

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC





Deploying Next Generation Guest Experiences with Meraki Dashboard

Fletcher Joyce, Solutions Engineer – Cisco Networking
BRKEWN-2418



Fletcher Joyce

Solutions Engineer, Networking
fjoyce@cisco.com



CISCO *Live!*

#CiscoLiveAPJC



About Me



Cisco Webex App

Questions?

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

How

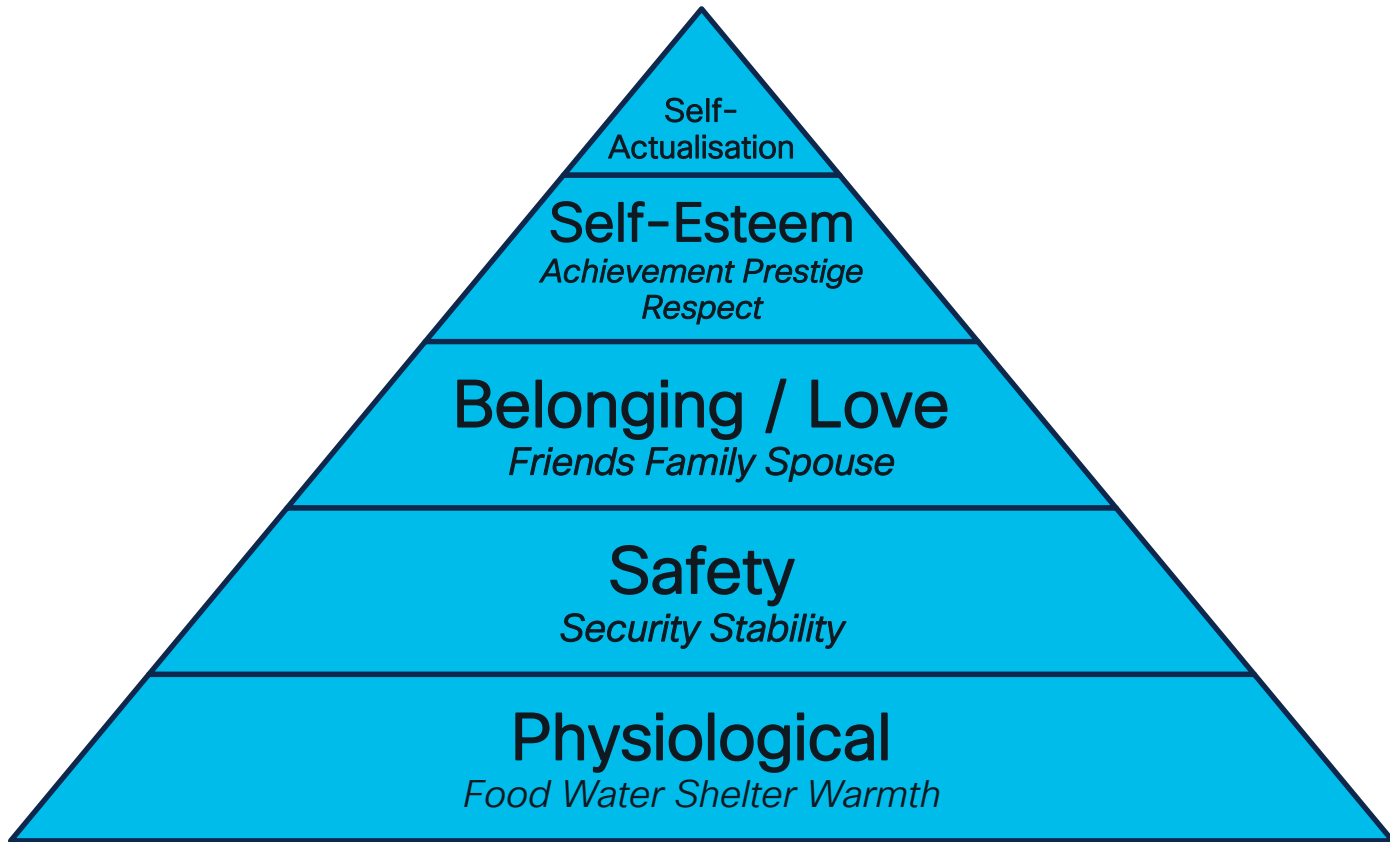
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

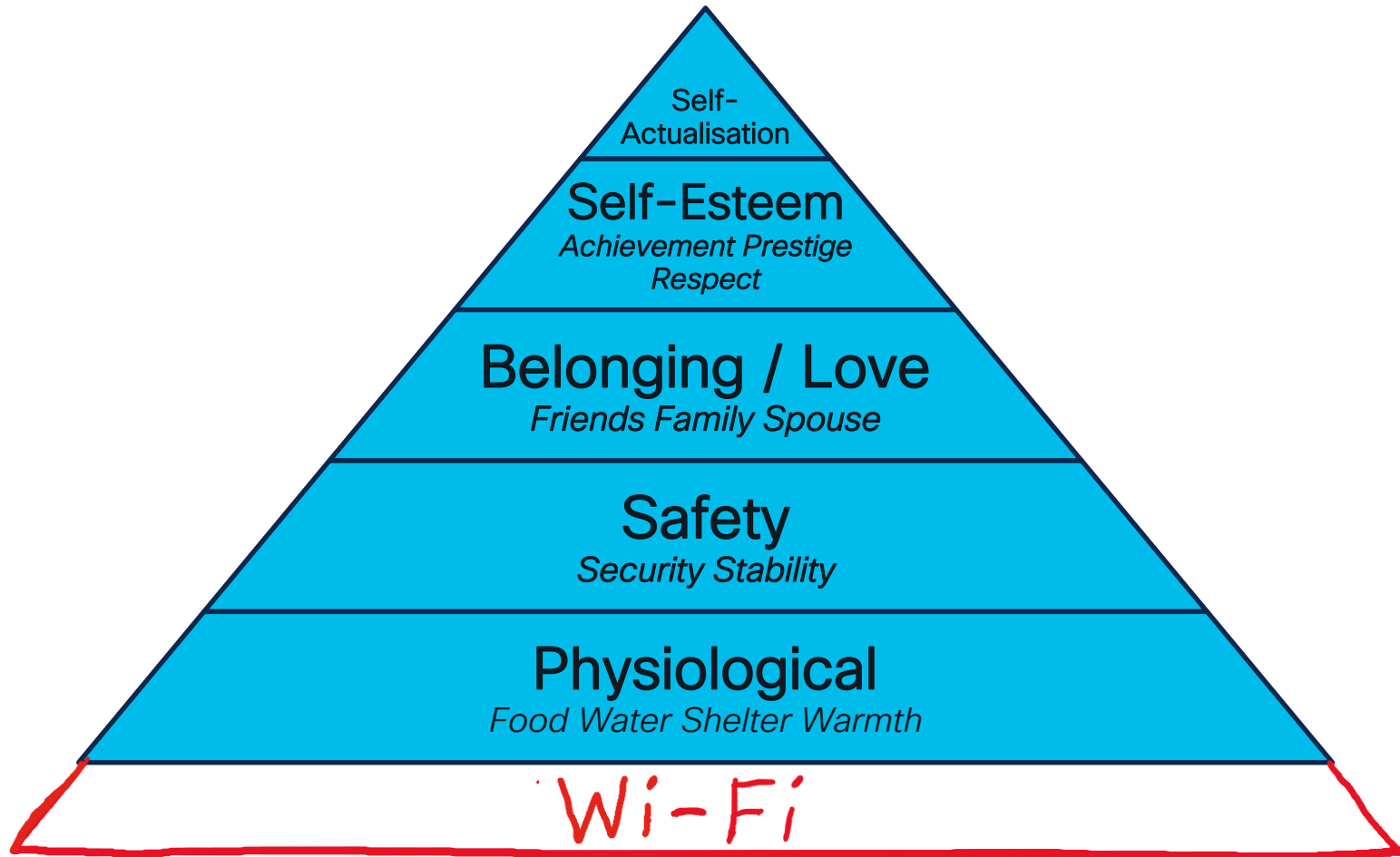
Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKEWN-2418>







Agenda

- The need for compelling guest experiences
- iPSK and Wireless Personal Network (WPN)
- Beyond the Wi-Fi domain
 - Meraki IoT for healthy and sustainable guest experiences
 - Assa Abloy Door Lock Integration
- Conclusion



Who is a Guest?

A photograph of a man with glasses and a beard, wearing a brown hoodie, sitting at a wooden desk in a modern office. He is looking at a laptop. In the foreground, another person is seen from the back, also working on a laptop. The office has large windows and a modern lighting fixture with multiple glass shades.

Corporate



Corporate



Aged Care



Corporate



Aged Care



Campus
Housing



Corporate



Aged Care



Campus
Housing



Mining
Camps

Key Finding:

*Tourists value quality
guest Wi-Fi even higher
than breakfast...*

International Journal of Contemporary Hospitality
Management, Kucukusta, 2017

Online Reviews

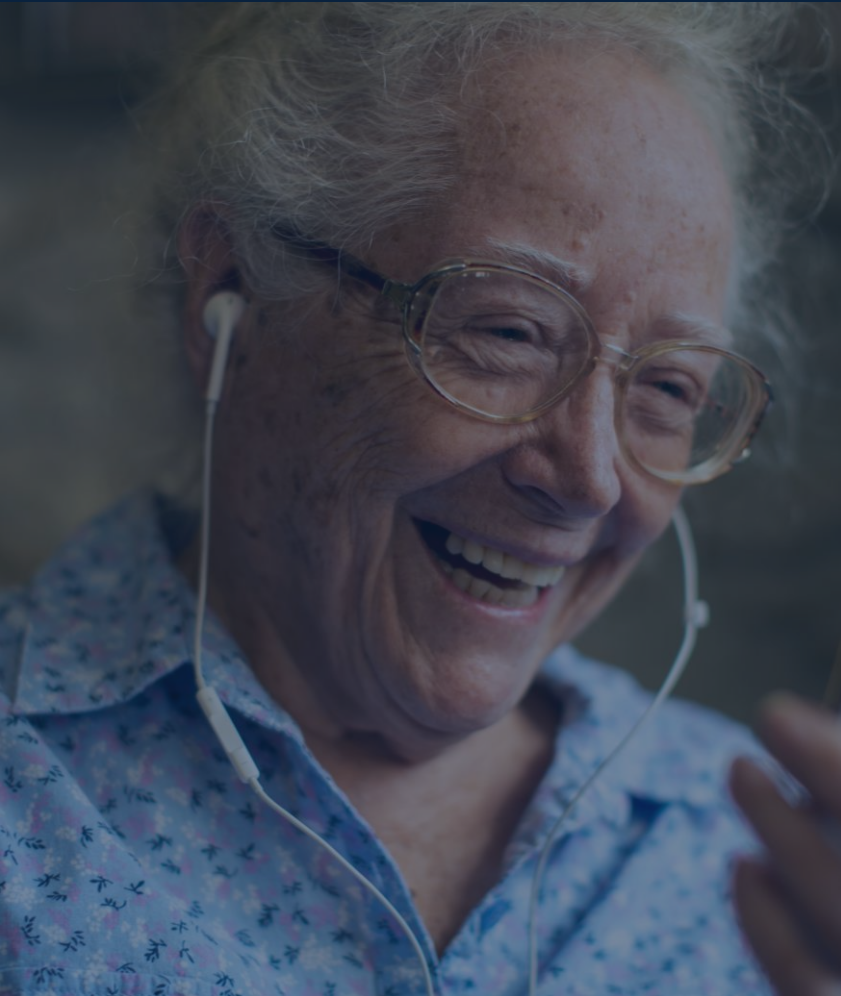
“....Seriously Australia, why are you so stingy with Wi-Fi?”

“On their website, they advertise with the words „WiFi, featured in all 20 rooms“. This is definitely not true. The signal of the WiFi is rather bad and I wasn't able to log into it at all during my stay!!”

“Having read previous reviews about poor WiFi and responses from the [hotel] reporting it was fixed, it was disappointing to find such poor service and dropouts. Will think twice before going there again, and I cannot trust any responses they give to counter bad reviews.”

“It’s Skibidi... 0/5 Stars”

Brock, Aged 15



74.5% of adults over 65
use the internet regularly

Australian Bureau of Statistics, 2020

A Common Scenario



Common Guest Methods

Splash Pages

Lobby Ambassadors

Sponsored Guest
Access

*BYOD onboarding
workflows*

Backend Infrastructure (NAC)



Other Common Challenges

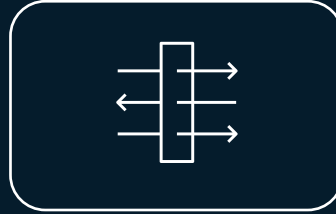
- Device Support (802.1X / Certificates)
- Splash Page Issues
- Support for Multiple Devices
- Inflexible Segmentation
- Reliance on backend infrastructure / Complex Integrations
- Proactive Monitoring / Visibility



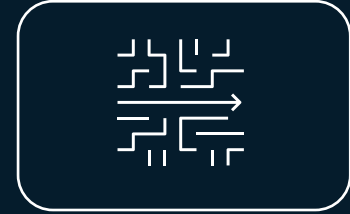
WHAT WE REALLY WANT IS AN “AT HOME” EXPERIENCE



Secure



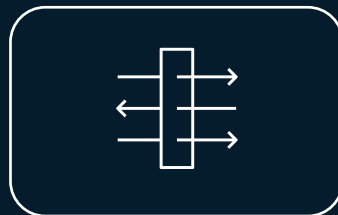
Segmented



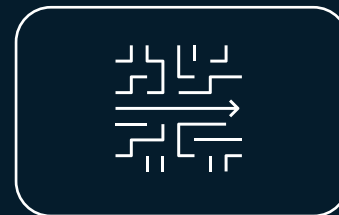
Simple



iPSK



WPN



API

HOW DOES THIS WORK IN PRACTICE?





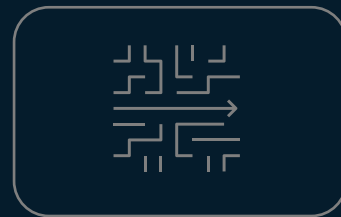
A Frictionless Guest Experience



iPSK



WPN



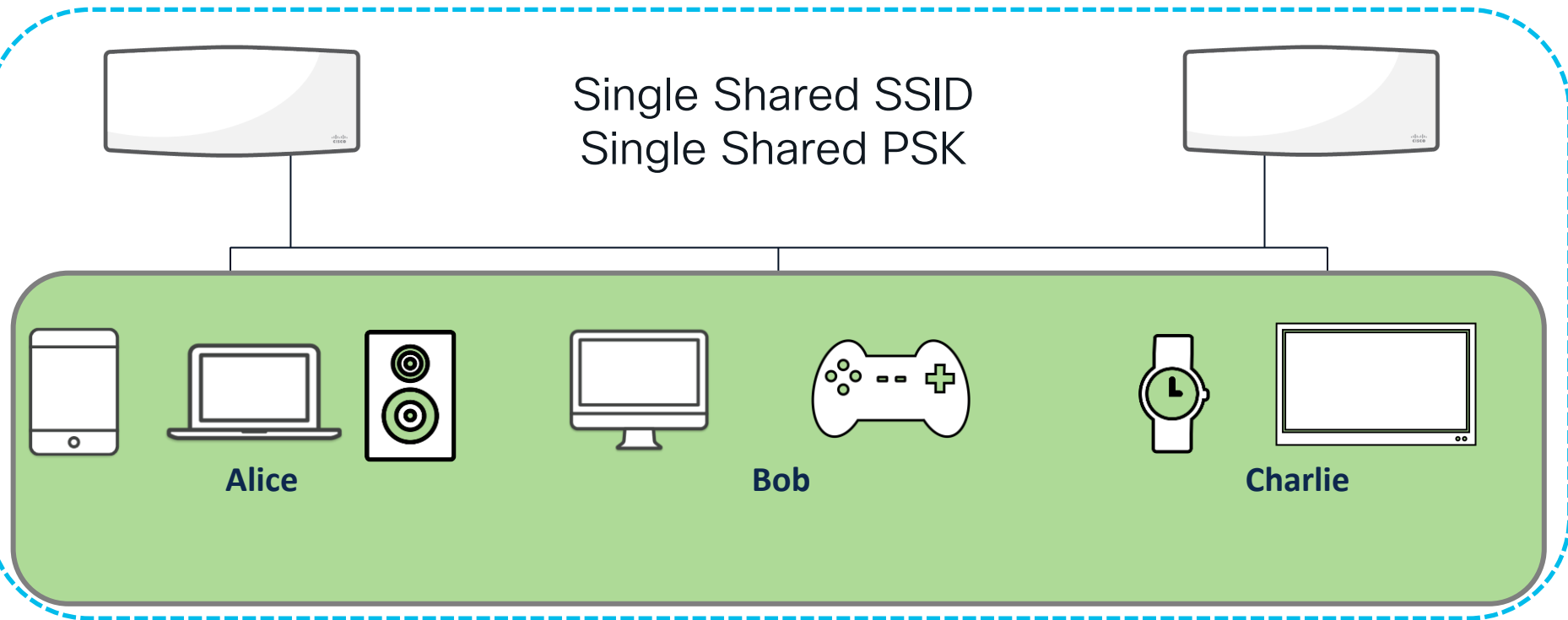
API

WHY CAN'T WE PROVIDE AN “AT HOME”
EXPERIENCE IN AN “AT HOME” WAY?

