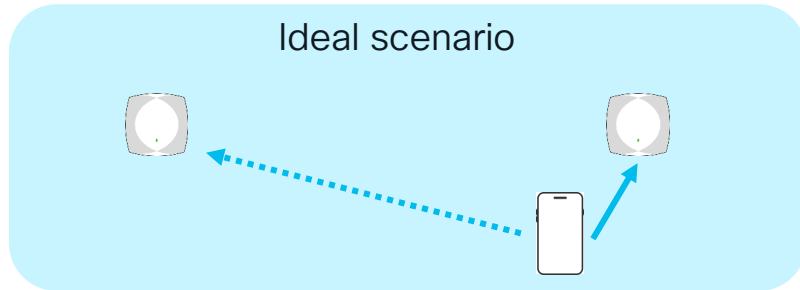


Number of client count doesn't mean the AP is busy. AP-1 can have 30 clients that are sleeping (low channel utilization), and AP-2 can have 10 clients that are transferring files (high channel utilization)

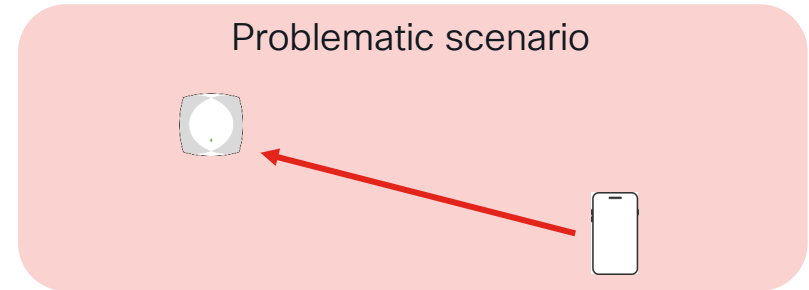
https://documentation.meraki.com/MR/Other_Topics/Client_Balancing

RX-SOP

Need appropriate planning and survey before enabling



1. Client tries to connect to a distant AP
2. AP ignores as received RSSI signal is lower than configured threshold
3. Client connects to closer AP

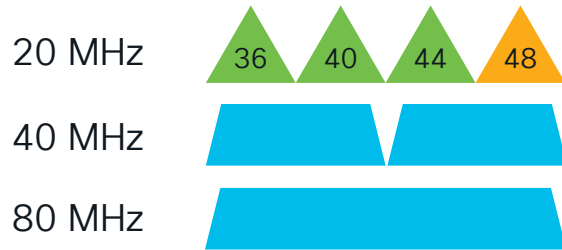


1. Client tries to connect to a distant AP
2. AP ignores as received RSSI signal is lower than configured threshold
3. Client cannot connect

[https://documentation.meraki.com/MR/Radio_Settings/Receive_Start_of_Packet_\(RX-SOP\)](https://documentation.meraki.com/MR/Radio_Settings/Receive_Start_of_Packet_(RX-SOP))

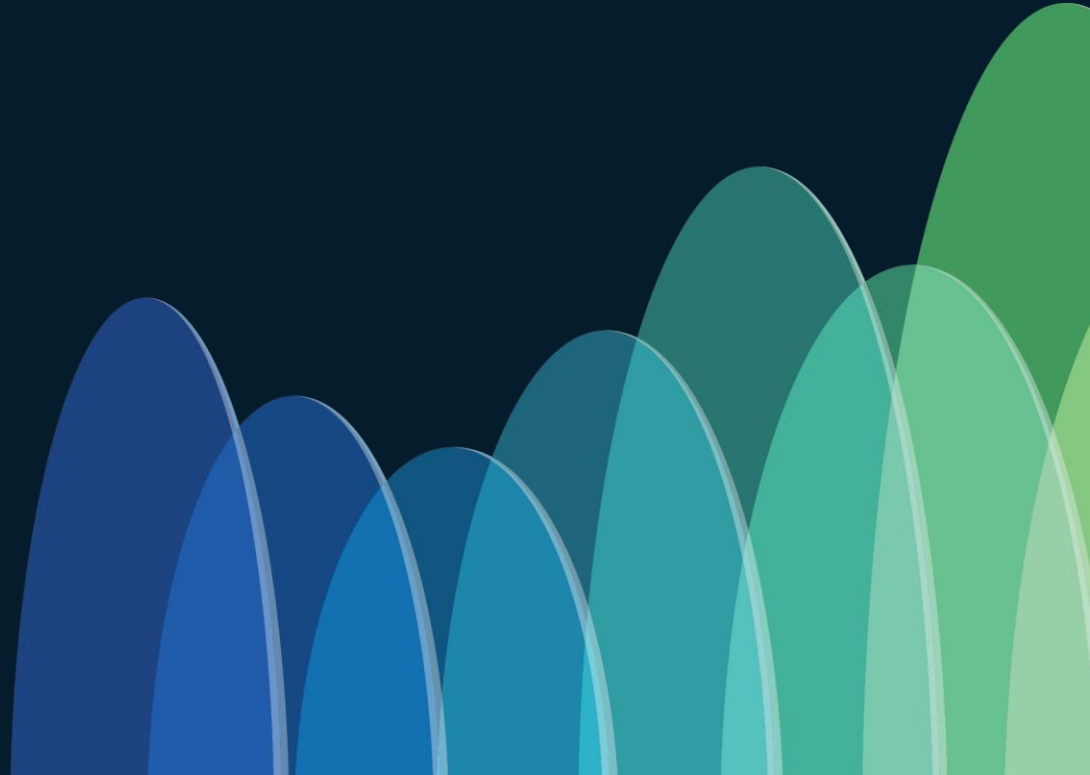
Channel width

Configure to 40 MHz or in a very dense environment, 20 MHz.
Default “Auto” is very aggressive selecting 80 MHz