CHALLENGE #1 – IDENTITY

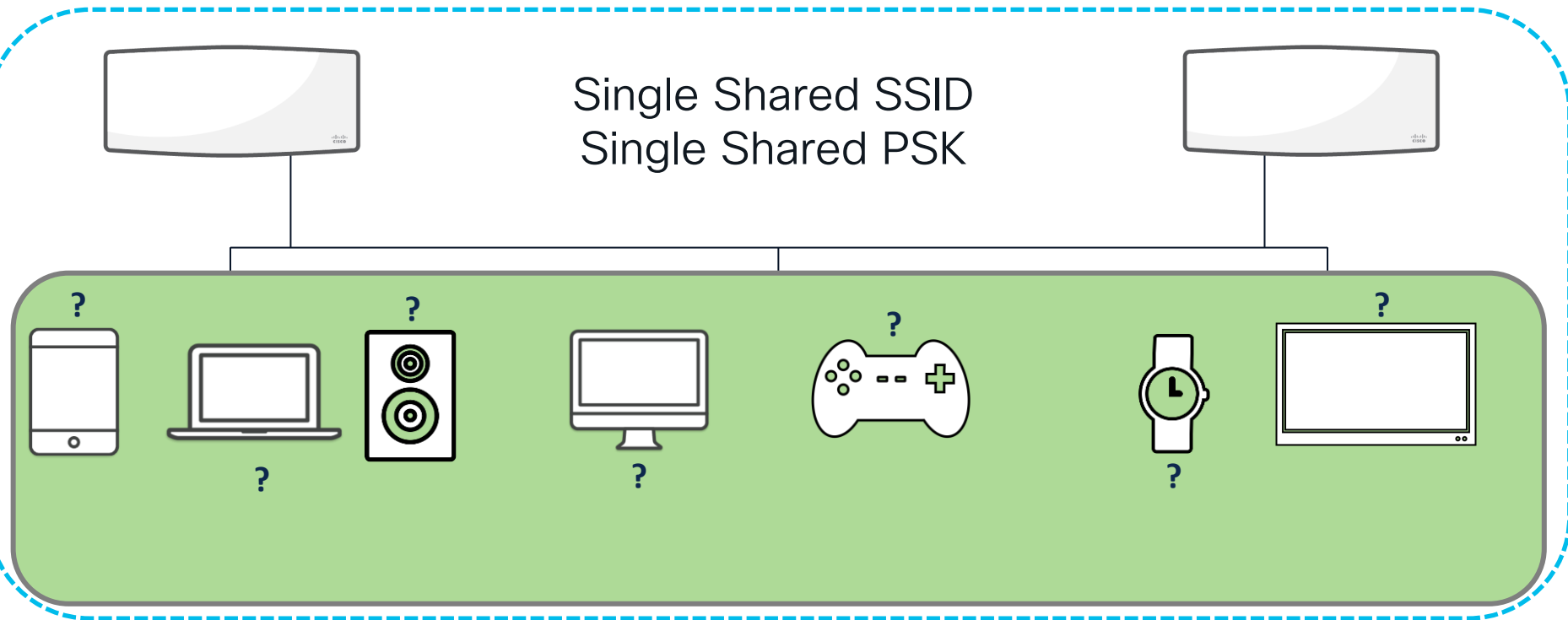
Connect + Secure

Shared SSID – Traditional WPA-Personal



Connect + Secure

Shared SSID – Traditional WPA-Personal



CHALLENGE #2 – SHARED SECRETS

GUEST

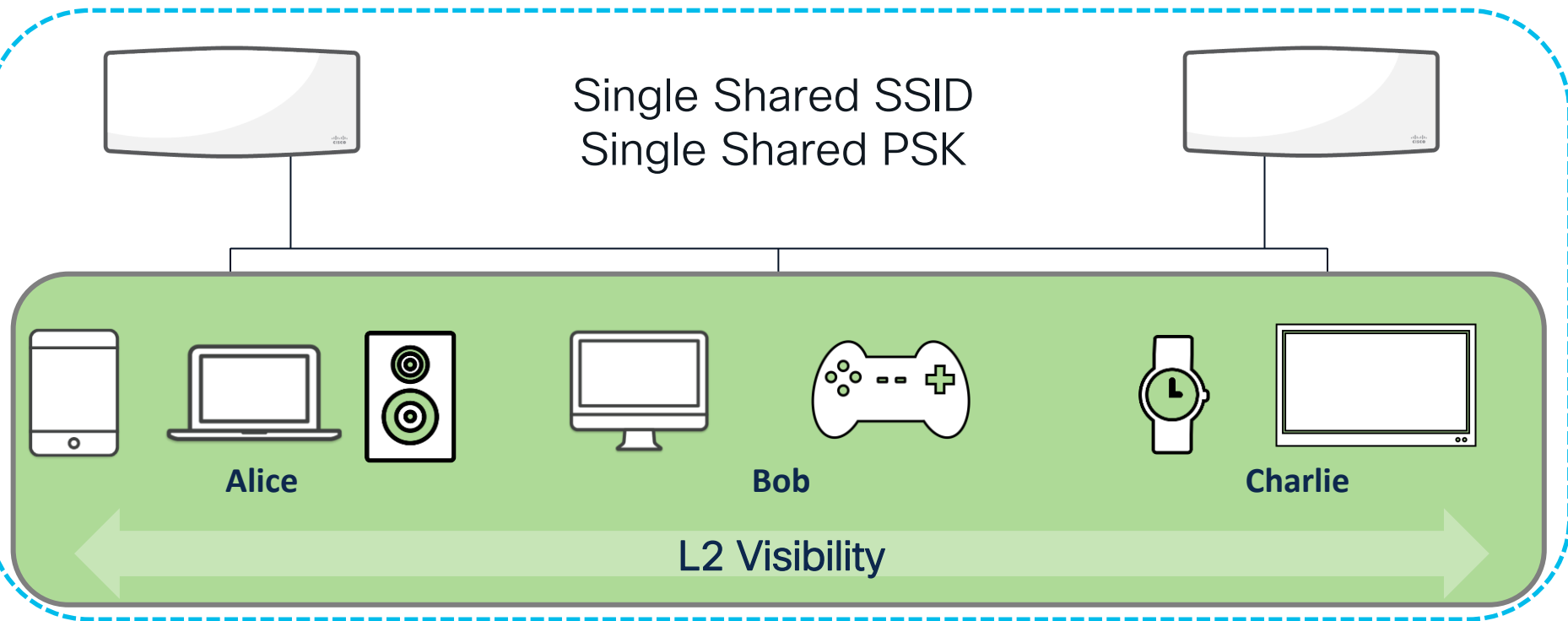
Wi-Fi

QtGu35t#

SHARED SECRETS GET
SHARED

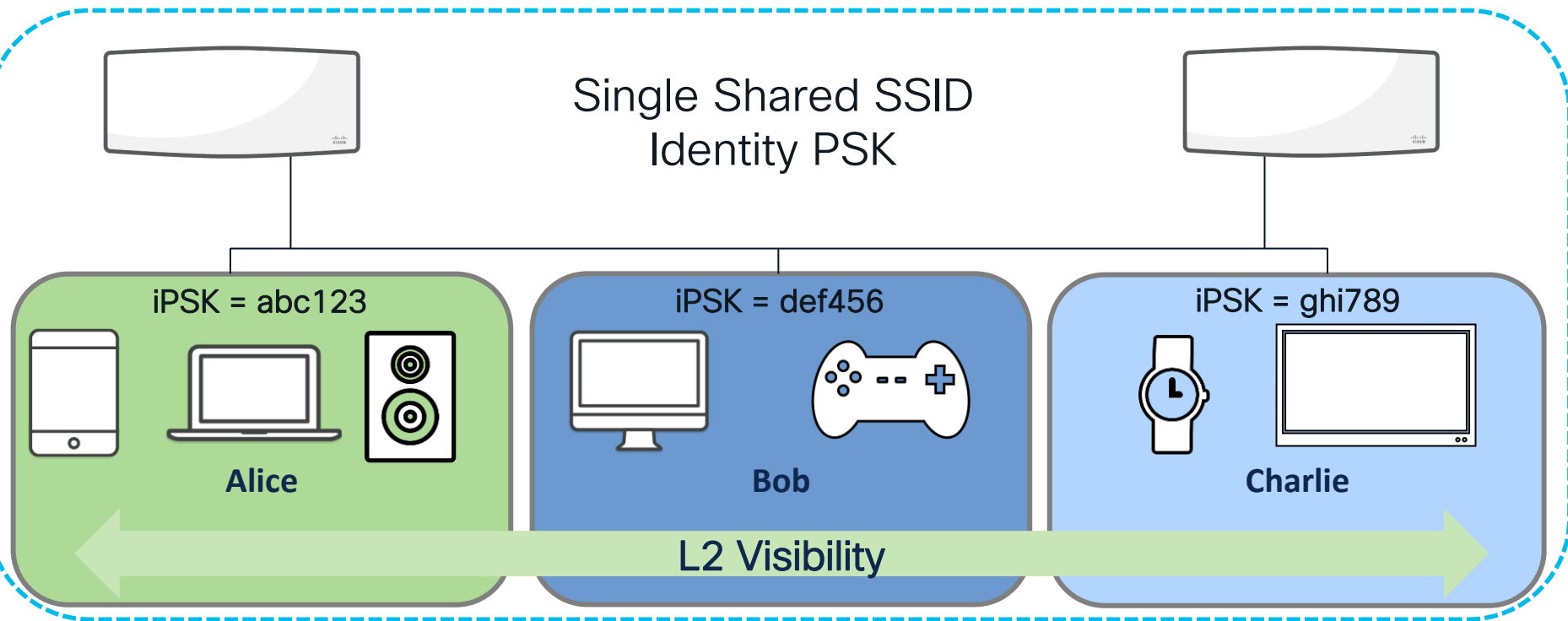
Connect + Secure

Shared SSID – Traditional WPA-Personal



Connect + Secure

Shared SSID – Identity PSK without RADIUS



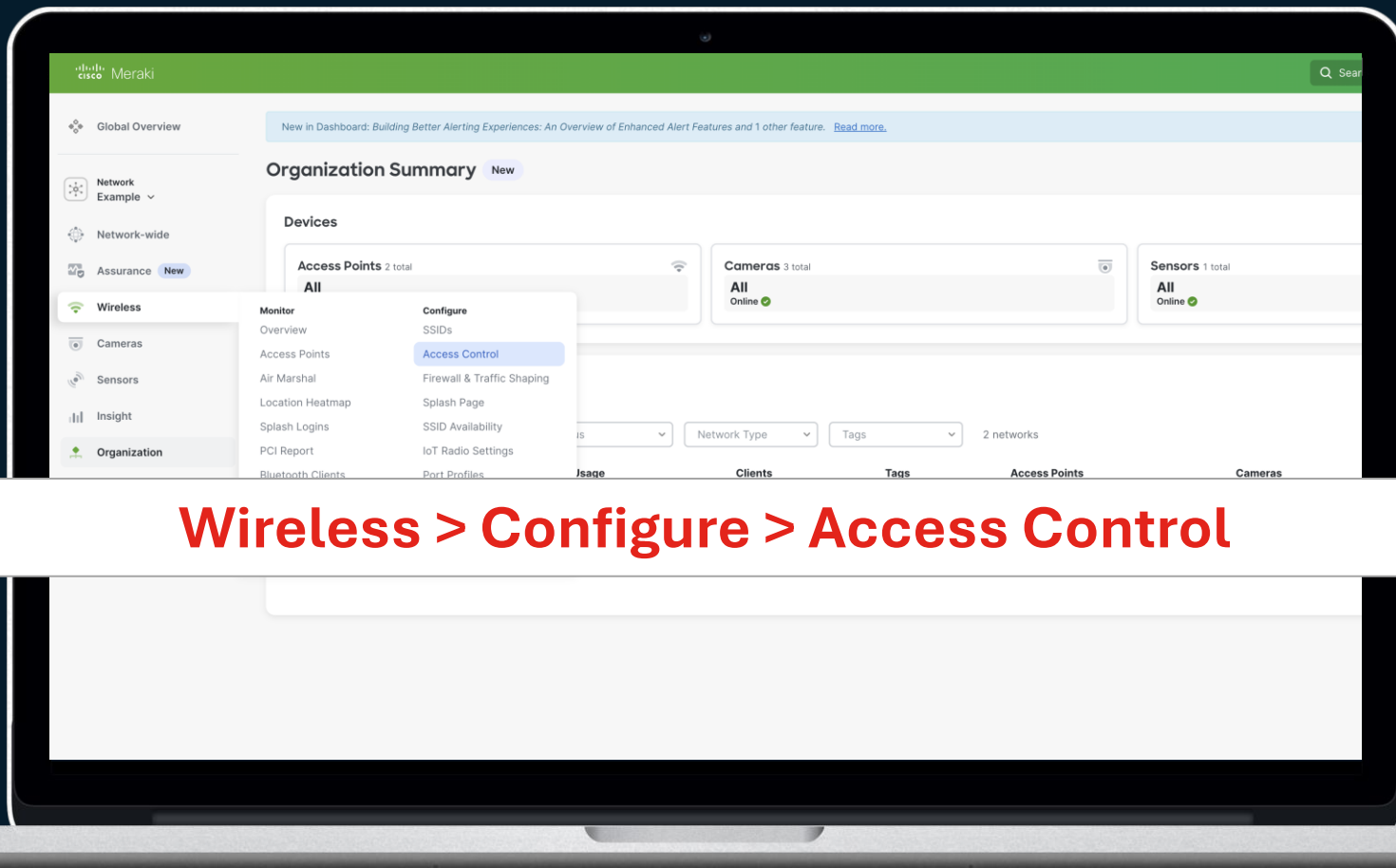
Connect + Secure

Shared SSID – Identity PSK without RADIUS

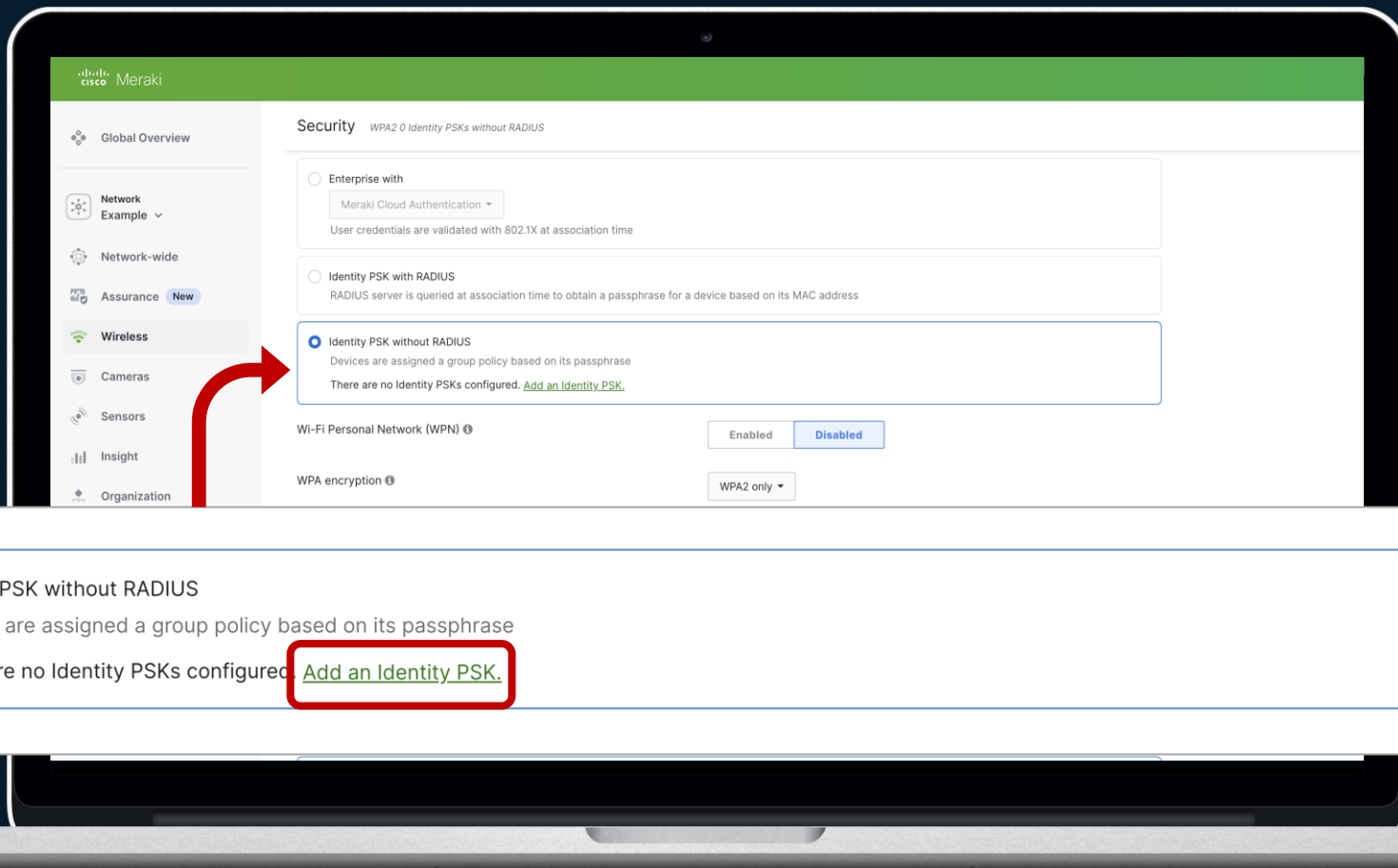
iPSK
abc123
def456
ghi789
<.....>



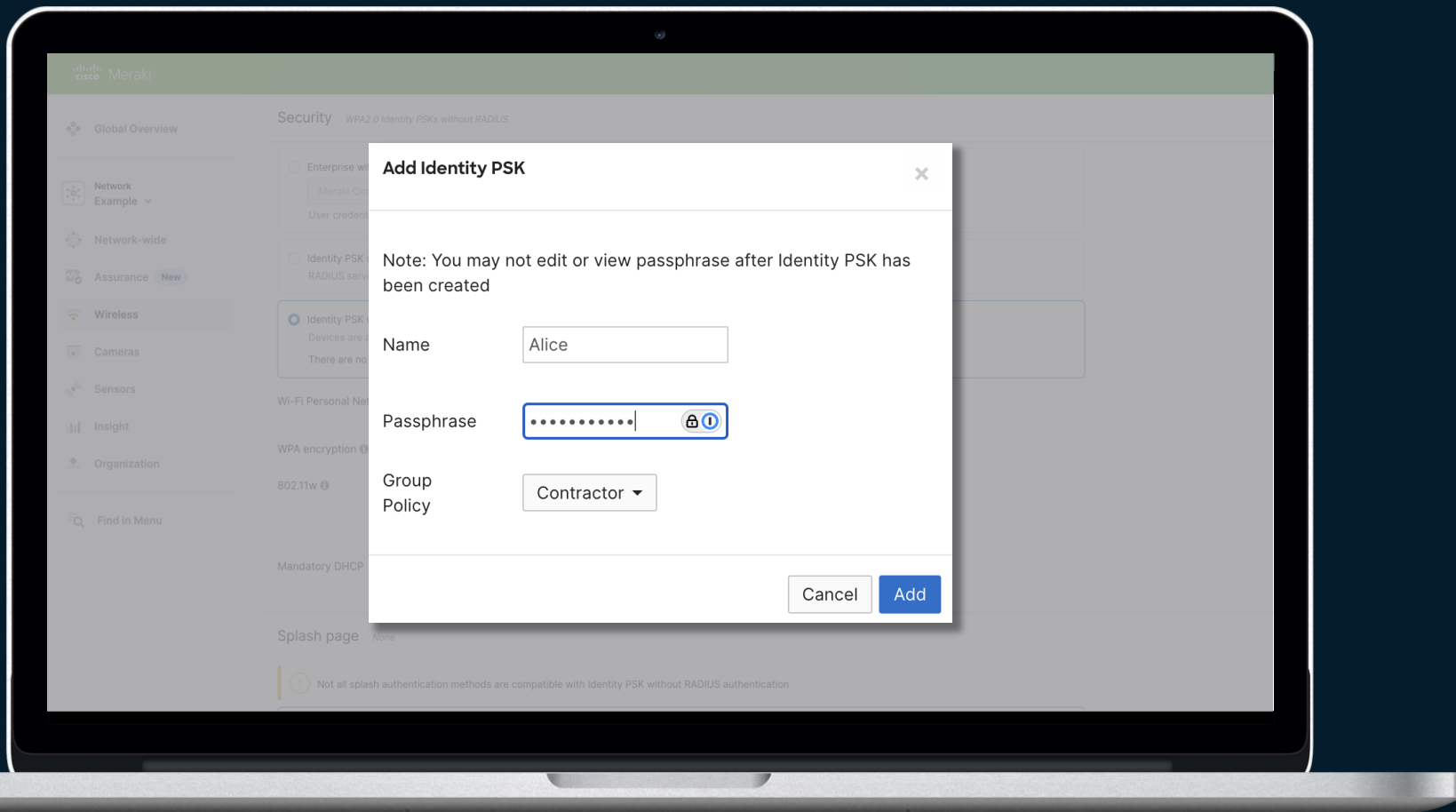
Up to 5000 iPSKs per SSID



Wireless > Configure > Access Control



- ☒ Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase
There are no Identity PSKs configured. [Add an Identity PSK.](#)



Global Overview

Network Example ▾

Network-wide

Assurance **New**

Wireless

Cameras

Sensors

Insight

Organization

Find in Menu

Security WPA2 3 Identity PSKs without RADIUS

☒ Identity PSK without RADIUS

Devices are assigned a group policy based on its passphrase

0

Search Identity PSKs...

3 Identity PSKs

Add

Delete

☐	Name ▲	Pre-Shared Key	Group Policy
☐	Alice		Contractor
☐	Bob		Contractor
☐	Charlie		Contractor

Wi-Fi Personal Network (WPN) ⓘ

Enabled

Disabled

WPA encryption ⓘ

WPA2 only ▾

802.11w ⓘ

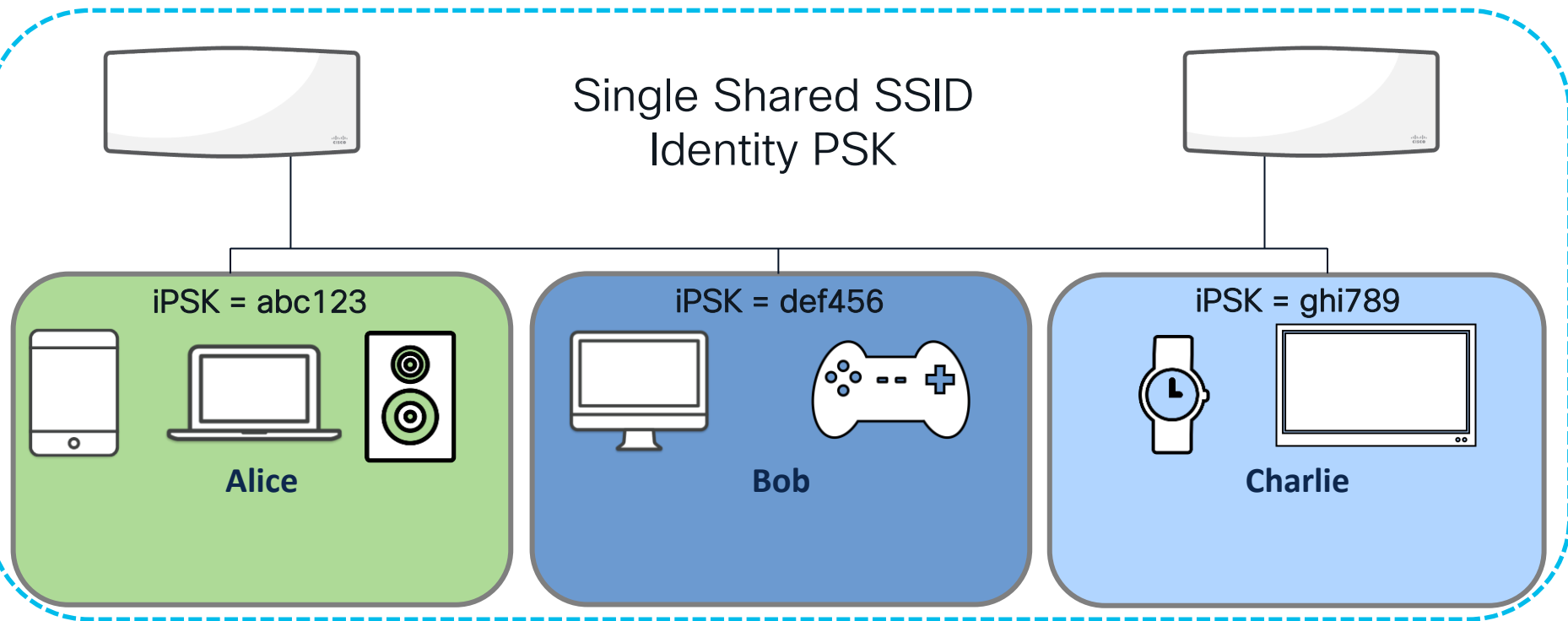
☐ Enabled (allow unsupported clients)

☐ Required (reject unsupported clients)

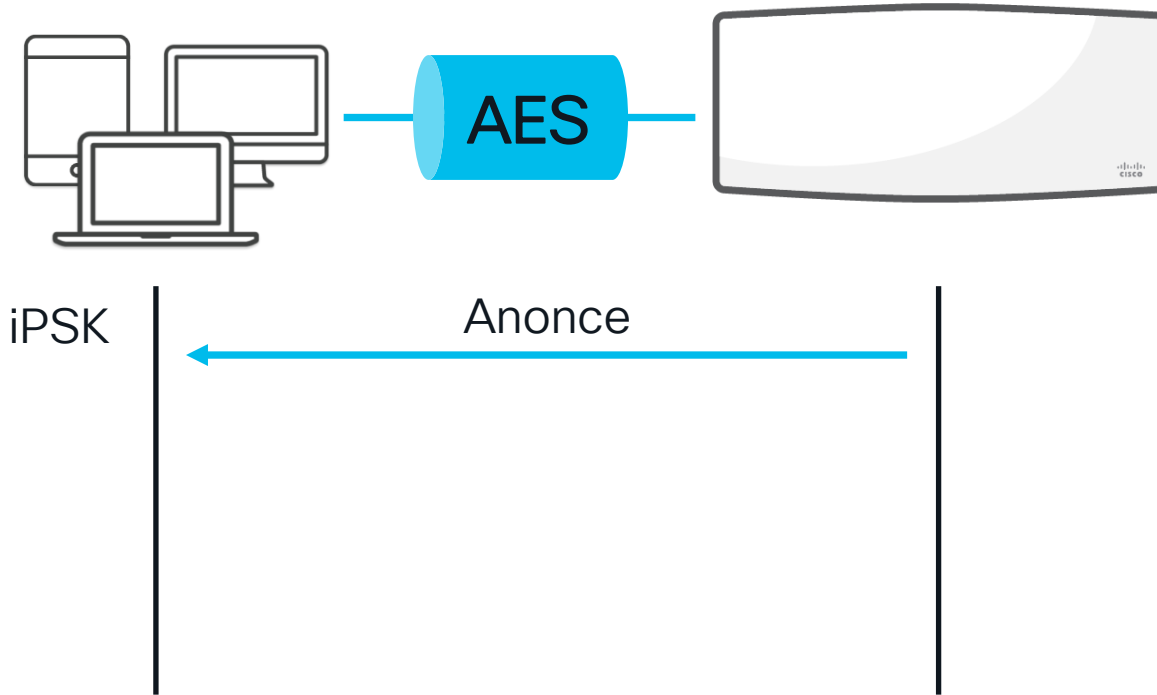
☒ Disabled (never use)

Connect + Secure

Shared SSID – Identity PSK without RADIUS

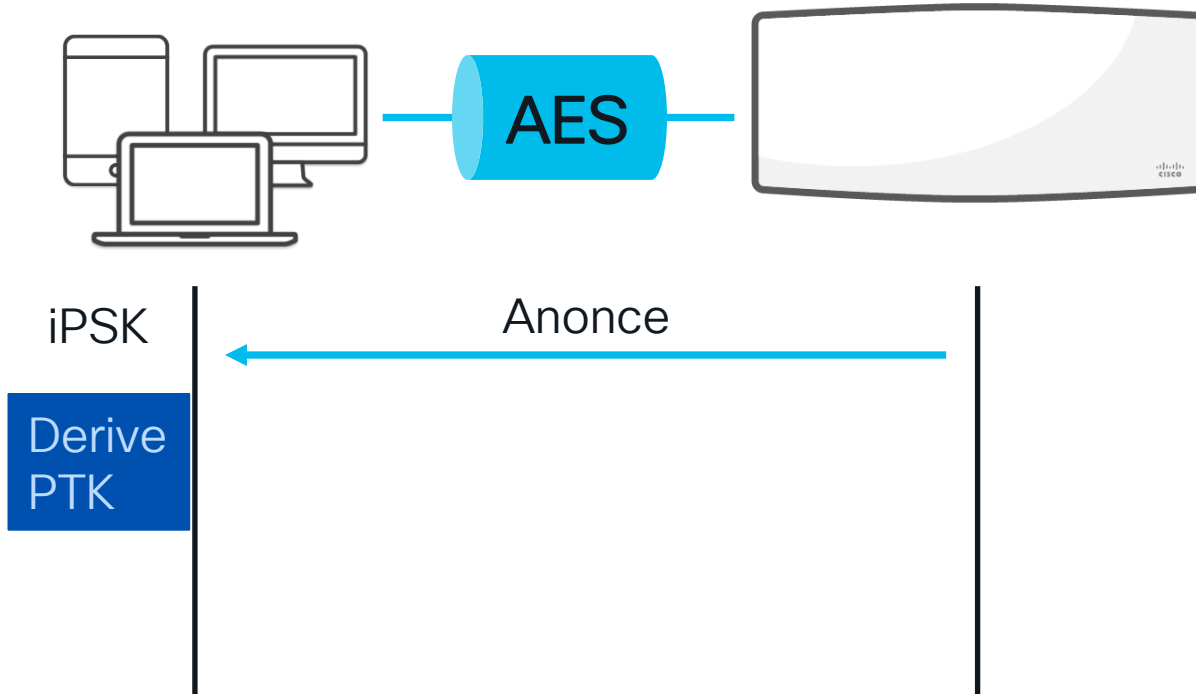


iPSK without RADIUS



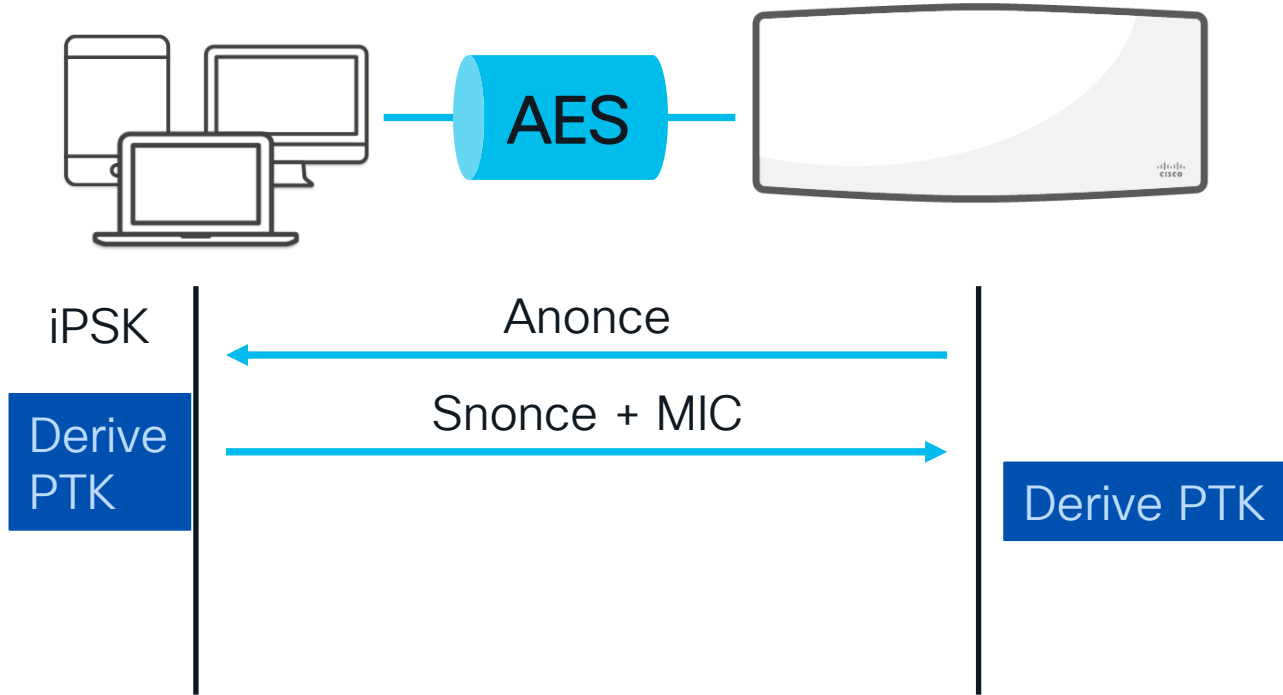
$$\text{PTK} = \text{PRF} (\text{PSK} + \text{Anonce} + \text{Snonce} + \text{AP MAC} + \text{STA MAC})$$

iPSK without RADIUS



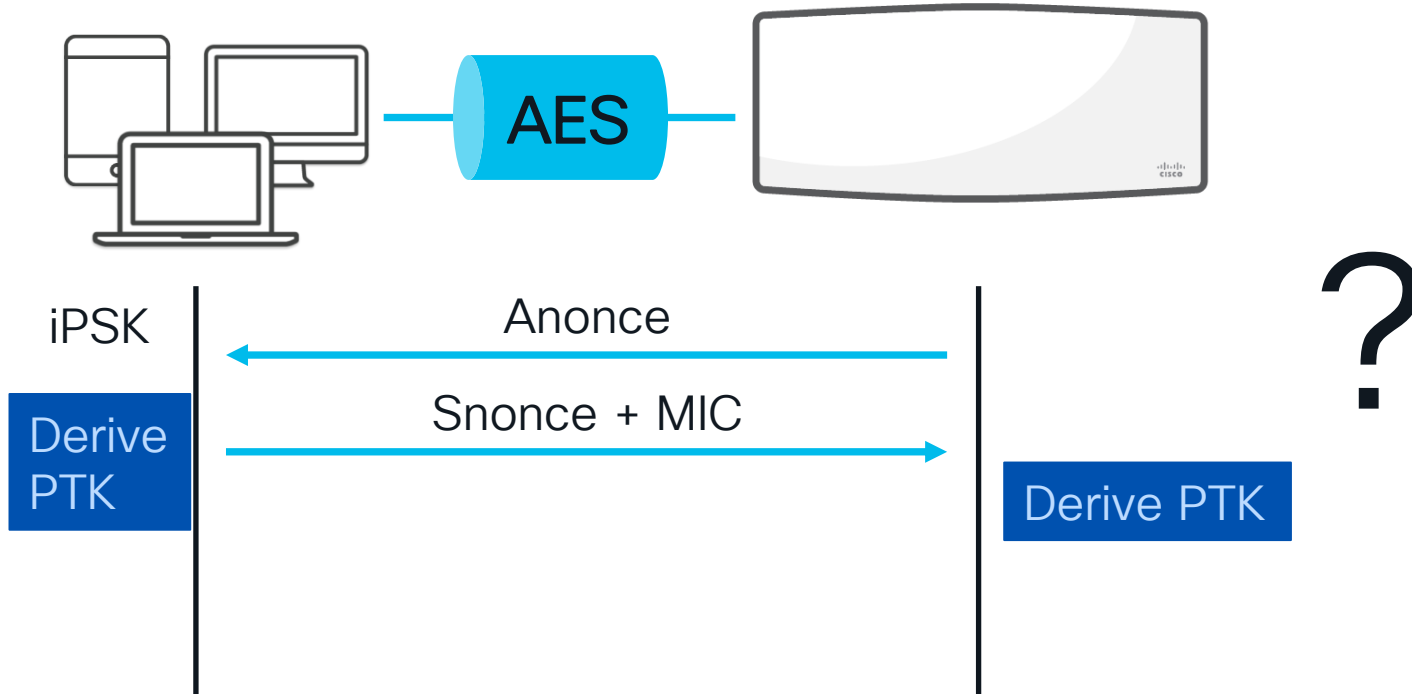
$$\text{PTK} = \text{PRF} (\text{PSK} + \text{Anonce} + \text{Snonce} + \text{AP MAC} + \text{STA MAC})$$

iPSK without RADIUS



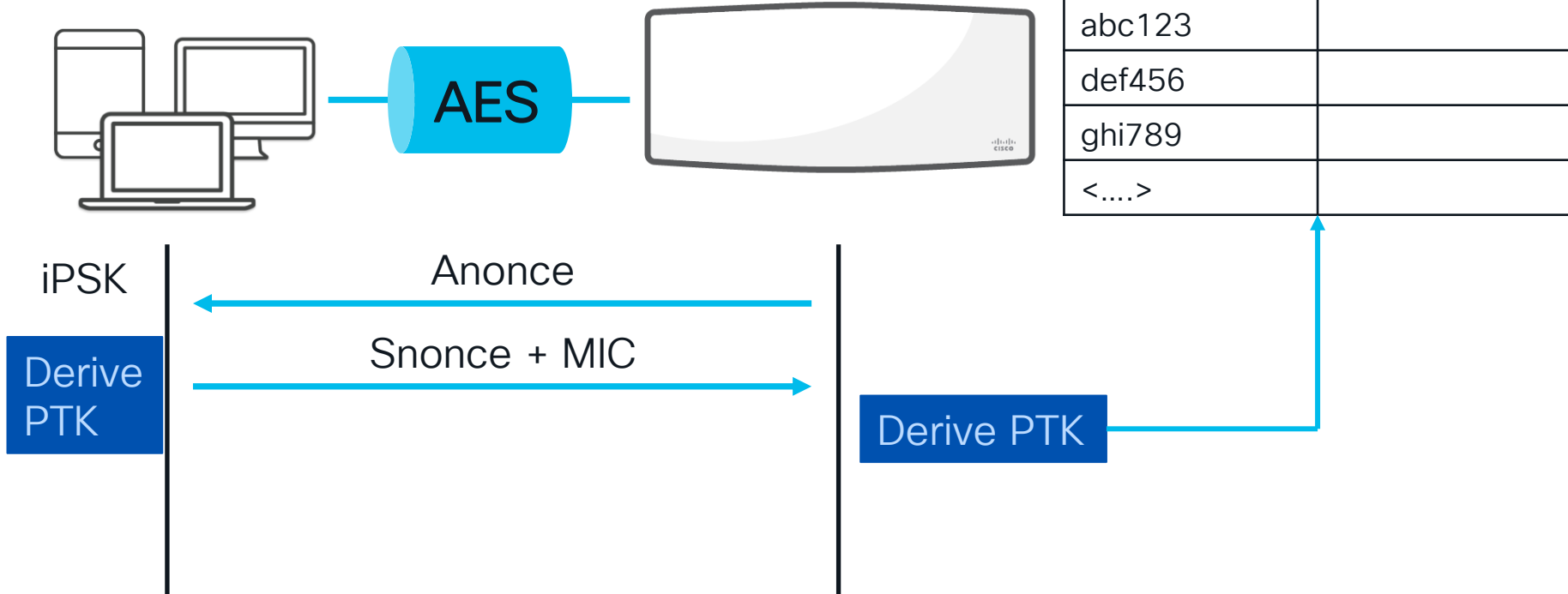
$$\text{PTK} = \text{PRF} (\text{PSK} + \text{Anonce} + \text{Snonce} + \text{AP MAC} + \text{STA MAC})$$

iPSK without RADIUS



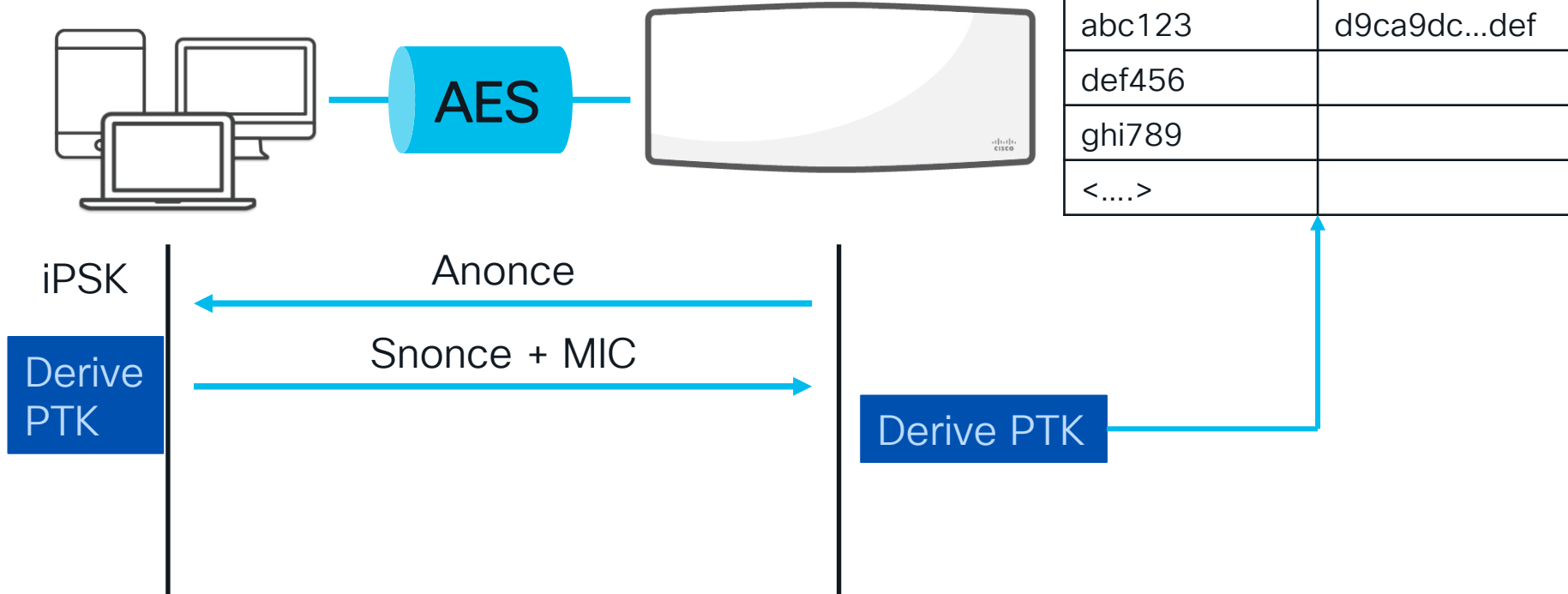
$$PTK = PRF (PSK + Anonce + Snonce + AP\ MAC + STA\ MAC)$$