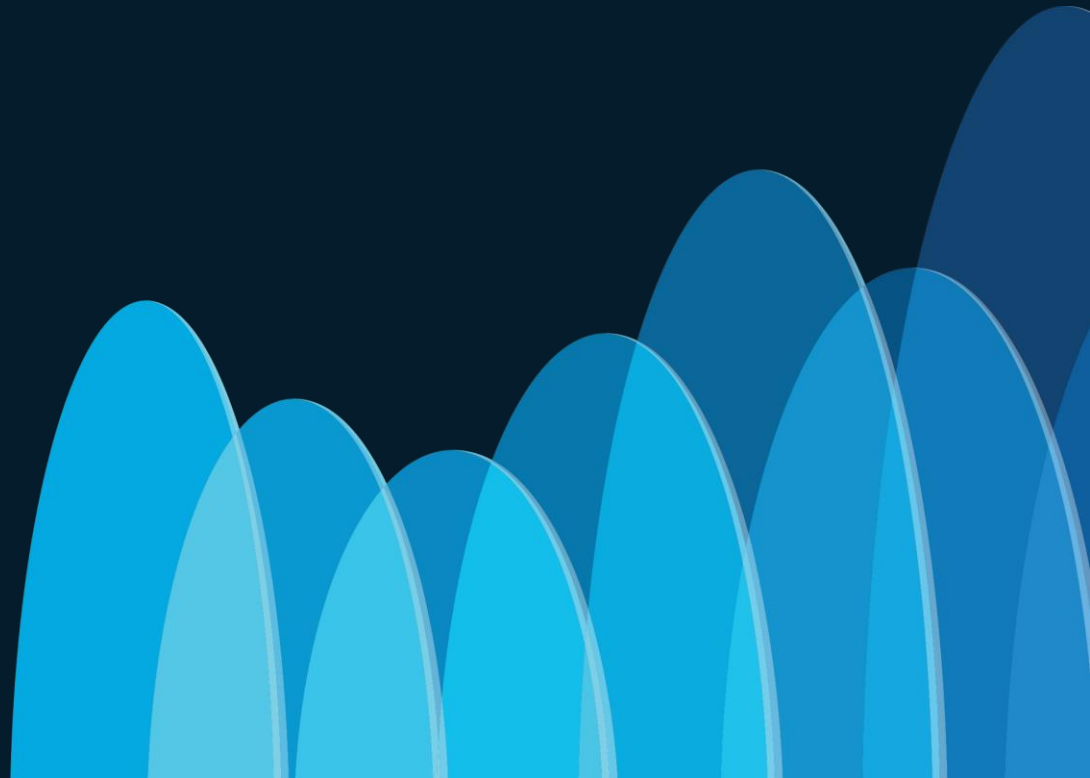


APs and clients will use the whole channel width even if there is interference on one of the channels. On the scenario on the left with interference on channel 48, an 80 MHz channel width could have lower throughput than a 40 MHz channel width.