iPSK without RADIUS



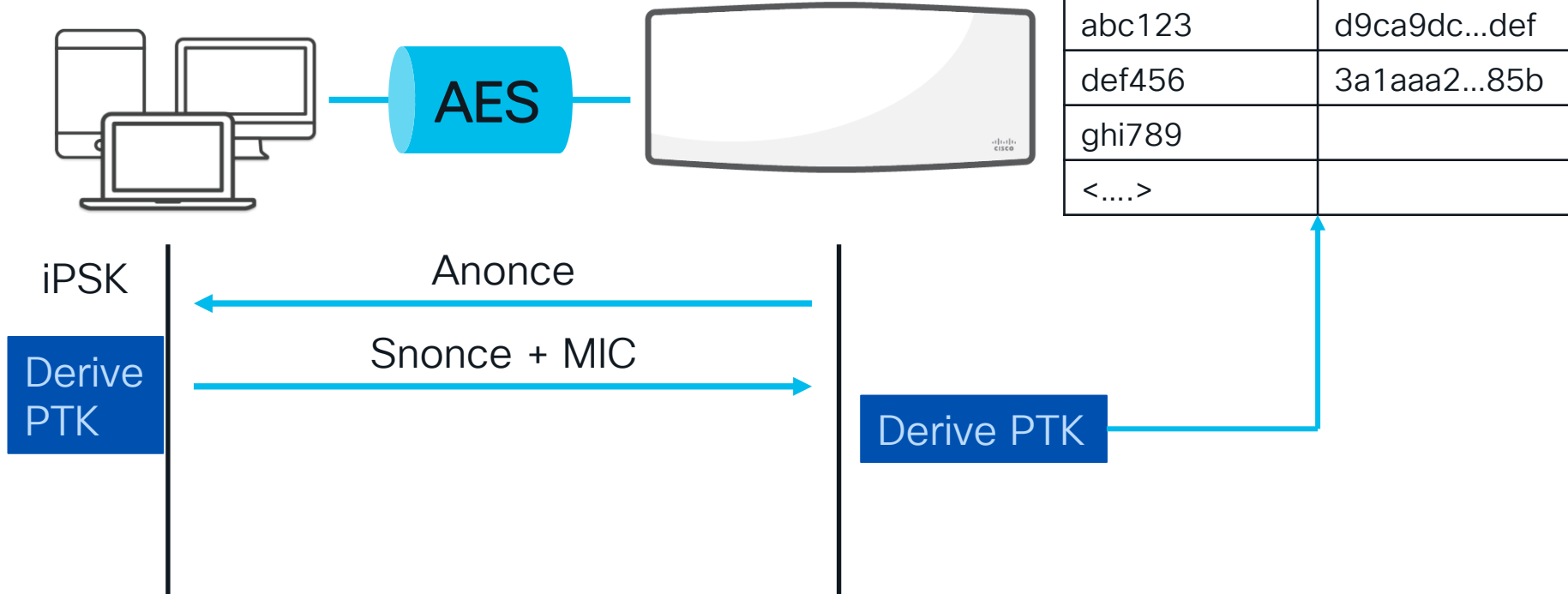
PTK = PRF (PSK + Anonce + Snonce + AP MAC + STA MAC)

iPSK without RADIUS



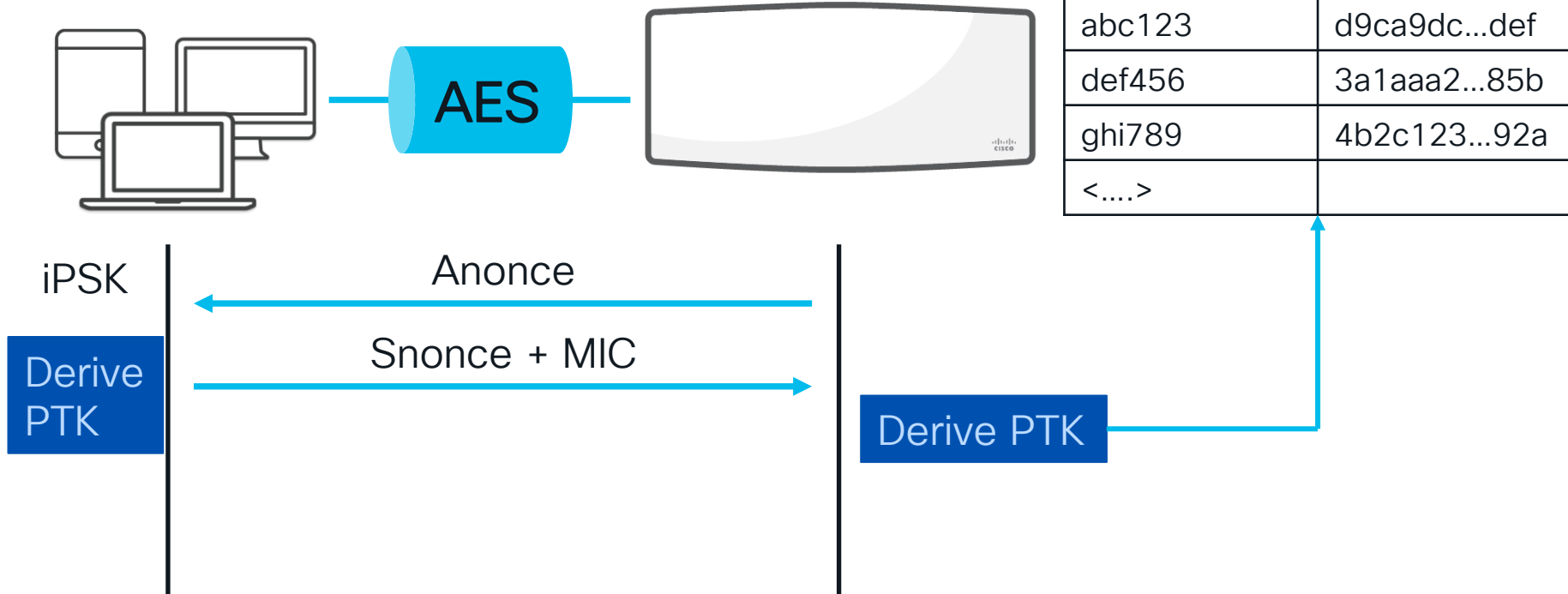
PTK = PRF (PSK + Anonce + Snonce + AP MAC + STA MAC)

iPSK without RADIUS



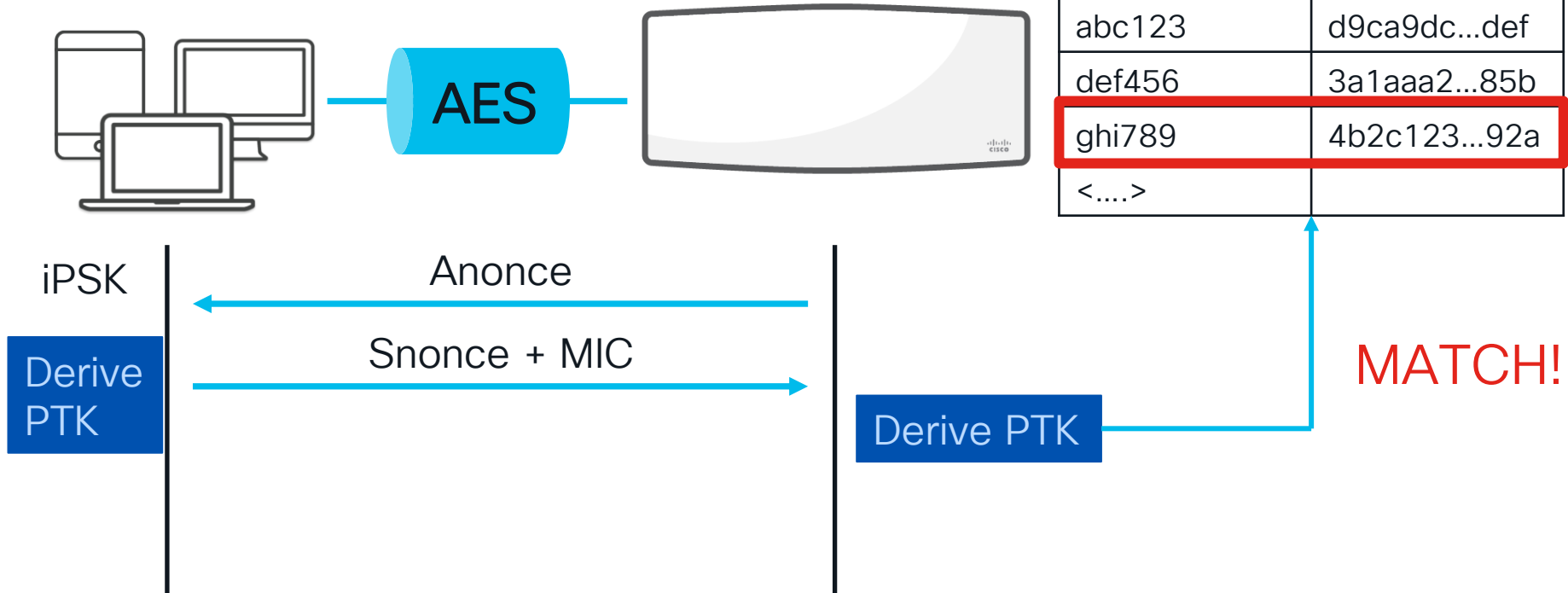
$$\text{PTK} = \text{PRF}(\text{PSK} + \text{Anonce} + \text{Snonce} + \text{AP MAC} + \text{STA MAC})$$

iPSK without RADIUS



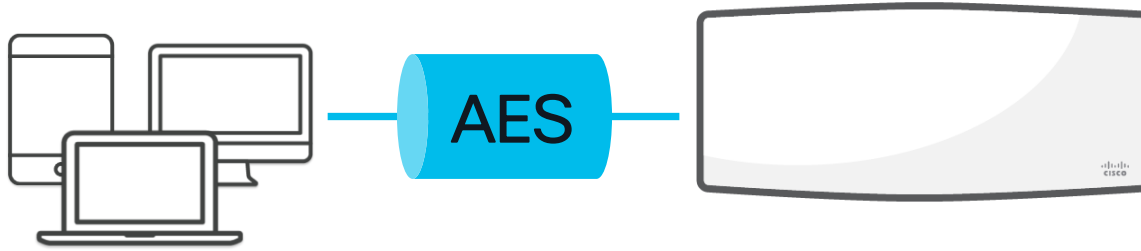
$$PTK = PRF(PSK + Anonce + Snonce + AP\ MAC + STA\ MAC)$$

iPSK without RADIUS



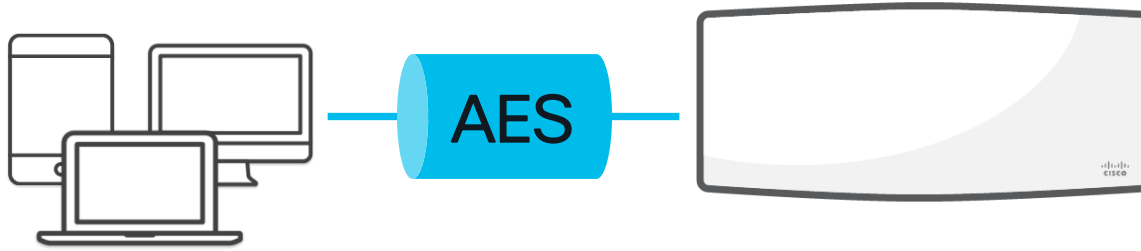
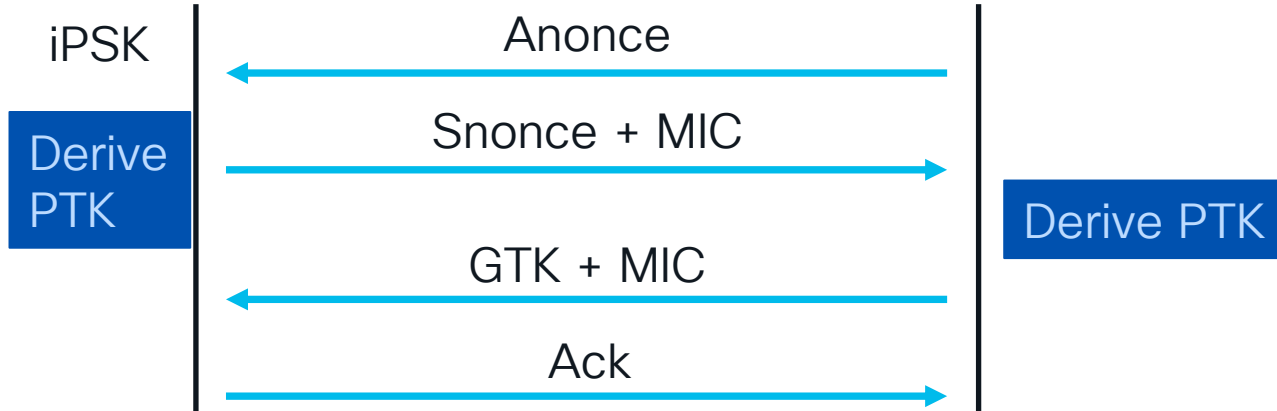
PTK = PRF (PSK + Anonce + Snonce + AP MAC + STA MAC)

iPSK without RADIUS



$$PTK = PRF(PSK + Anonce + Snonce + AP\ MAC + STA\ MAC)$$

iPSK without RADIUS



$PTK = PRF(PSK + Anonce + Snonce + AP\ MAC + STA\ MAC)$

WPA2-PSK Security

$PTK = PRF(PSK + Anonce + Snonce + AP\ MAC + STA\ MAC)$

WPA2-PSK Security

PTK = PRF (PSK + Anonce + Snonce + AP MAC + STA MAC)