Demo/Recap



6 GHz



Choose 6GHz for flex radio selection

Configure 6 GHz as band preference for MR57, CW9166I, and CW9166D1 in RF-profile

Flex radio selection

Access point model	Band preference
MR57	6 GHz ▾
CW9166I	6 GHz ▾
CW9166D1	6 GHz ▾

Current default is 5 GHz

https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

WPA3 encryption is required for 6 GHz

WPA3 Only

> 31.1.X

WPA3 Transition Mode + 802.1X

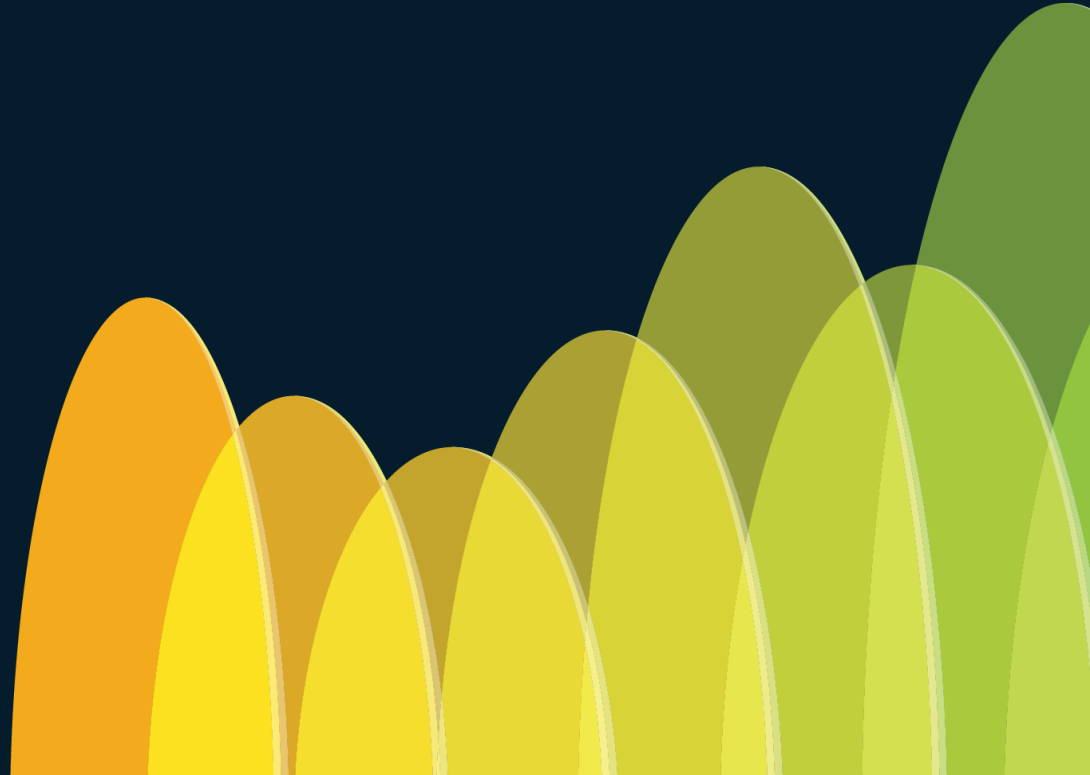
The screenshot shows a configuration page for WPA3. It has five radio button options: Password, MAC-based access control (no encryption), Enterprise with, Identity PSK with RADIUS, and Identity PSK without RADIUS. The 'WPA encryption' dropdown at the bottom is highlighted with a blue box and shows 'WPA3 only'.

The screenshot shows a configuration page for WPA3. It has three radio button options: Enterprise with, Identity PSK with RADIUS, and Identity PSK without RADIUS. The 'Enterprise with' option is selected and highlighted with a blue box. Below it, the 'WPA encryption' dropdown is also highlighted with a blue box and shows 'WPA3 Transition Mode'.

Create a 6 GHz only SSID if required

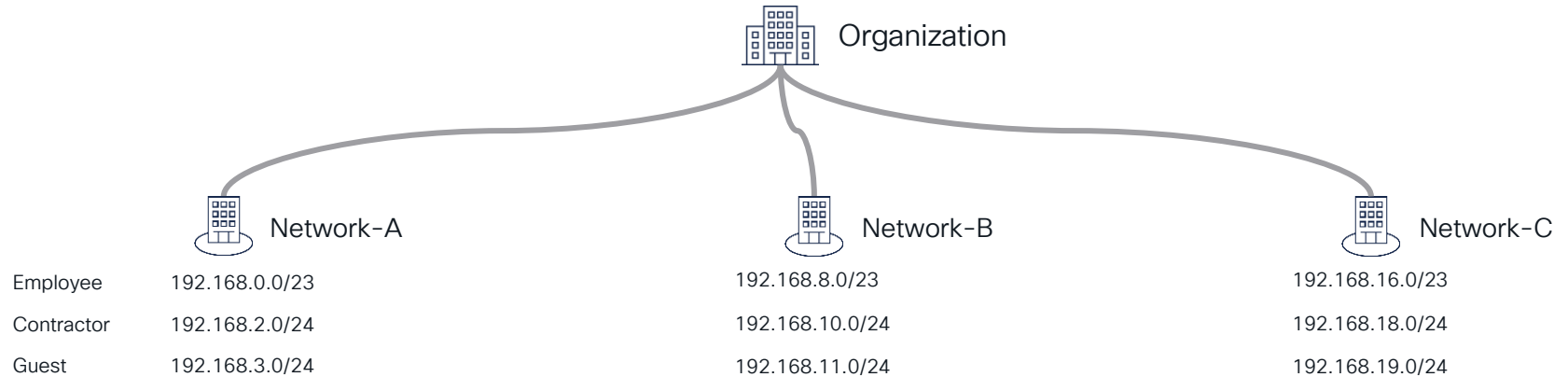
https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

Design



Small/medium networks

Nothing special. It just works.



Large networks



Cloud Dashboard limitation

General rule of thumb is don't go over 80% of the limit

Item	Scope	Limit	
Maximum networks	Per organization	20,000	
Maximum devices	Per organization	25,000	
Maximum devices	Per network	1,000	
Maximum clients	Per network	50,000	

Access point limitation

General rule of thumb is don't go over 80% of the limit

Item	Scope	Limit	
Maximum SSIDs	Per network	15	
Maximum SSIDs	Per organization	15,000	
Maximum allow list MACs	Per network	3,000	
Maximum layer 3 firewall rules	Per AP	1,800	
Maximum traffic shaping rules	Per SSID	8 (4 if default enabled)	
Maximum IPSKs without RADIUS	Per SSID	5,000	