THIS IS THE ONLY UNKNOWN

WPA2-PSK Security

Susceptible to Offline Attacks

Rainbow Tables

Dictionary Attacks

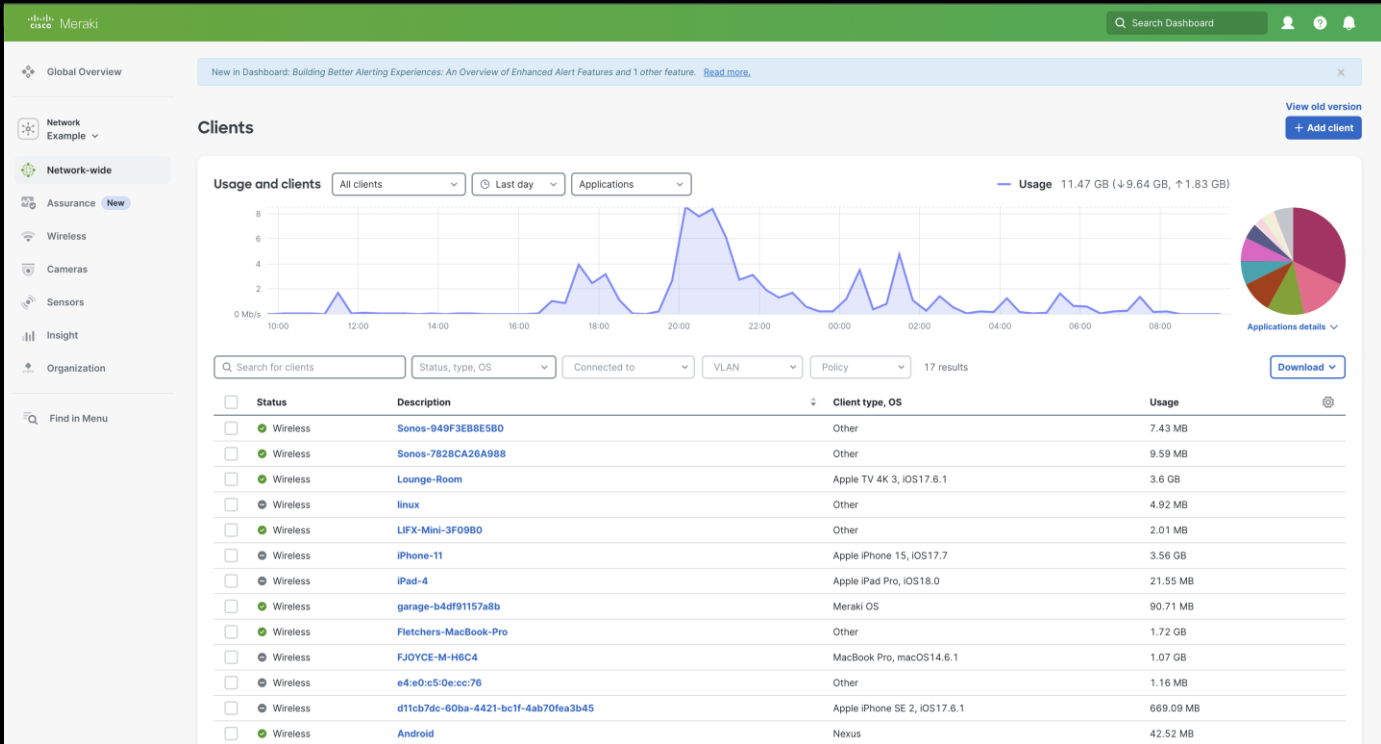
WPA2-PSK Security

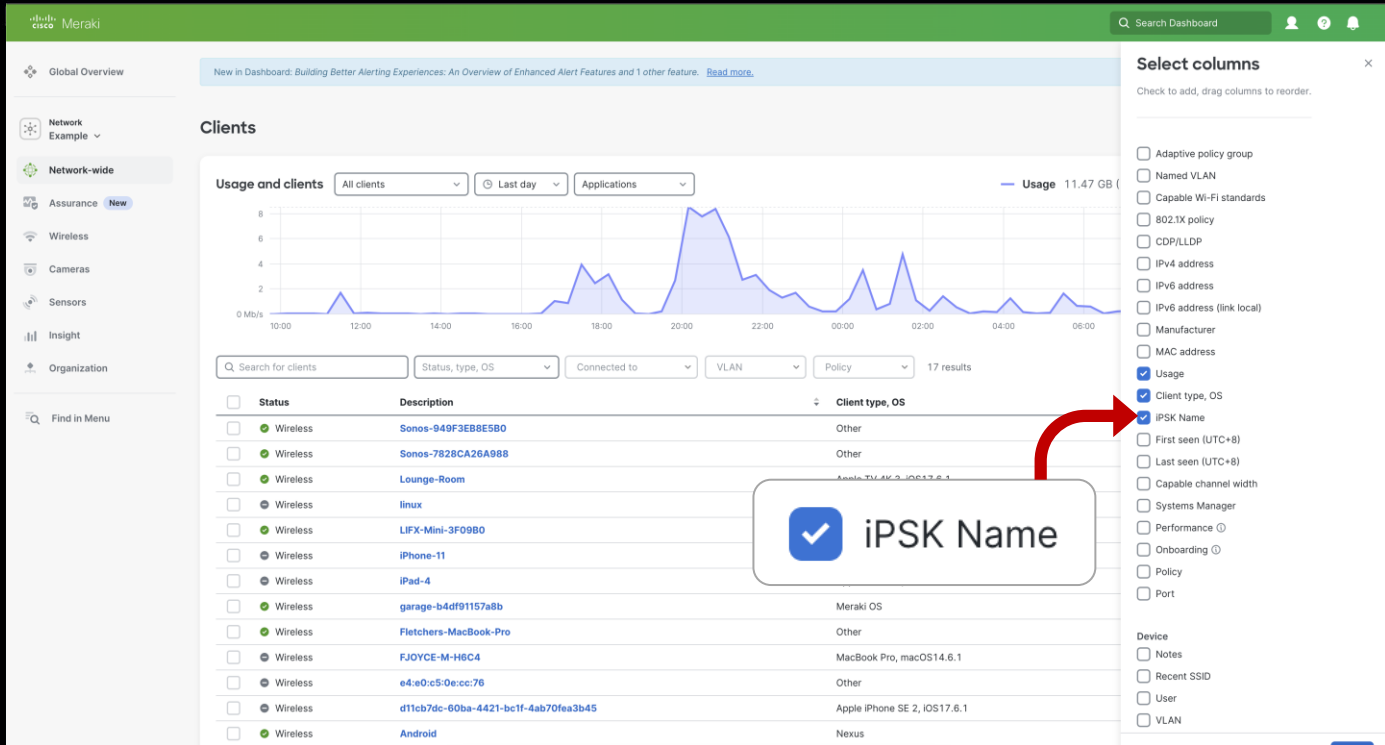
Susceptible to Offline Attacks

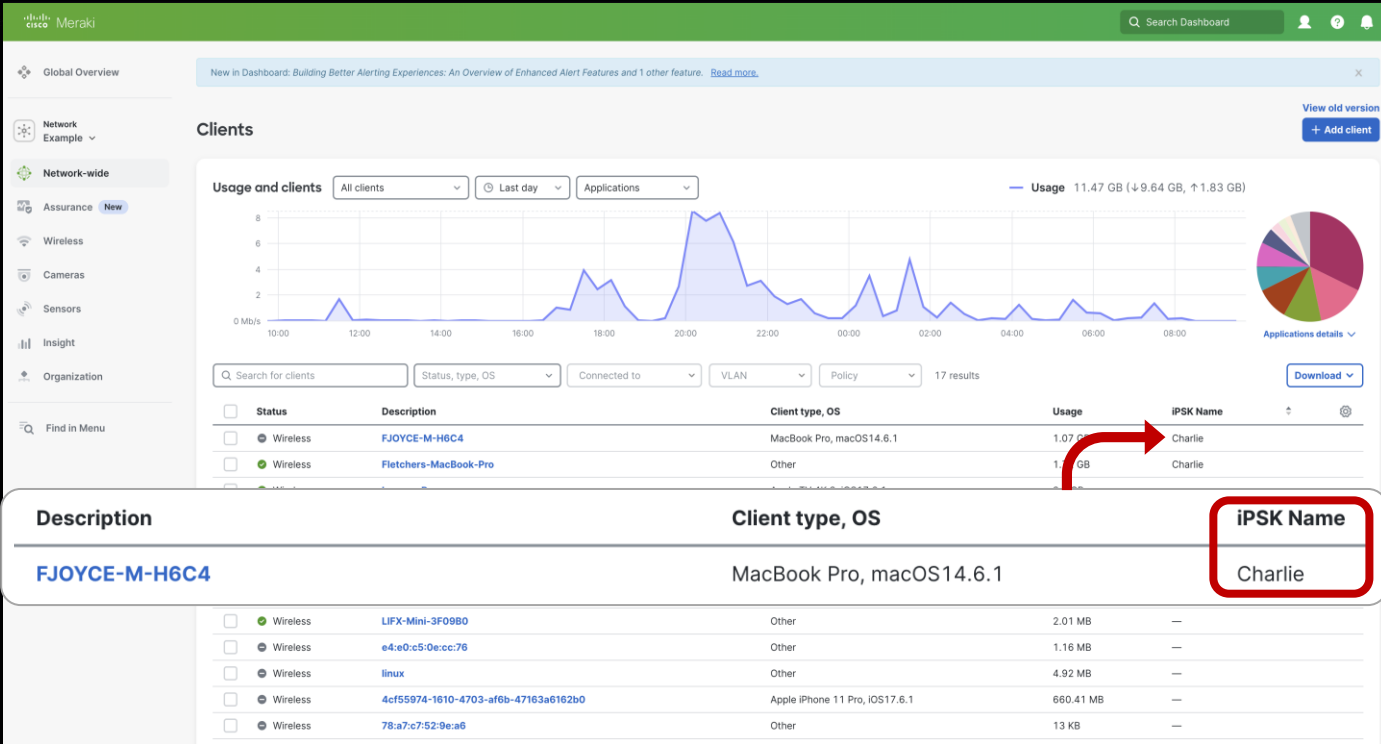
Rainbow Tables

Dictionary Attacks

STRONG SECRETS MATTER







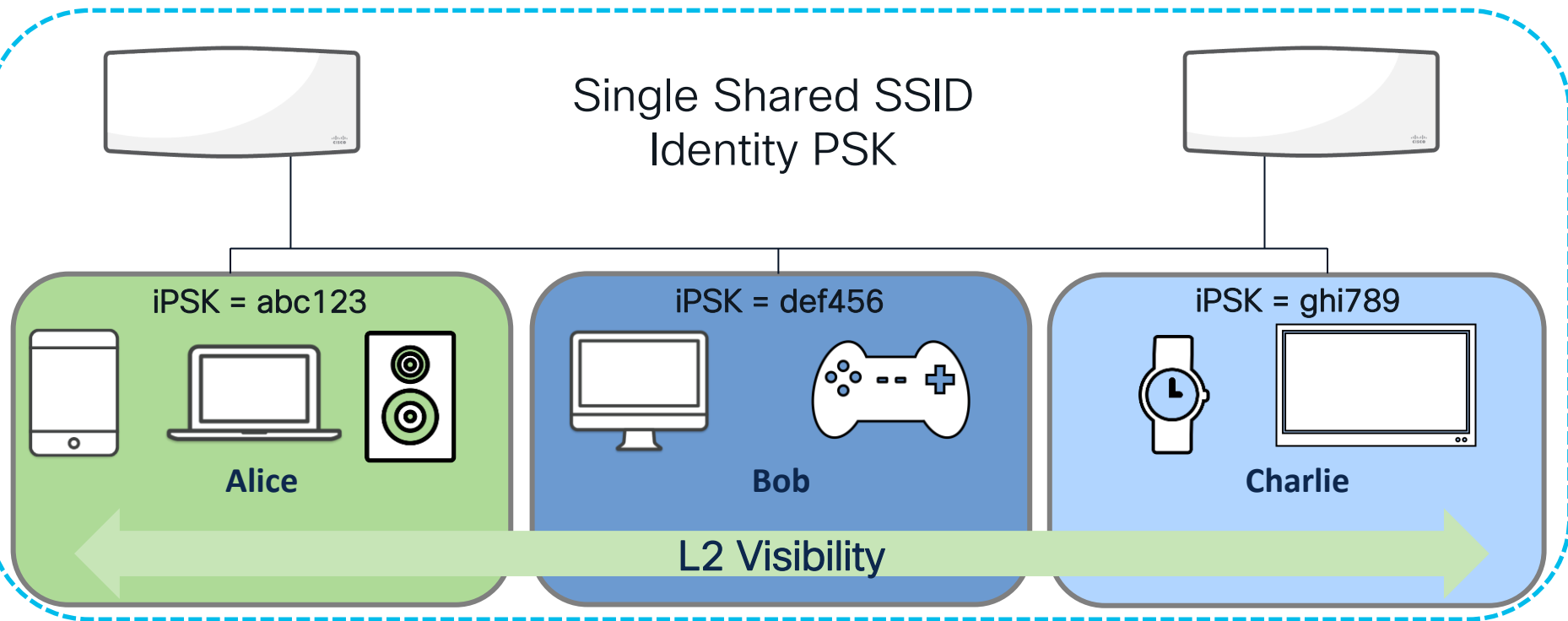
Connect + Secure

iPSK without Radius – Requirements

- MR27.1 to MR29.X
 - Supported only up to 50 iPSK per SSID
- MR30.1
 - Supports up to 5000 iPSK per SSID
- Wi-Fi Wave 2 APs and later
- Bridge Mode – No AP NAT

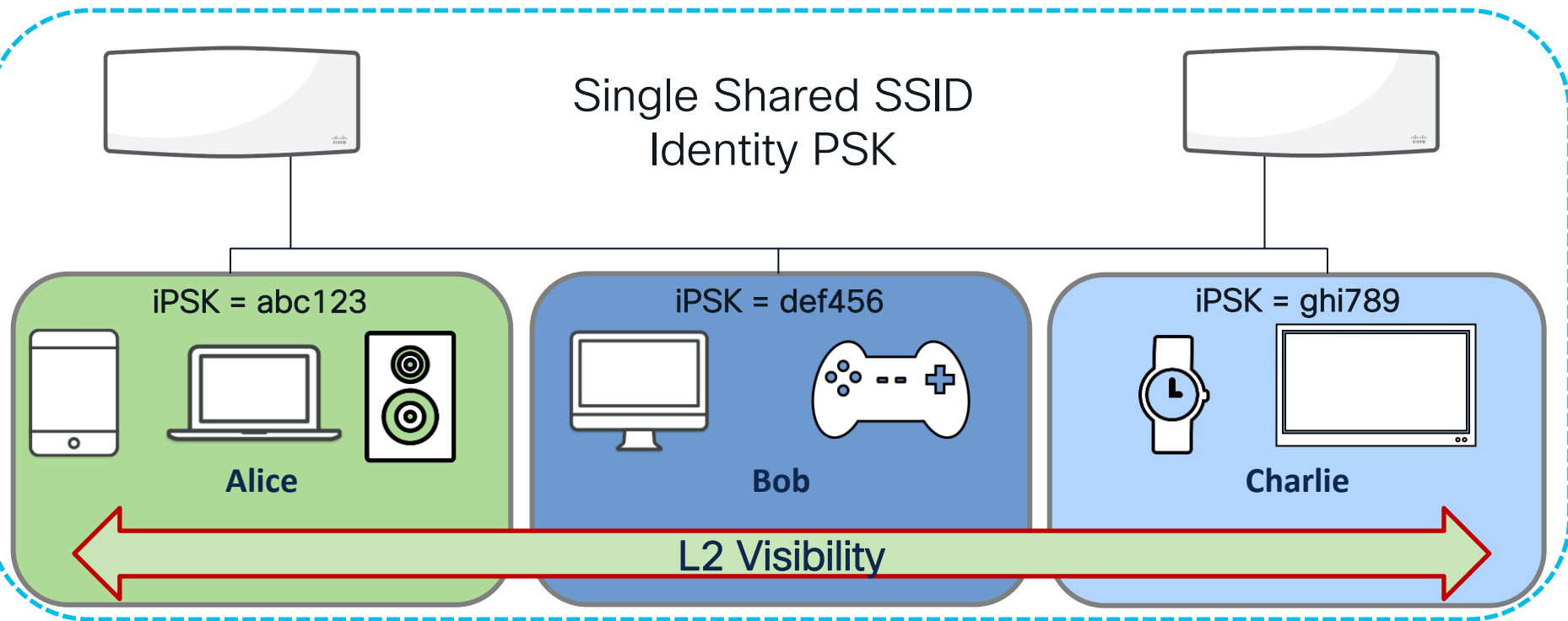
Connect + Secure

Shared SSID – Identity PSK without RADIUS



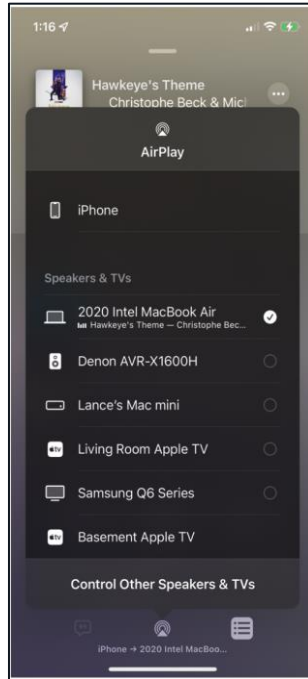
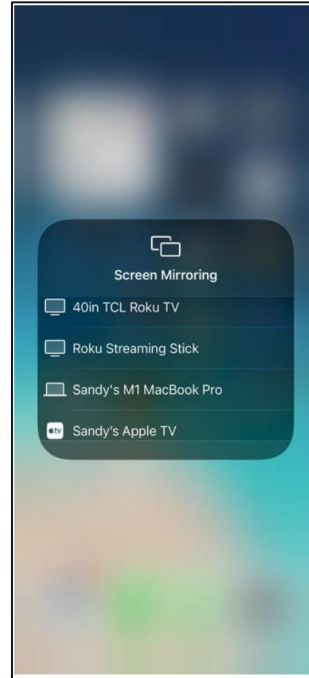
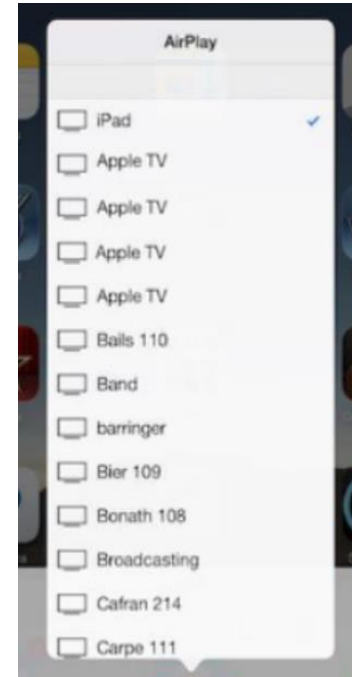
Connect + Secure

Shared SSID – Identity PSK without RADIUS



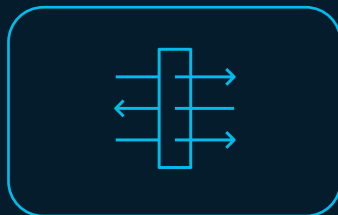
Connect + Secure

Device Discovery and Shared Networks

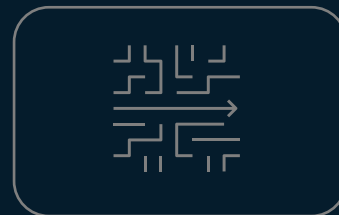




iPSK



WPN



API



SEGMENTING NETWORKS WITH TRADITIONAL METHODS DOESN'T **SCALE** WELL

Segment

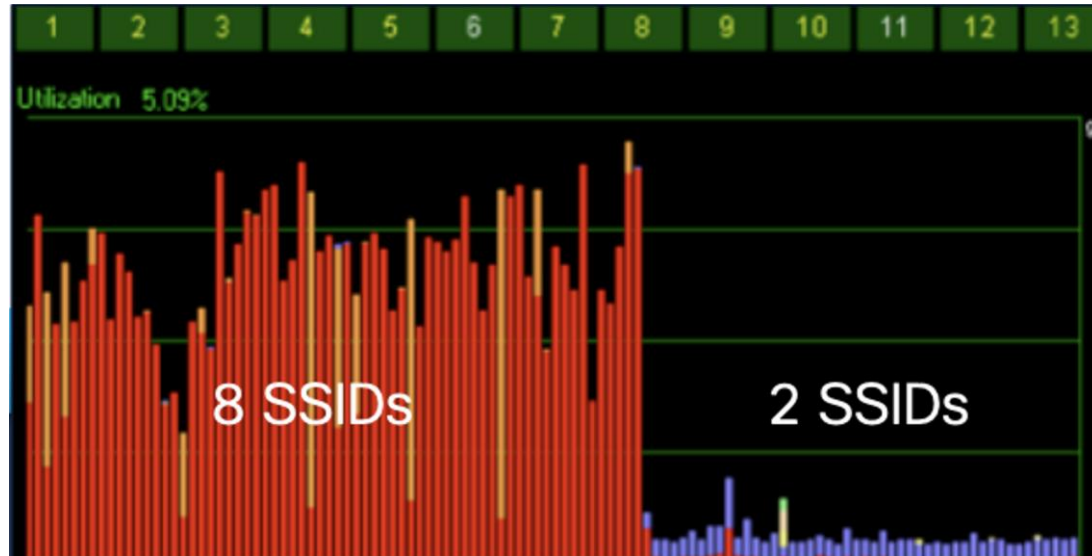
Static SSID to VLAN Assignment

1 SSID : 1 VLAN

Segment

Static SSID to VLAN Assignment

1 SSID : 1 VLAN



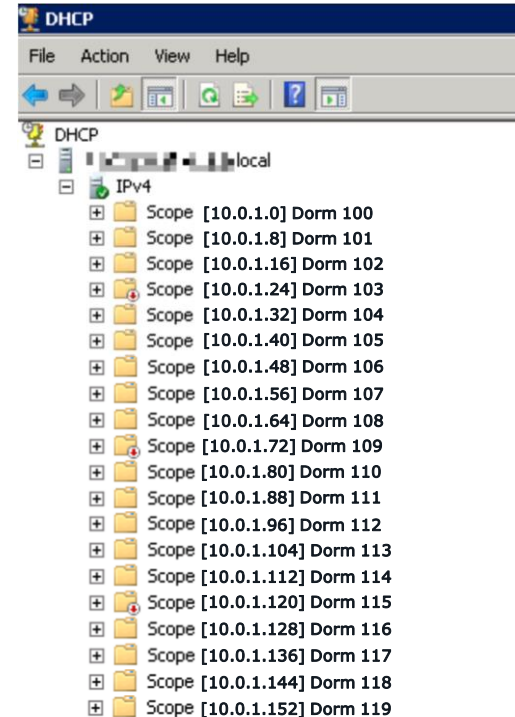
Segment

Dynamic VLAN Assignment

Room Number	VLAN ID	Subnet
Room 100	100	10.0.1.0/29
Room 101	101	10.0.1.8/29
Room 102	102	10.0.1.16/29
Room 103	103	10.0.1.24/29
Room 104	104	10.0.1.32/29
Room 105	105	10.0.1.40/29
Room 106	106	10.0.1.48/29
Room 107	107	10.0.1.56/29
Room 108	108	10.0.1.64/29
Room 109	109	10.0.1.72/29
Room 110	110	10.0.1.80/29
Room 111	111	10.0.1.88/29
Room 112	112	10.0.1.96/29
Room 113	113	10.0.1.104/29
Room 114	114	10.0.1.112/29
Room 115	115	10.0.1.120/29
Room 116	116	10.0.1.128/29
Room 117	117	10.0.1.136/29
Room 118	118	10.0.1.144/29
Room 119	119	10.0.1.152/29

VLANs

Subnets



DHCP
Scopes

Segment

Let's not think about the Firewall Rules

Access
Control
Lists

Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.0/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any
.					
.					
.					
Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.72/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any
.					
.					
.					
Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.152/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any

Segment

Let's not think about the Firewall Rules

Access
Control
Lists

Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.0/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any
.					
.					
.					
Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.72/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any
.					
.					
.					
Policy	Protocol	Source	Src Port	Destination	Dst Port
Deny	Any	10.0.1.152/29	Any	10.0.1.0/24	Any
Permit	Any	Any	Any	Any	Any