Large networks



Meraki AP mode

Meraki AP mode is FlexConnect local switching local authentication



FlexConnect

= AP continues to operate even if connection to management is down

Local switching

= All data traffic exits directly out of AP

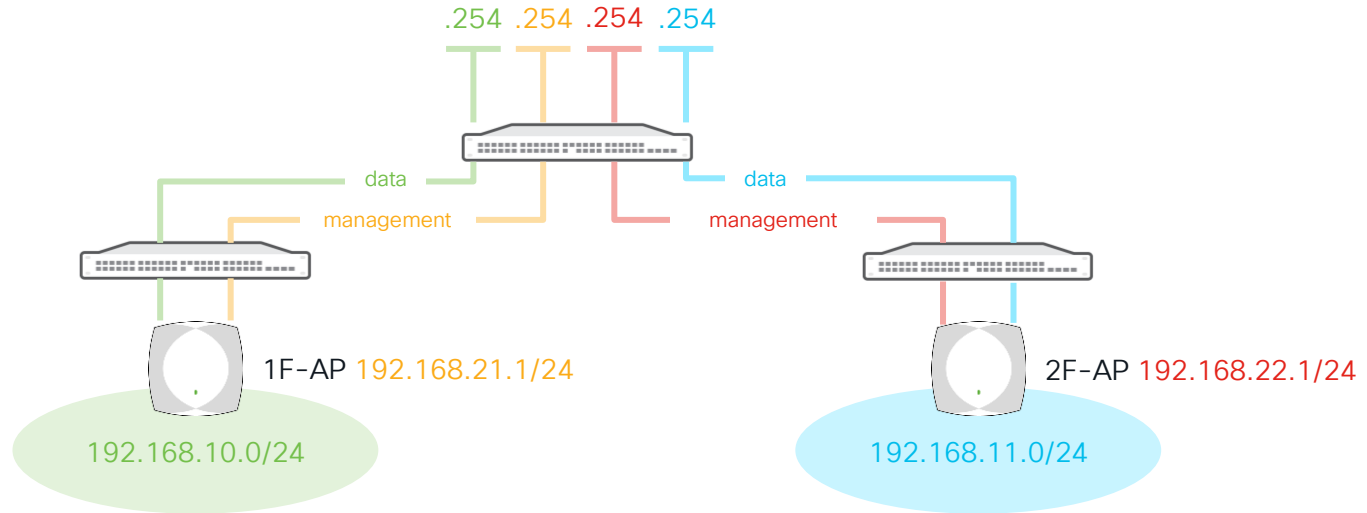
Local authentication

= All authentication packets exit directly out of AP

All APs need to be added as RADIUS client on RADIUS server

Layer 3 roaming

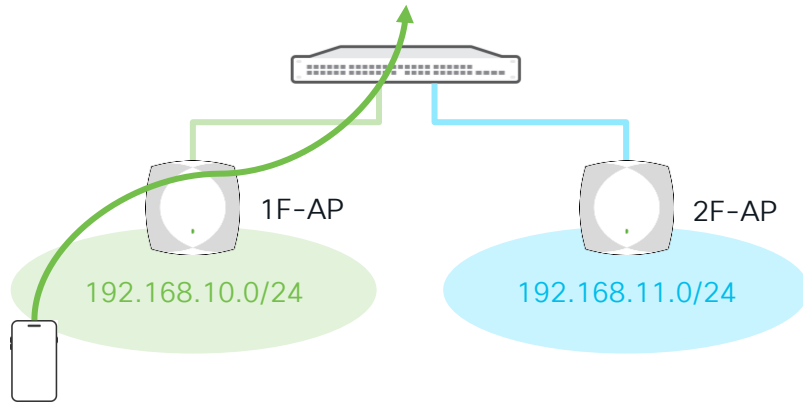
Each floor/section has its own subnet to limit the broadcast domain



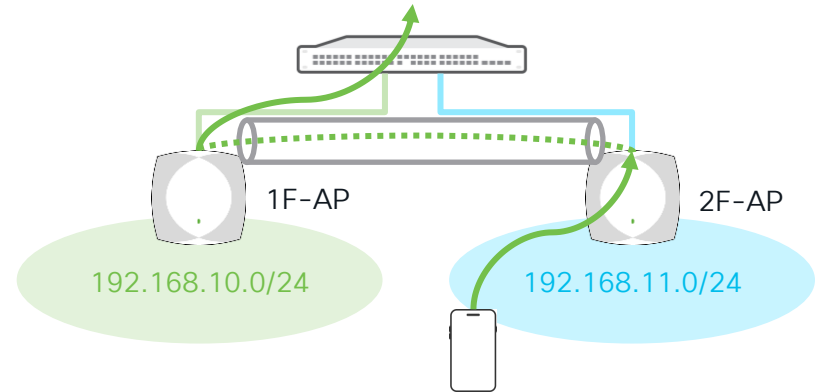
If client moved from 1F-AP to 2F-AP, DHCP process kicks in

Distributed Layer 3 Roaming

Use initially connected AP as an anchor to maintain client's IP address. Load increases on anchor AP



Client connects to 1F-AP

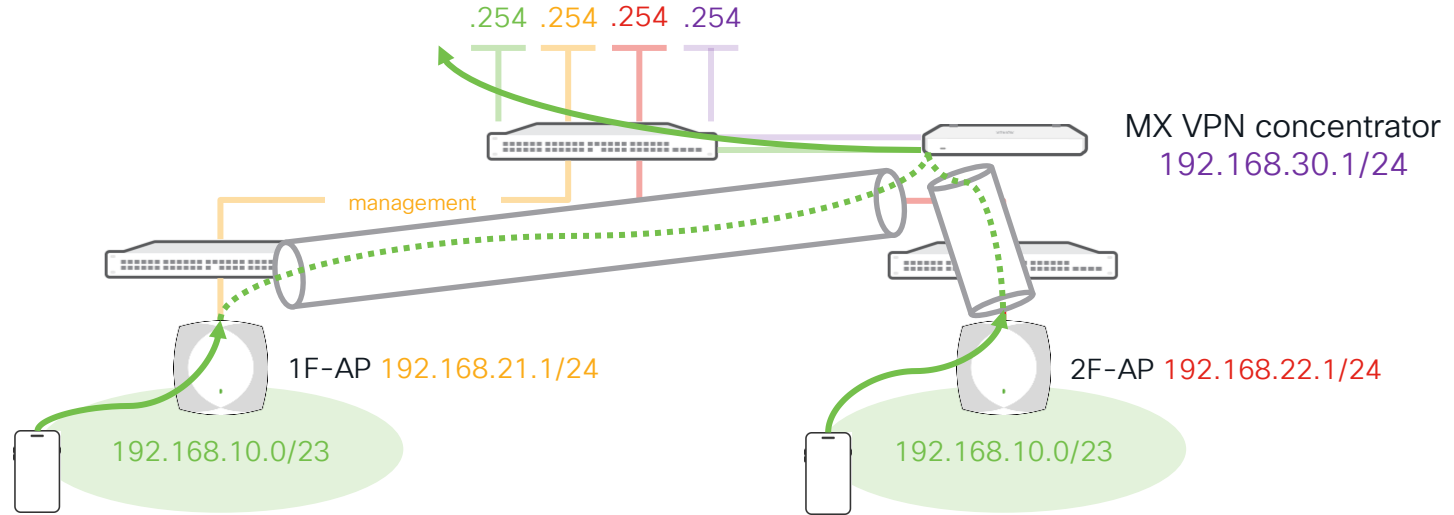


Client roams to 2F-AP and traffic hairpins through 1F-AP

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_Layer_3_Roaming_Best_Practices

Concentrator-Based Layer 3 Roaming

All traffic goes through the MX via tunnel to maintain client IP



Good for guest SSID to terminate in DMZ

https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MR_Wireless/Wireless_Layer_3_Roaming_Best_Practices

MX specification

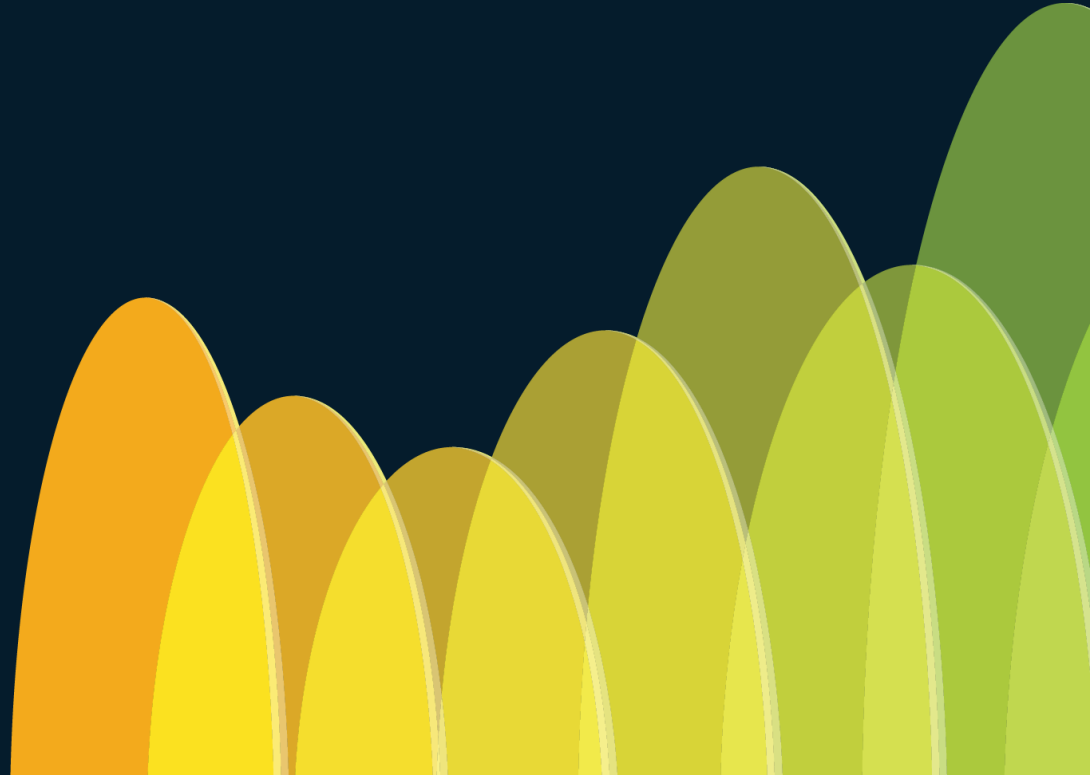
Meraki access point create site to site VPN tunnel to MX, and each MX has a limit

Item	MX105	MX250	MX450
Maximum site to site VPN tunnel count	1000	3000	5000
Recommended maximum site to site VPN tunnel count	500	1000	1500
Multi-Tunnel VPN Throughput RFC2544 1400 Byte	3 Gbps	3.5 Gbps	4.5 Gbps
Multi-Tunnel VPN Throughput EMIX	≤ 2 Gbps	≤ 2 Gbps	4.5 Gbps