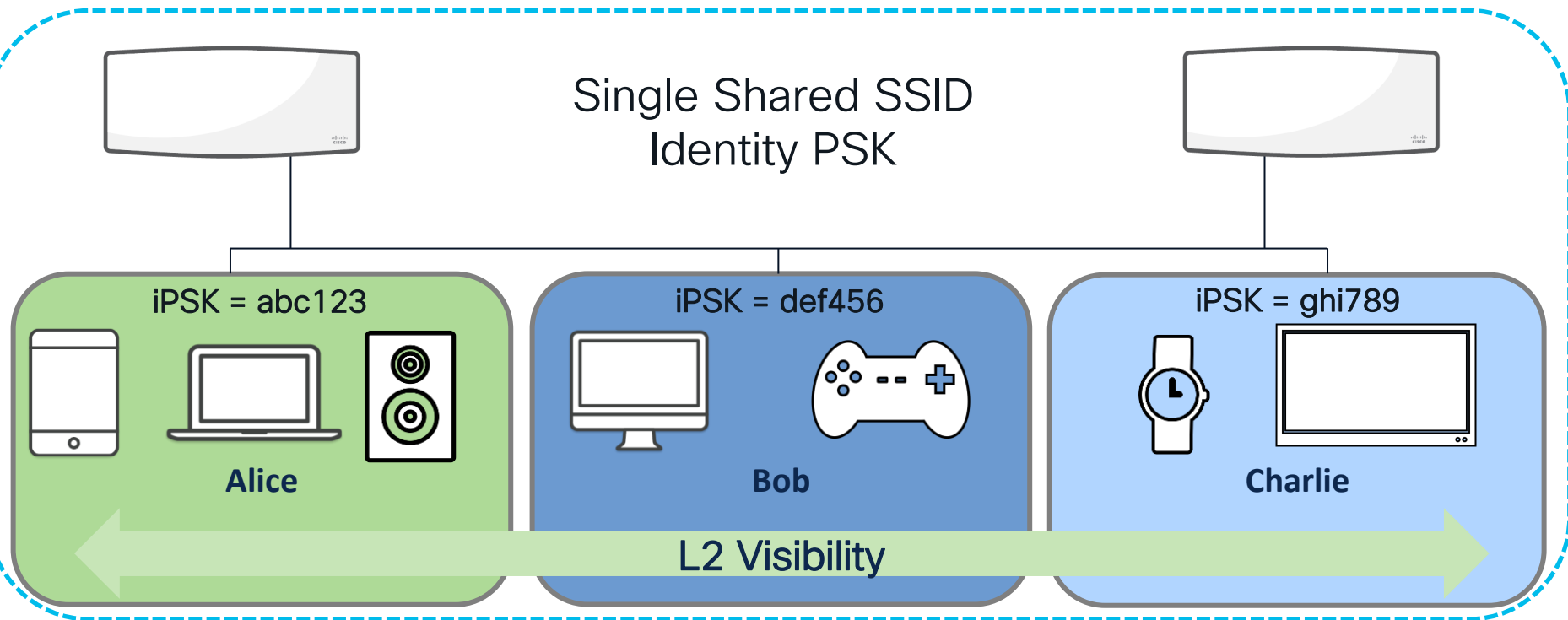


Peer 2 Peer Blocking

L2 Isolation

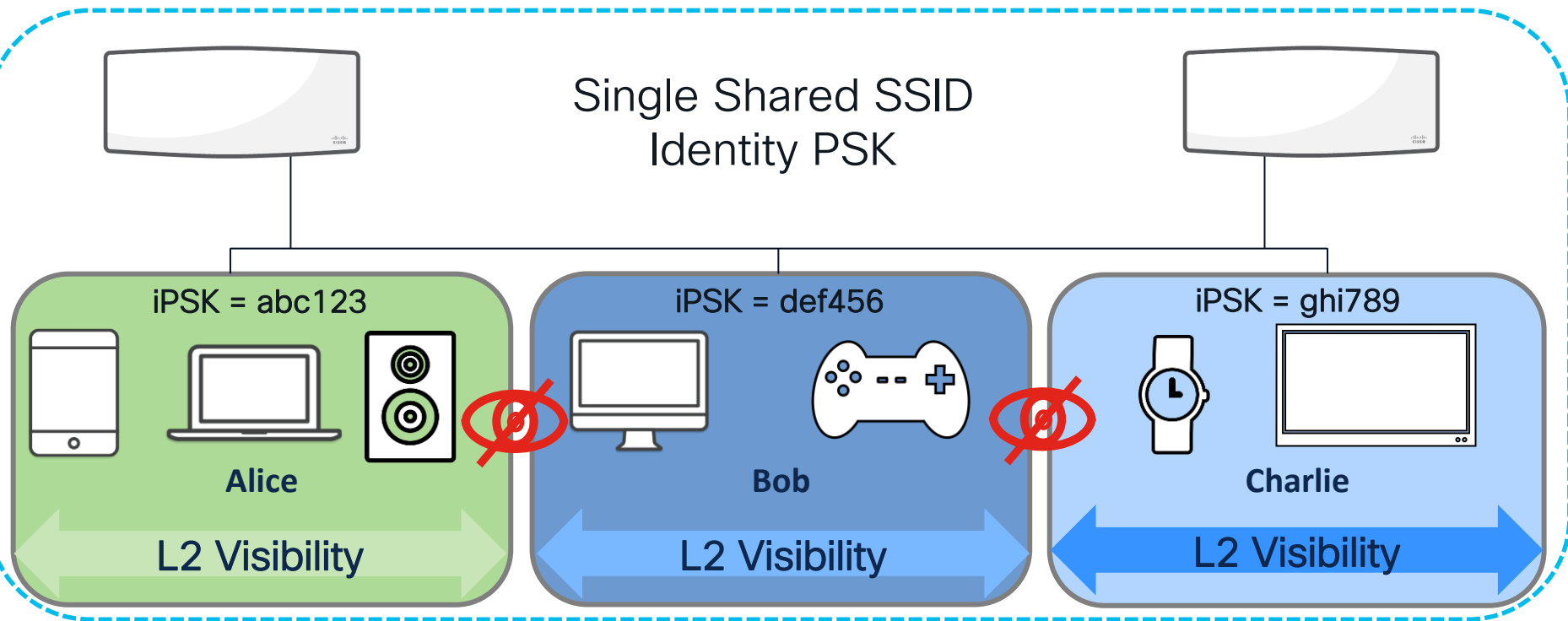
Segment

Shared SSID – Identity PSK without RADIUS



Segment

Shared SSID – Wireless Personal Network (WPN)



Security WPA2 3 Identity PSKs without RADIUS

☒ Identity PSK without RADIUS

Devices are assigned a group policy based on its passphrase

0

Search Identity PSKs...

3 Identity PSKs

Add

Delete

☐	Name ▲	Pre-Shared Key	Group Policy
☐	Alice		Contractor

Wi-Fi Personal Network (WPN) ⓘ

Enabled

Disabled

Wi-Fi Personal Network (WPN) ⓘ

Enabled

Disabled

WPA encryption ⓘ

WPA2 only ▾

802.11w ⓘ

☐ Enabled (allow unsupported clients)

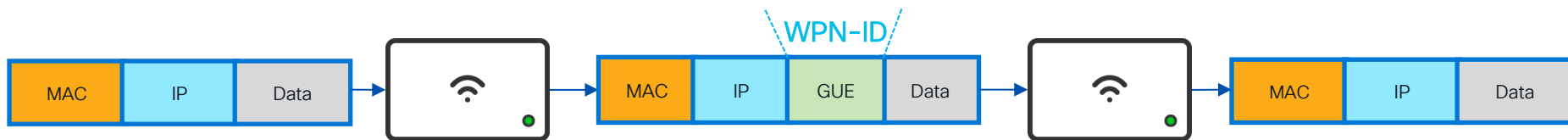
☐ Required (reject unsupported clients)

☒ Disabled (never use)

Segment

How WPN Works

- Generic UDP Encapsulation (GUE)
- Each IPSK has an assigned WPN-ID
- Devices associated with an IPSK assume the WPN-ID during encapsulation



Source AP encapsulates packets not destined for the gateway

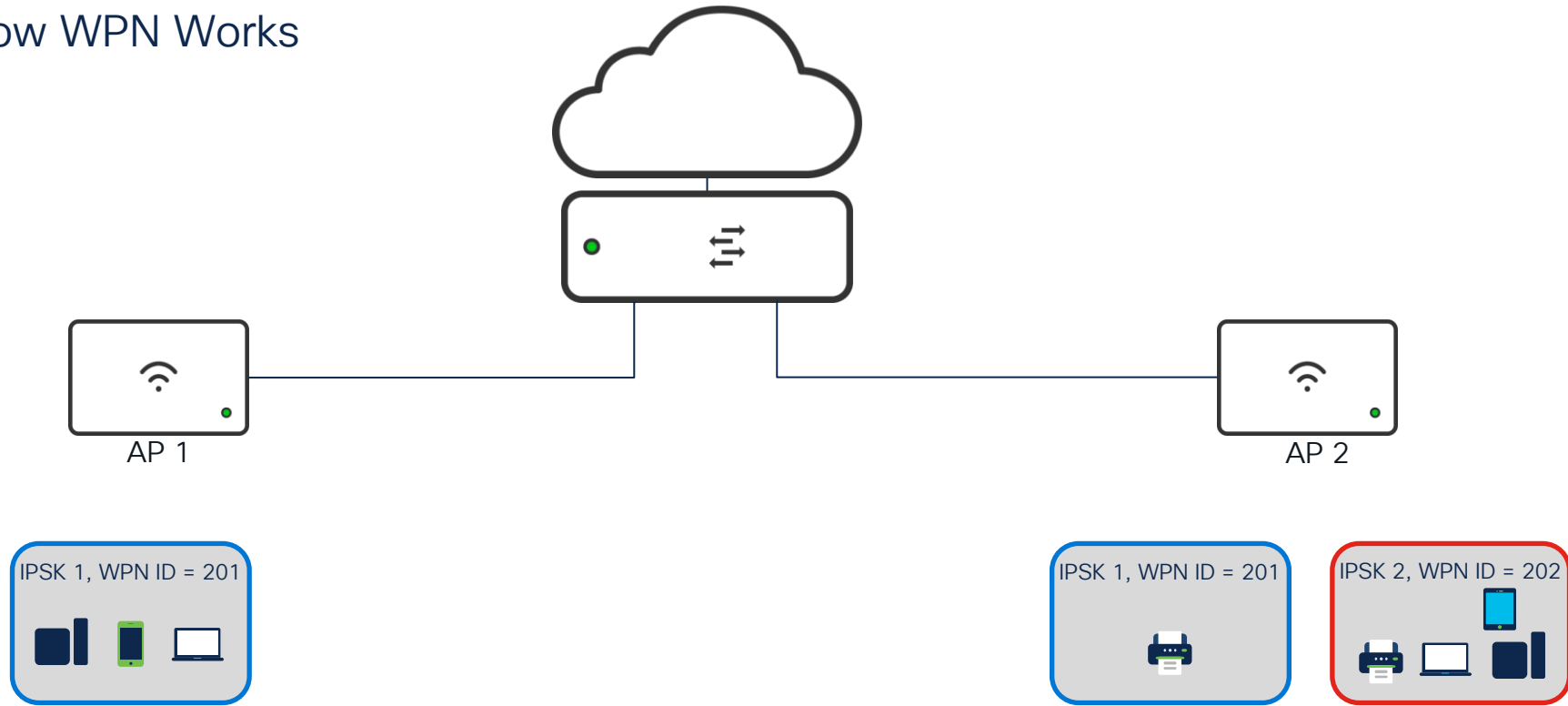


Destination AP strips the GUE header

Packets are forwarded to clients using the same IPSK (WPN-ID)