MX650 does not support SSID tunneling in initial release

https://documentation.meraki.com/MX/MX_Sizing_Information/MX_Sizing_Principles

Demo/Recap

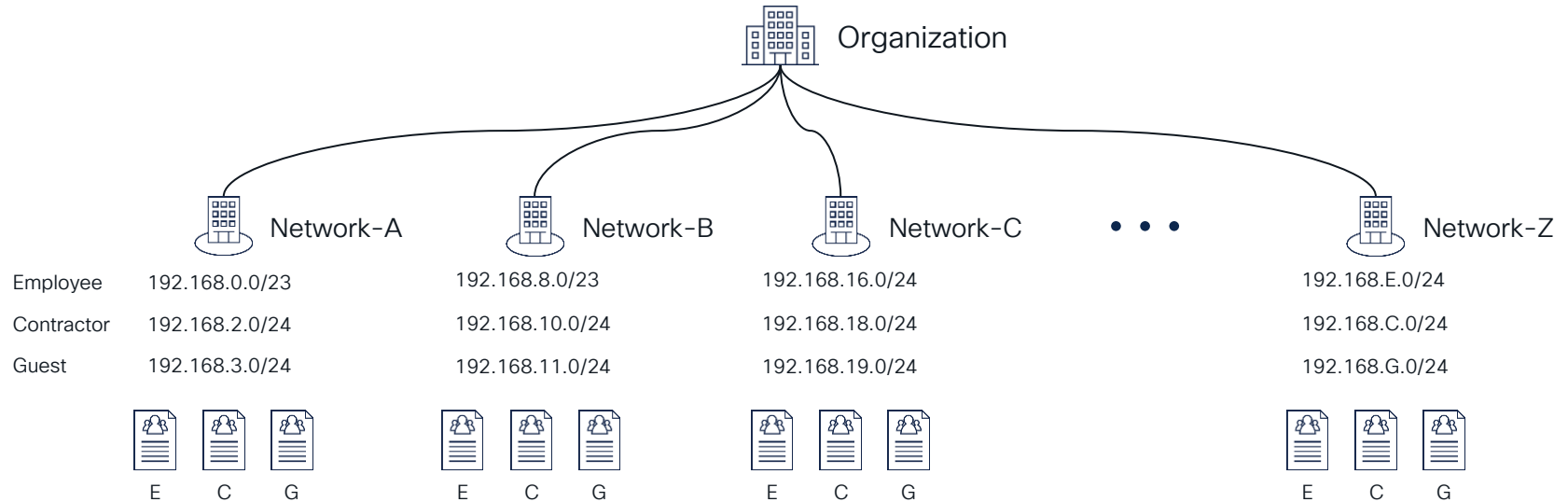


Segmentation



Dynamic group policies with 802.1X

Required to create same group policies for each network



https://documentation.meraki.com/MR/Encryption_and_Authentication/Device_Posturing_using_Cisco_ISF

Network-A contractor group policy

Contractor can communicate with Contractor and IoT, but not Employee

Name

Schedule ⓘ

Bandwidth ⓘ 100 Mbps [details](#)

Hostname visibility

Firewall and traffic shaping ⓘ

Layer 3 firewall

#	Policy	Protocol	Destination	Port	Comment	Actions
1	<input type="button" value="Deny"/>	<input type="button" value="Any"/>	<input type="text" value="192.168.0.0/23"/>	<input type="text" value="Any"/>	<input type="text" value="Network-A Employee"/>	<input type="button" value="⊕"/> <input type="button" value="✕"/>
2	<input type="button" value="Deny"/>	<input type="button" value="Any"/>	<input type="text" value="192.168.8.0/23"/>	<input type="text" value="Any"/>	<input type="text" value="Network-B Employee"/>	<input type="button" value="⊕"/> <input type="button" value="✕"/>
3	<input type="button" value="Deny"/>	<input type="button" value="Any"/>	<input type="text" value="192.168.16.0/24"/>	<input type="text" value="Any"/>	<input type="text" value="Network-C Employee"/>	<input type="button" value="⊕"/> <input type="button" value="✕"/>
	<input type="button" value="Allow"/>	<input type="button" value="Any"/>	<input type="text" value="Any"/>	<input type="text" value="Any"/>	<input type="text" value="Default rule"/>	

[Add a firewall rule](#)

Create the same group policy in Network-B and C. What do you do when Network-D, E, F, and more networks are added?

Adaptive Policy (TrustSec)

Each group should have an identifier on packets (Secure Group Tag), and that ID should be leveraged for policies



1 - Employee



- 1



- 2



- 3



2 - Contractor



- 1



- 2



- 3



3 - Guest



- 1



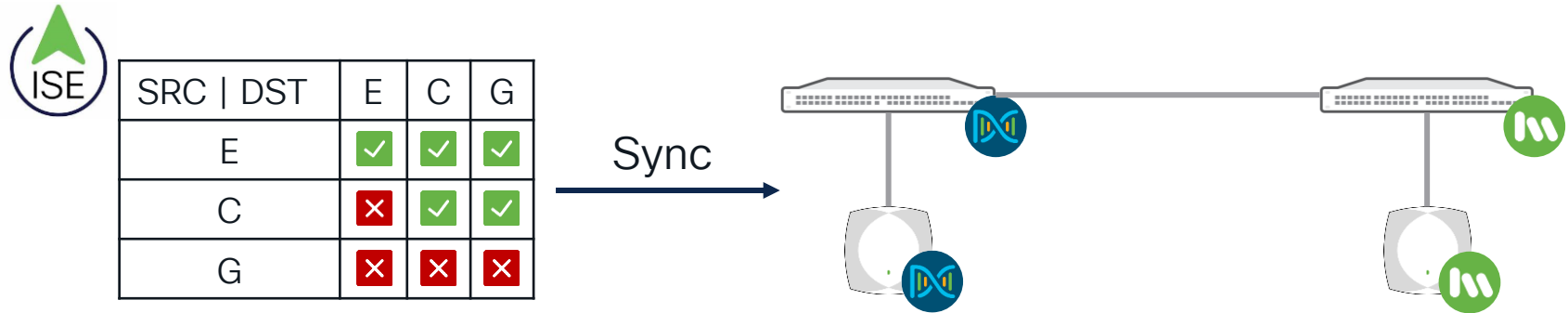
- 2



- 3

Cross domain with Cisco ISE

Secure Group Tag (SGT) is a technology compatible with other Cisco devices. Cisco Identity Service Engine (ISE) can be used to centrally manage SGT and sync to those devices



https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Adaptive_Policy_Overview

Demo

CISCO *Live!*



Adaptive policy license

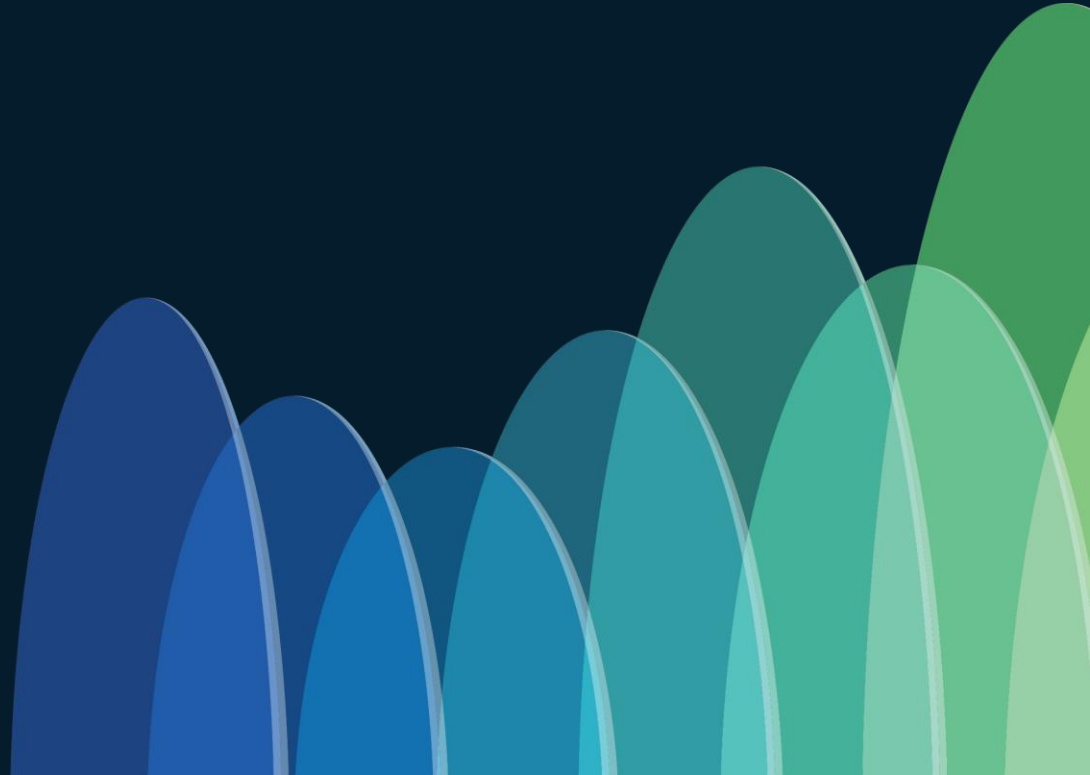
License	Adaptive Policy
MX Enterprise	
MX Advanced Security	(Transport only)
MX SD-WAN Plus	✓
MS Enterprise	
MS Advanced	✓
MR Enterprise	
MR Advanced	✓

Adaptive policy limitation

Item	Limit
Maximum adaptive policy groups	60
Maximum number of policies configured	3600
Maximum custom ACL per policy	7
Maximum number of ACE entries per custom ACL	16
Maximum IP to SGT mappings	8000

https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Adaptive_Policy_Configuration_Guide

Architecture



Unified hardware

Architecture decision is not tied to device refresh cycle



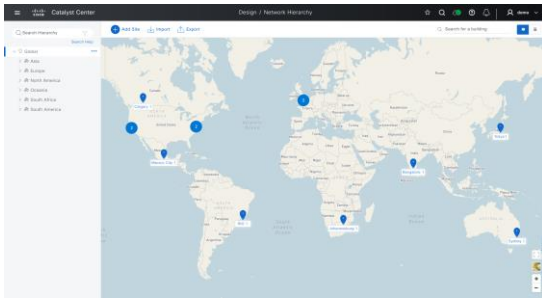
Cisco DNA Management Mode
C9800 & Catalyst Center Stack