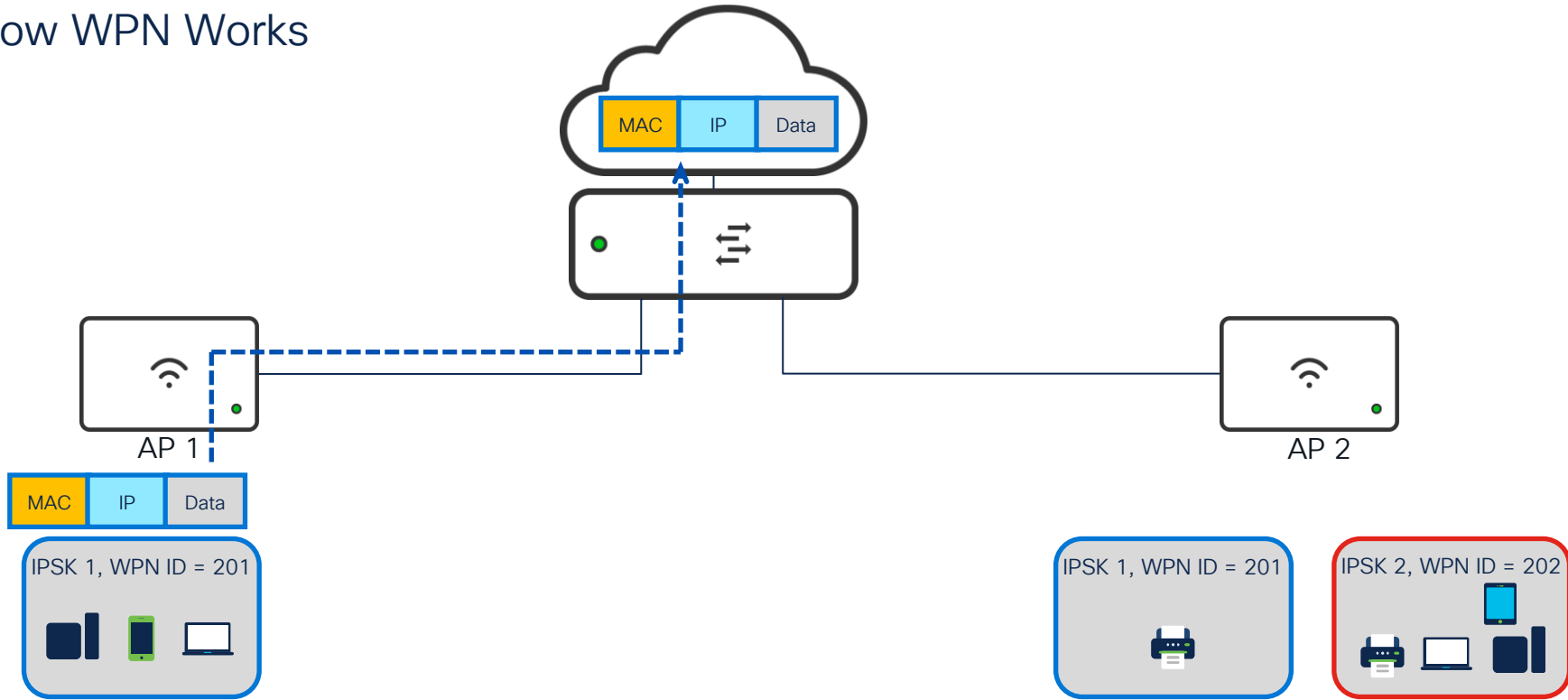
Segment

How WPN Works



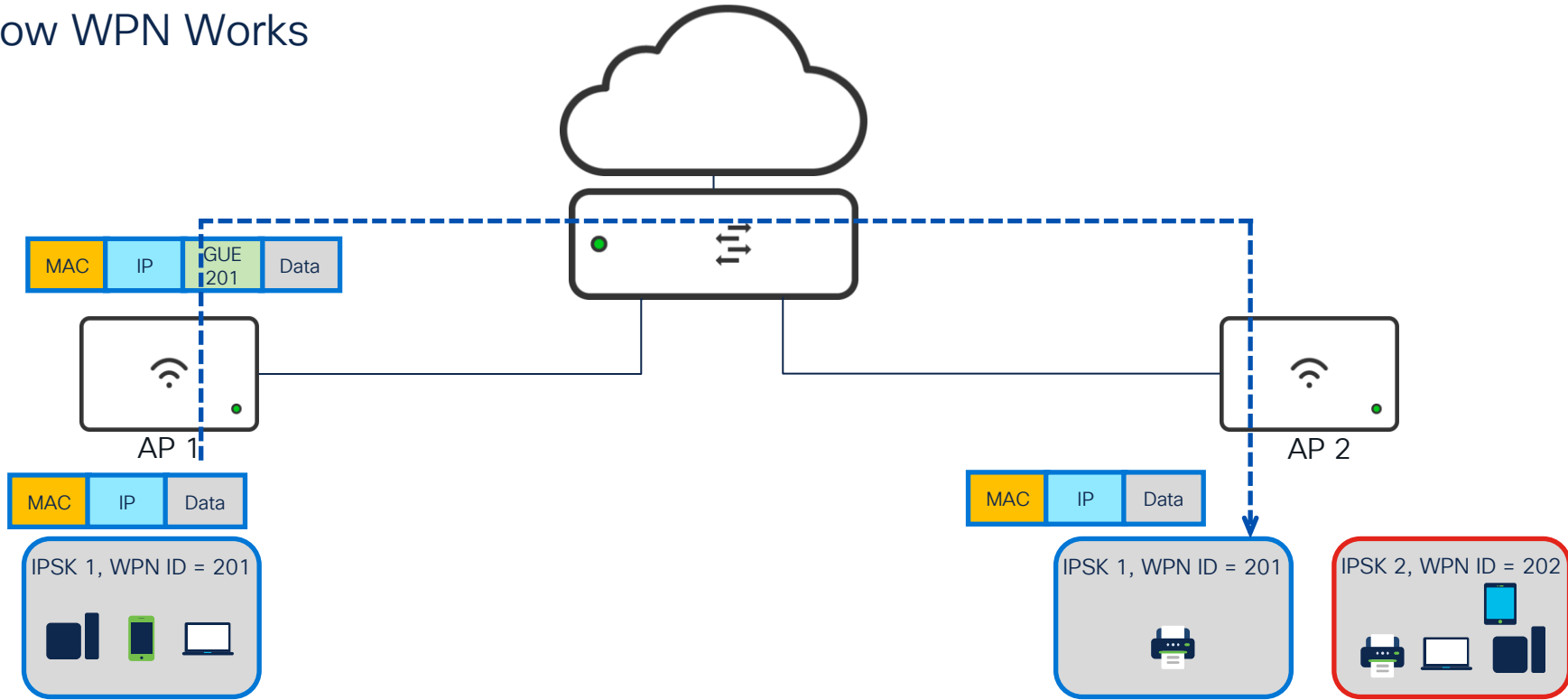
Segment

How WPN Works



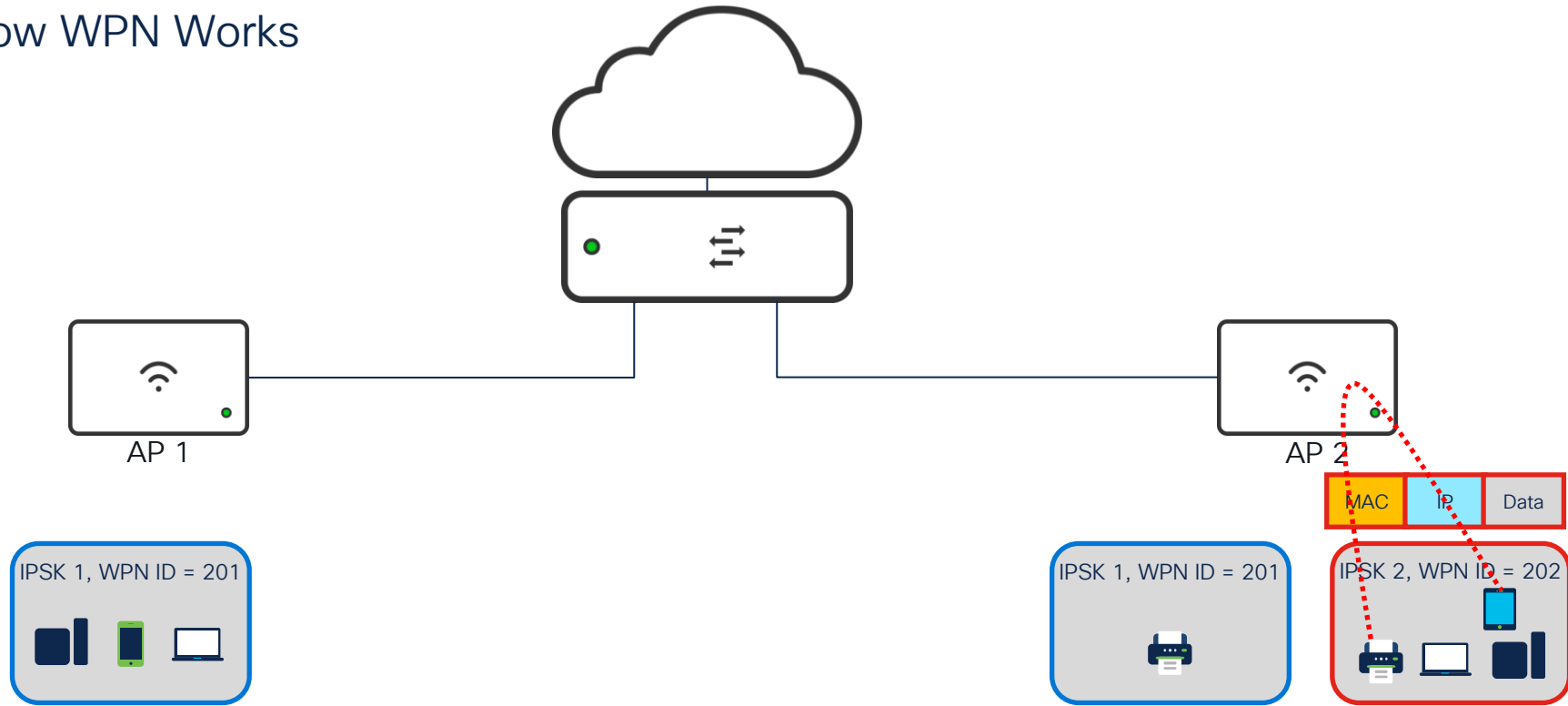
Segment

How WPN Works



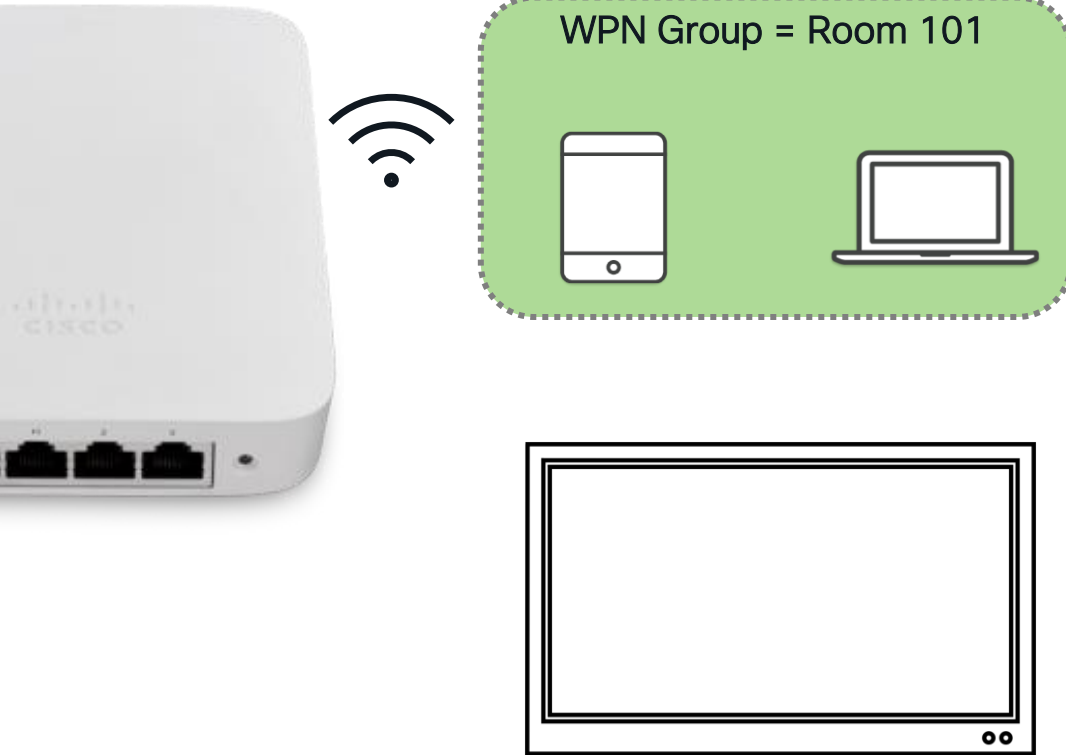
Segment

How WPN Works

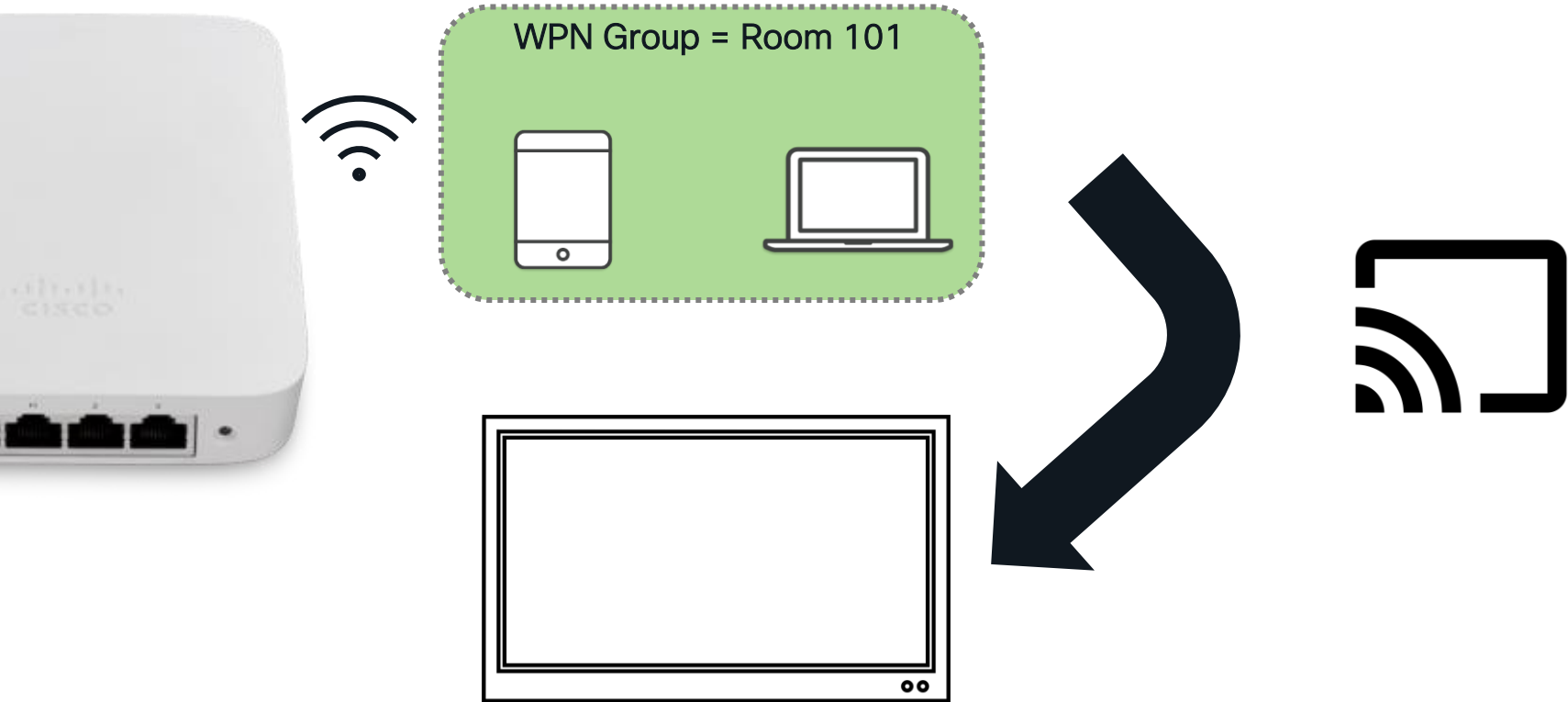


WHAT ABOUT WIRED DEVICES?

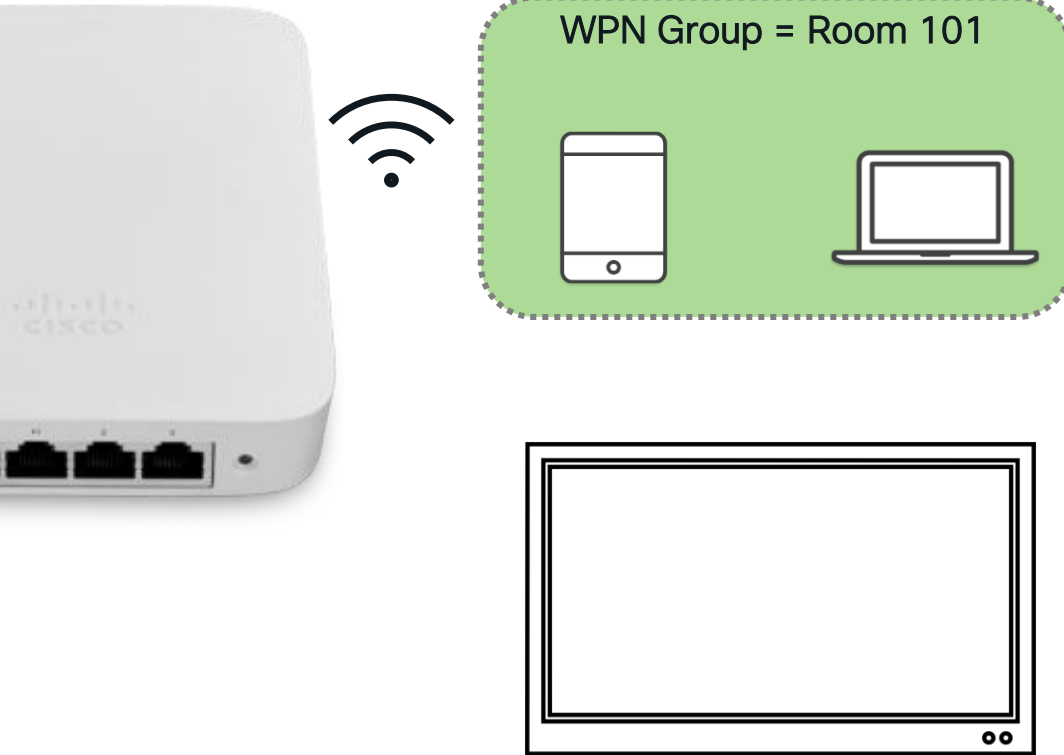
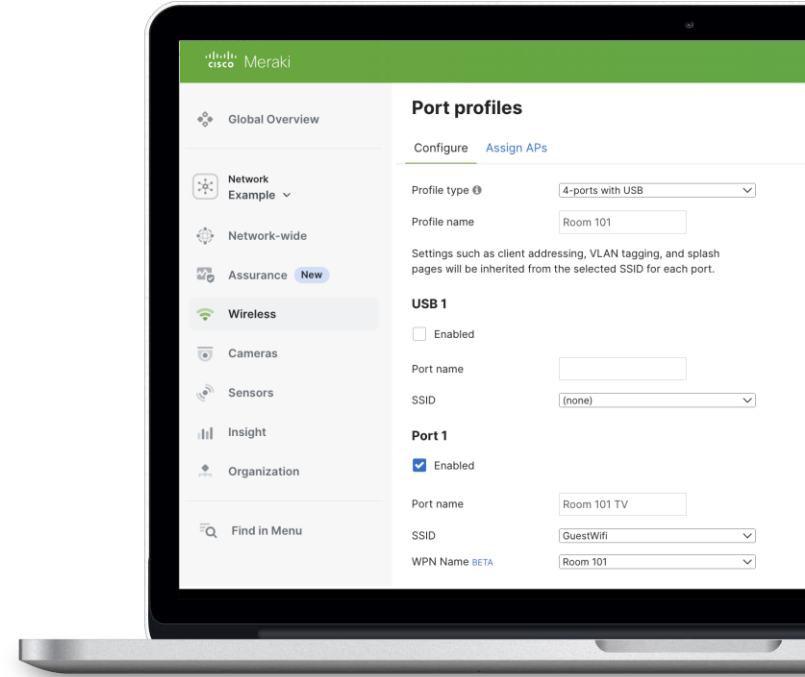
Mapping WPN to Wired Ports



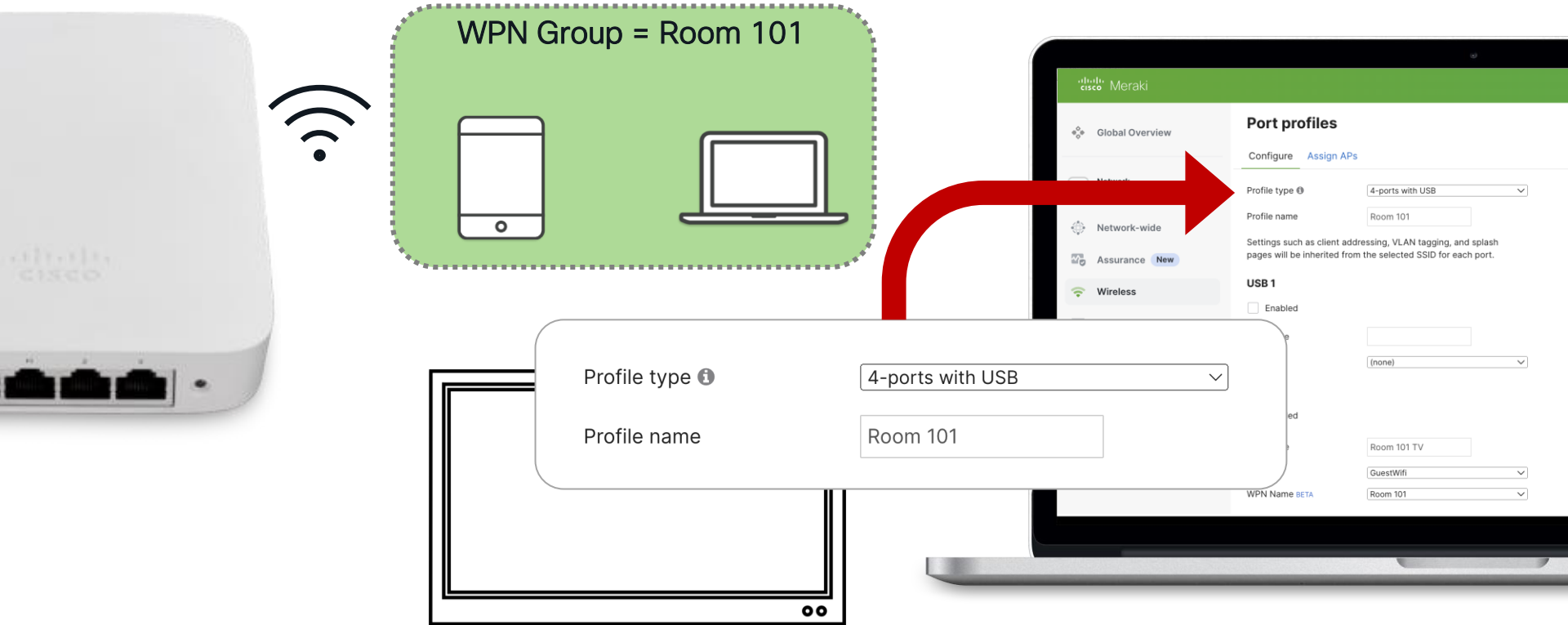
Mapping WPN to Wired Ports



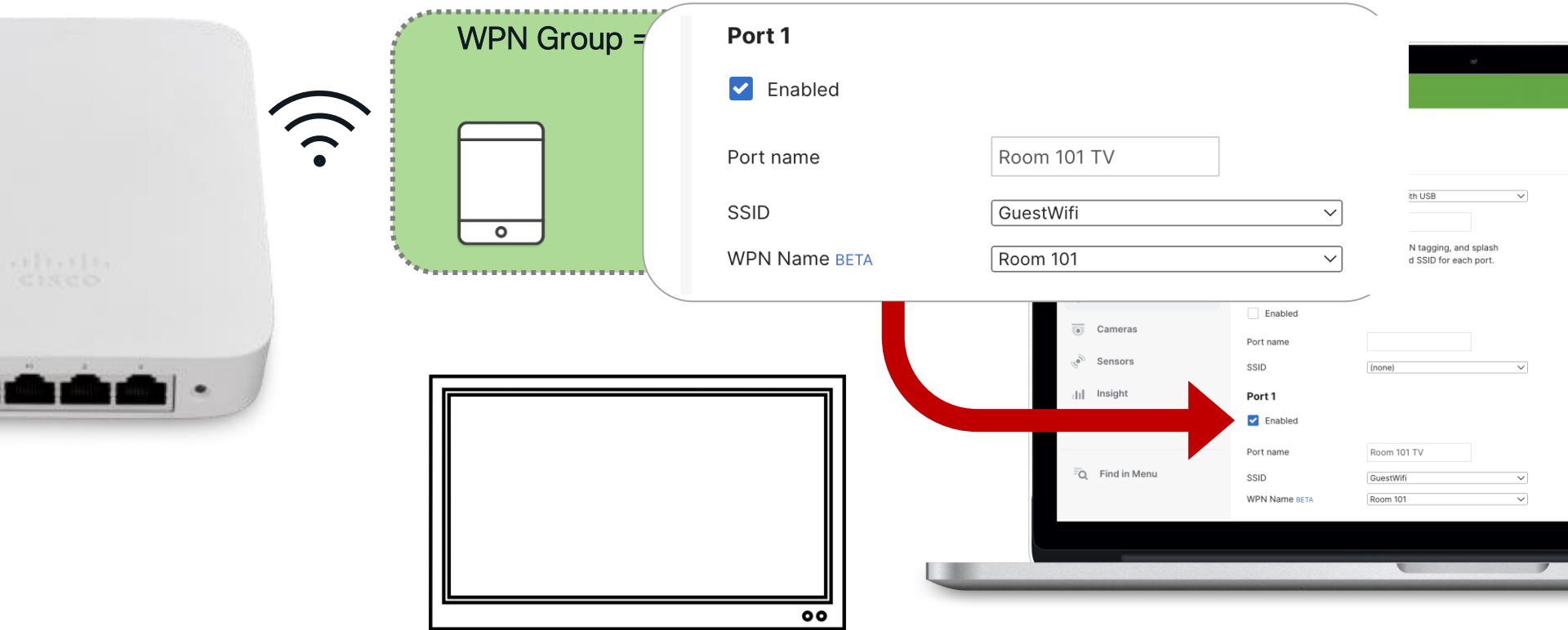
Mapping WPN to Wired Ports



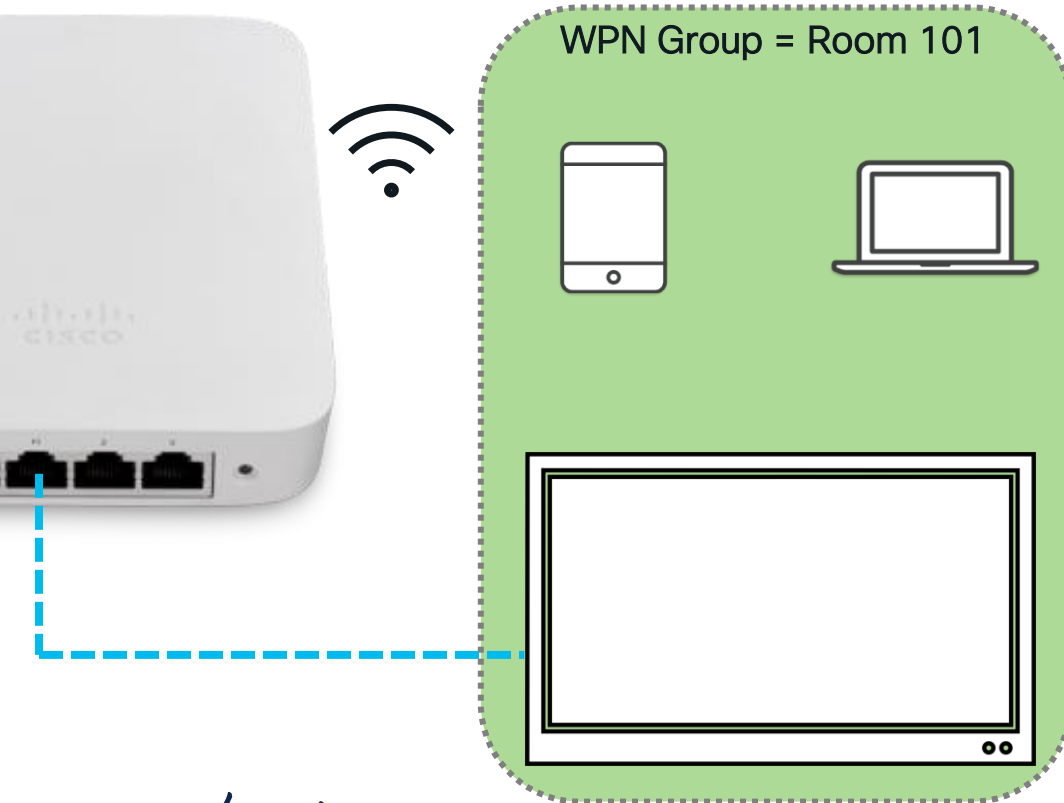
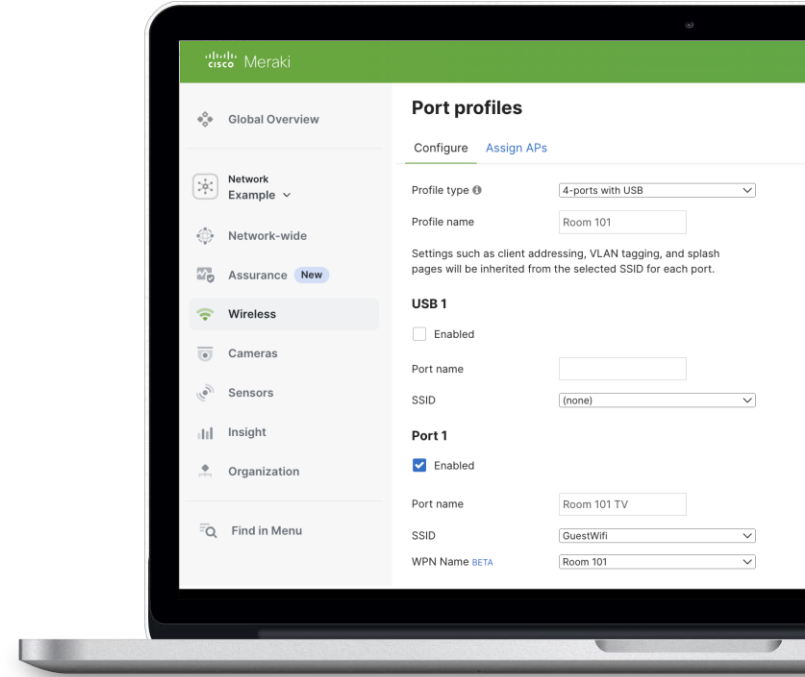
Mapping WPN to Wired Ports



Mapping WPN to Wired Ports



Mapping WPN to Wired Ports



Segment

Wireless Personal Network (WPN) – Requirements

- MR29.1 or Higher
- Wired Support on MR30H and MR36H
- Bridge Mode
- No Support for Tunnelled SSIDs

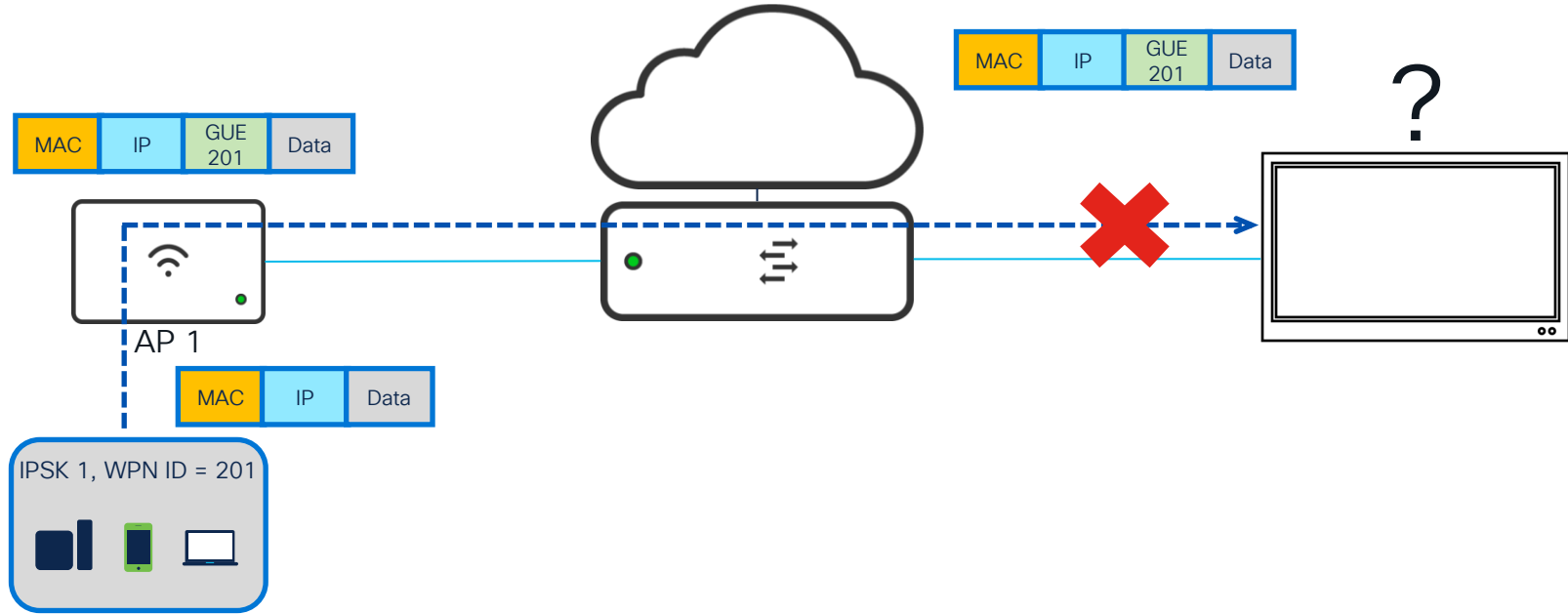
Segment

Wireless Personal Network (WPN) – Caveats

Wireless clients connected to a WPN-enabled SSID **CANNOT** communicate with wired clients on the same VLAN (except the default gateway)

Segment

Wireless Personal Network (WPN) - Caveats



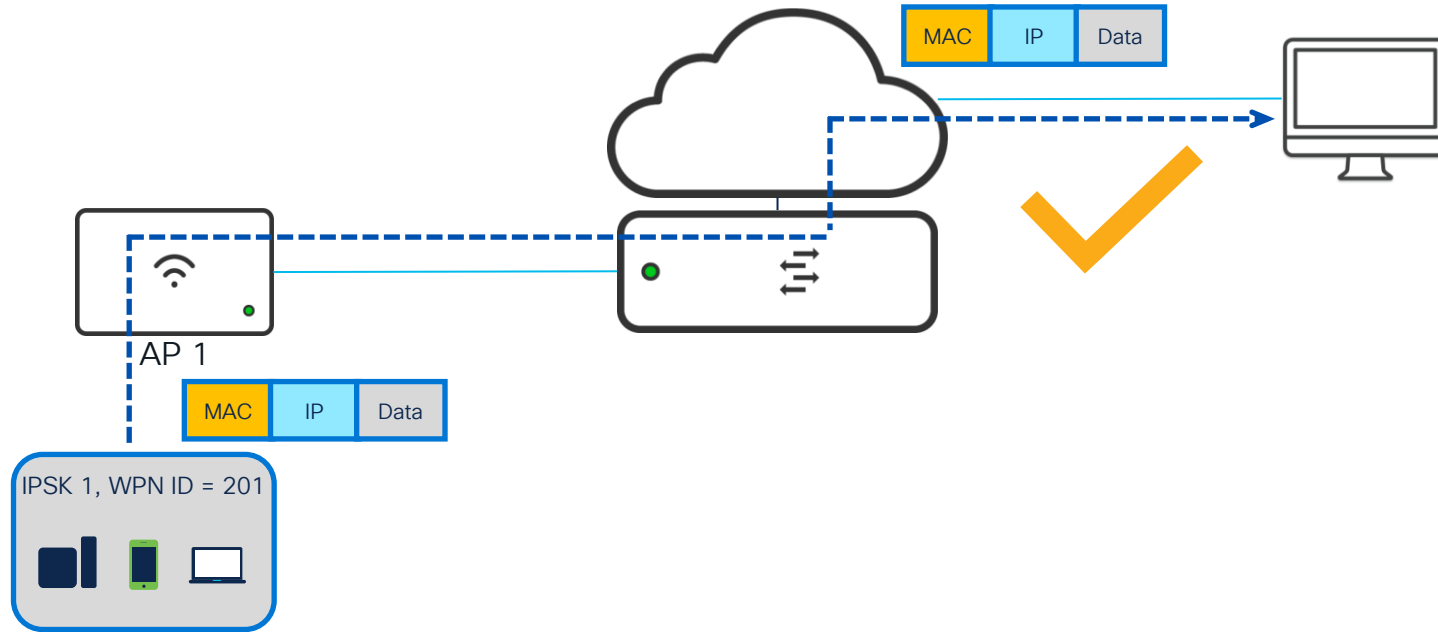
Segment

Wireless Personal Network (WPN) – Caveats

Wireless clients connected to a WPN-enabled SSID **CAN** communicate with any clients on a different VLAN (via L3 Routing)

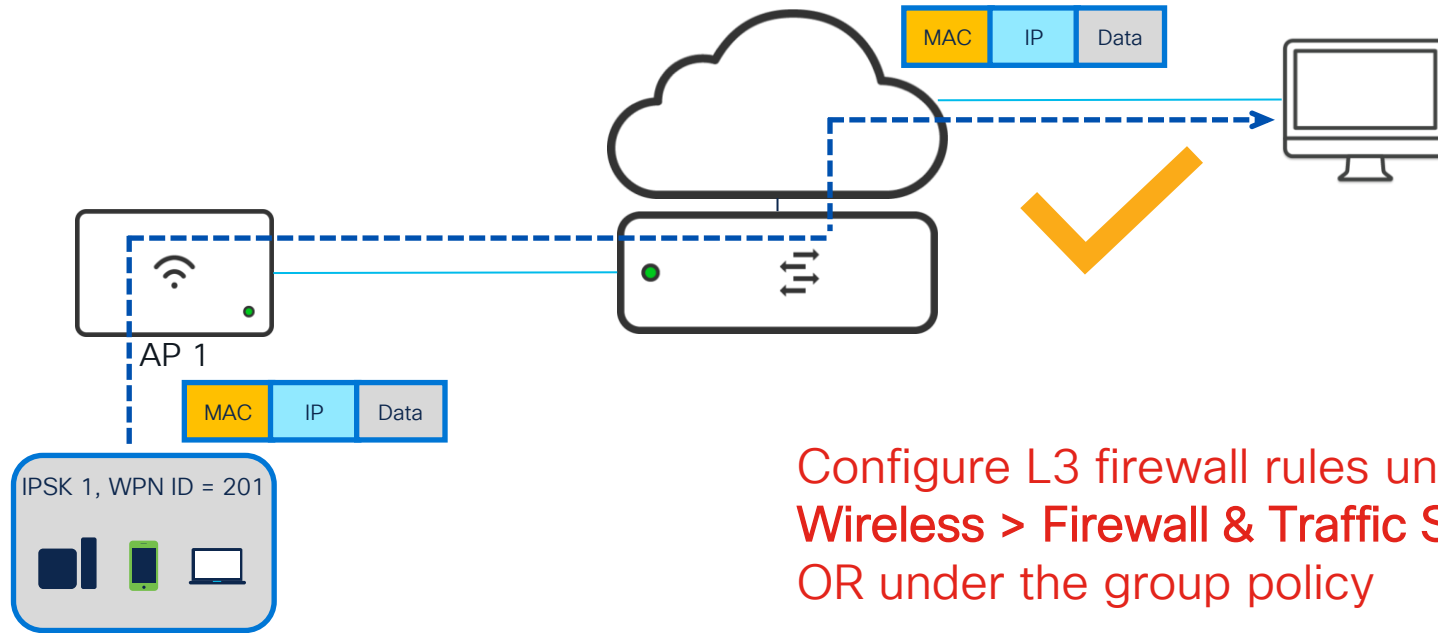
Segment

Wireless Personal Network (WPN) – Caveats



Segment

Wireless Personal Network (WPN) – Caveats



Segment

Wireless Personal Network (WPN) – Caveats

WPN enabled and Non-WPN enabled SSIDs
on the same VLAN **CAN** communicate

Segment

Wireless Personal Network (WPN) – Exempt Traffic

DHCP and DHCPv6

DNS

ARP

NDP and IPv6 NDP

IGMP

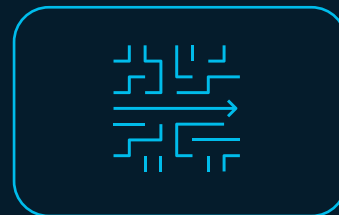
MLD



iPSK



WPN



API

WHAT IS THE DASHBOARD API?

Simplify

The Meraki Dashboard API

Update Network

Operation ID: updateNetwork

Description: Update a network

PUT /networks/{networkId}

Request Parameters

Path

networkId * | String

Body

updateNetwork | Object

Schema Definition

Example Body

```
{
  "name": "Long Island Office",
  "timeZone": "America/Los_Angeles",
  "tags": [ "tag1", "tag2" ]
}
```



<http://developer.cisco.com/meraki>

<https://developer.cisco.com/meraki/api-v1/>



<https://github.com/meraki>

<https://github.com/meraki/dashboard-api-python/>





“Is Charlie allowed
access to this
site?”



Access Control System



“Yes, and Charlie
is a **contractor**”



Access Control System

“I’d like to allocate
Charlie to a room”



Property Management System



“Charlie is
allocated and
checked-in to
Room 101”



Access Control System

Property Management System

“Create an iPSK
for Charlie”



“Success,
Charlie’s WPN id is
1284392014819”



POST

/networks/{networkId}/wireless/ssids/{number}/identityPsk

```
{  
  "name": "Charlie",  
  "passphrase": "x6azprQ17156",  
  "groupPolicyId": "115",  
  "expiresAt": "2018-02-11T00:00:00.090210Z"  
}
```

← Guest Identifier

← iPSK for Charlie

← Contractor Group Policy ID

← Key Expiry

<https://developer.cisco.com/meraki/api-v1/create-network-wireless-ssid-identity-psk/>



“Update Room
101 Port Profile for
Charlie’s WPN”



“Success”

Access Control System

Property Management System



PUT

Room 101 Port Profile id



```
/networks/{networkId}/wireless/ethernet/ports/profiles/{profileId}
```

```
{  
  "ports": [  
    {  
      "name": "Room 101",  
      "number": 1,  
      "ssid": 1,  
      "pskGroupId": "1284392014819"  
    }  
  ]  
}
```

AP Port Name

AP Port Number

Guest Wi-Fi SSID id

Charlie's WPN id

<https://developer.cisco.com/meraki/api-v1/update-network-wireless-ethernet-ports-profile/>



WHAT IF I WANT SOMETHING OFF THE SHELF?

The Meraki Marketplace



260+

Meraki Marketplace apps



100+

Ecosystem tech partners



50+

Business solutions and network management solutions categories



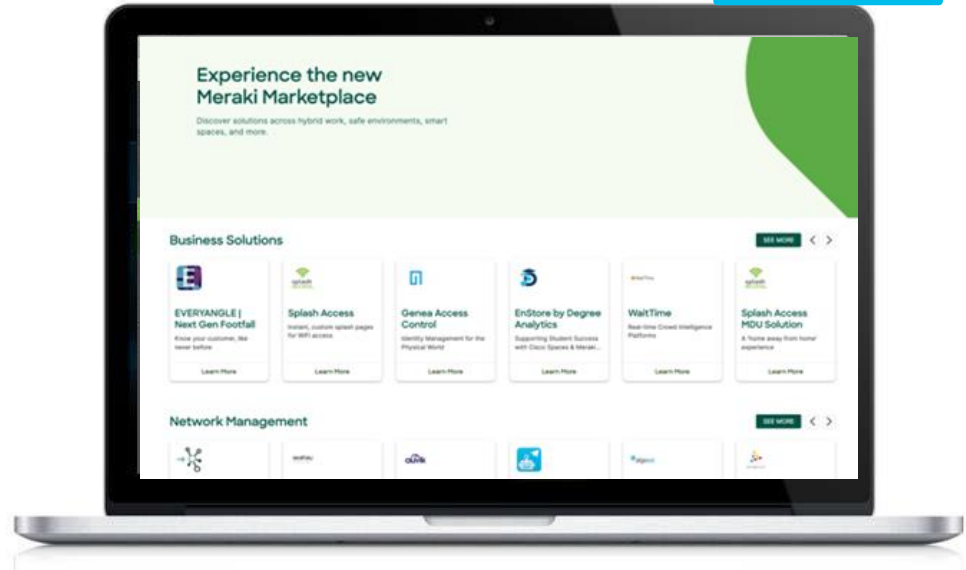
1,000+

Use cases



250+

Published customer wins



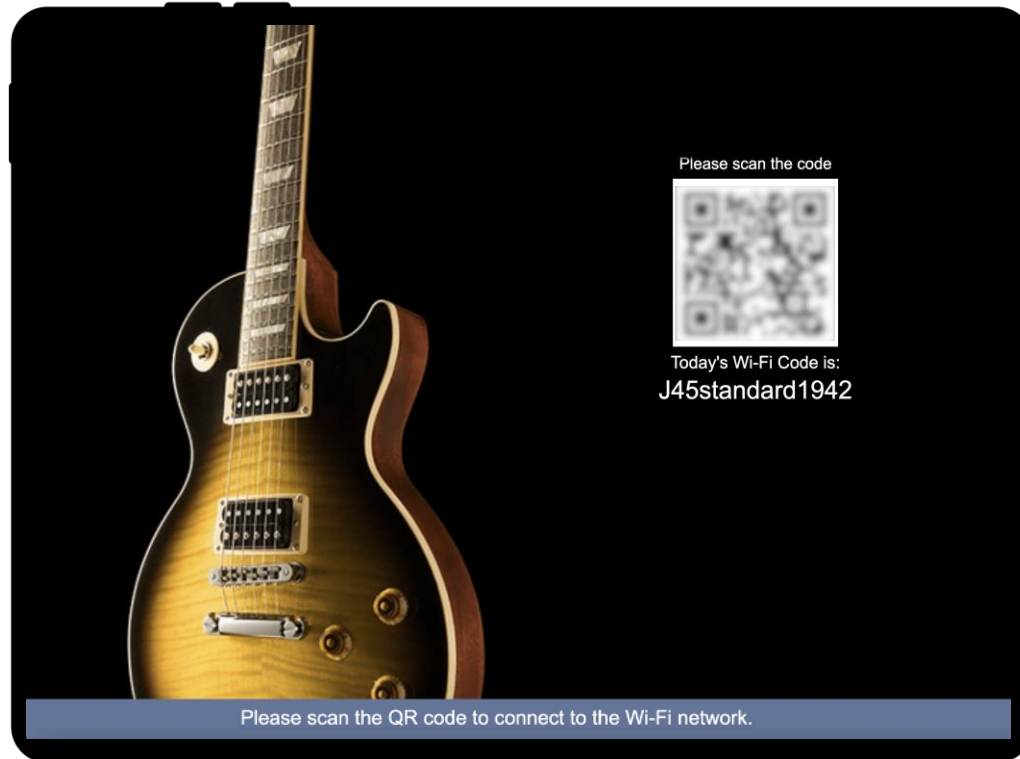
<https://apps.meraki.io/>

Splash Access

The login screen for Splash Access Visitor Manager is overlaid on a background image of three smiling people. The screen has a light gray header with the "splashaccess." logo and the title "Visitor Manager". Below the title is the instruction "Please enter your details below". There are four input fields: "Email Address *" and "Phone Number *" in the top row, and "First Name *" and "Last Name *" in the bottom row. A large green button labeled "Create WPA2" is centered below the fields. At the bottom left, there is a checked checkbox next to the text "I agree to the T&C's". At the bottom right, there are three links: "Your Info", "Our Terms", and "Privacy".

Splash Access

Rotating iPSK QR Code



Splash Access

User Self-Service

Identity PSK + WPN

☒ Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase

WiFi Personal Network (WPN)  Enabled Disabled

Using WPN will invalidate your [layer 2 isolation settings](#).

3 Identity PSKs Add Delete

☐ Name ▲	Pre-Shared Key	Group Policy
☐ Dorm 103	<input type="password" value="....."/> 	Dorm-103-WPN-GP
☐ Dorm 102	<input type="password" value="....."/> 	Dorm-102-WPN-GP
☐ Dorm 101	<input type="password" value="....."/> 	Dorm-101-WPN-GP

◀ {API} ▶



splashaccess.
Register your Details
Please complete the form below.

.....
.....

☒ I agree to the Terms and Conditions.
☐ Yes, I would like to receive news and offers via email.

Register

< Back

[Your Info](#) | [Terms & Conditions](#) | [Privacy Policy](#)

WPA2/Guest Registration Portal

Welcome, you can manage your Guest Code(s) and generate a WPA2 password below.
Account: Tim@splashaccess.co.uk

Generate a WPA2 password.

WPA2 Password

chjGa49vynfmVs



Copy WPA2 Password

Generate Password

Print

Scan the QR code to securely onboard your devices.



MT Sensor Information



CO2	TVOC	Humidity	Noise	Temperature	Air Quality
859ppm Fair	38µg/m³ Excellent	58% Excellent	62dBA Good	68.3°F 20.17°C	100/100 Excellent

WPA2/Guest Registration Portal

Welcome, you can manage your Guest Code(s) and generate a WPA2 password below.
Account: Tim@splashaccess.co.uk

Generate a WPA2 password.

WPA2 Password

chjGa49vynfmVs



Copy WPA2 Password

Generate Password

Print

Scan the QR code to securely onboard your devices.