Meraki Management Mode
MR Dashboard Stack

Gap for monitoring

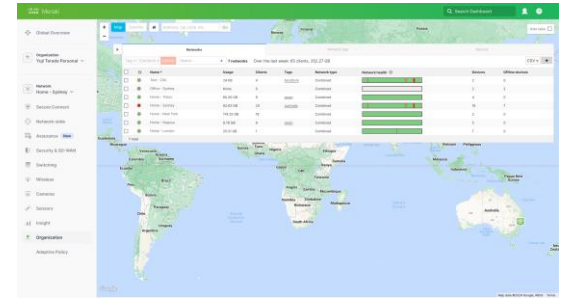
No monitoring for customers using Catalyst without Catalyst Center



Catalyst Center



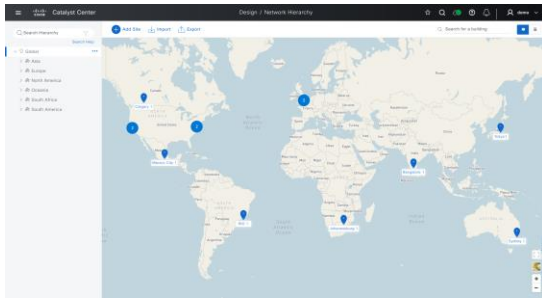
?



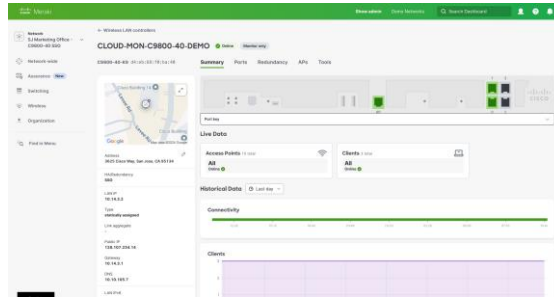
Cloud Dashboard

Monitor software

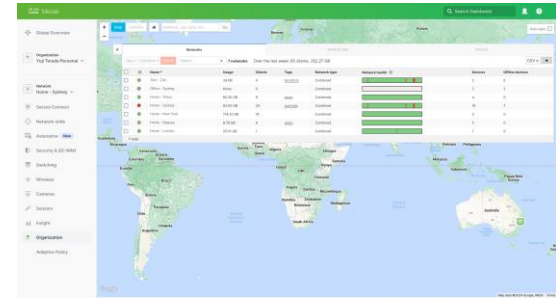
Cisco released C9800 monitor mode in Cloud Dashboard



Catalyst Center



C9800 monitor mode



Cloud Dashboard

Continue to manage your infrastructure through existing SNMP/Syslog software, and prepare infrastructure for the cloud

Demo



Monitor C9800 from Cloud Dashboard

The screenshot displays the Cisco Meraki Cloud Dashboard interface for monitoring a C9800-40 SSO controller. The top navigation bar is green with the Meraki logo and links for 'Show admin', 'Demo Networks', and a search bar. The left sidebar contains navigation options: Network (selected), Network-wide, Assurance (New), Switching, Wireless, and Organization. The main content area shows the controller's status as 'Online' and 'Monitor only'. It includes a map of the location at 3625 Cisco Way, San Jose, CA 95134, and a physical layout diagram of the controller. The 'Live Data' section shows 15 total access points, all online, and 3 total clients, all online. The 'Historical Data' section shows a connectivity graph for the last day.

Network
SJ Marketing Office -
C9800-40 SSO

← Wireless LAN controllers

CLOUD-MON-C9800-40-DEMO Online Monitor only

C9800-40-K9 d4:eb:68:f0:ba:40

Summary Ports Redundancy APs Tools

Map view showing location: Cisco Building 14, Levee Rd, Cisco Building. Address: 3625 Cisco Way, San Jose, CA 95134. HA/Redundancy: SSO. LAN IP: 10.14.3.2. Type: statically assigned. Link aggregate: -.

Physical layout diagram showing ports and status.

Port key

Live Data

Access Points 15 total
All Online Online

Clients 3 total
All Online Online

Historical Data Last day

Connectivity graph showing status over time (12:26 to 10:4).

https://documentation.meraki.com/Cloud_Monitoring_for_Catalyst/Getting_Started/Monitoring_Catalyst_Wireless_9800_Controllers

Limitations of hardware and Cloud Dashboard

Not all scenarios are supported in monitor mode as of today

	Hardware		Cloud Dashboard	
	Maximum number of access points	Maximum number of clients	Maximum number of access points	Maximum number of clients
C9800-L (F or C)	250 (500)	5,000 (10,000)	250	3,000
9800-40	2,000	32,000	1,300	10,000
9800-80	6,000	64,000	2,000	20,000

https://documentation.meraki.com/Cloud_Monitoring_for_Catalyst/Getting_Started/Cloud_Monitoring_for_Catalyst_Wireless_Requirements

Summary

Radio wave basic

- Wi-Fi and human voice

RF Profile

- Enable features only when required
- Can't beat physics!

6 GHz

- WPA3 required

Design

- Cloud Dashboard limitations
- Access point limitations
- Onprem WLC for L3 roaming (as for now)

Segmentation

- AdP to simplify policy management
- Cross architecture with SGT

Architecture

- Change to DNA or Meraki at your preference
- C9800 monitor mode

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC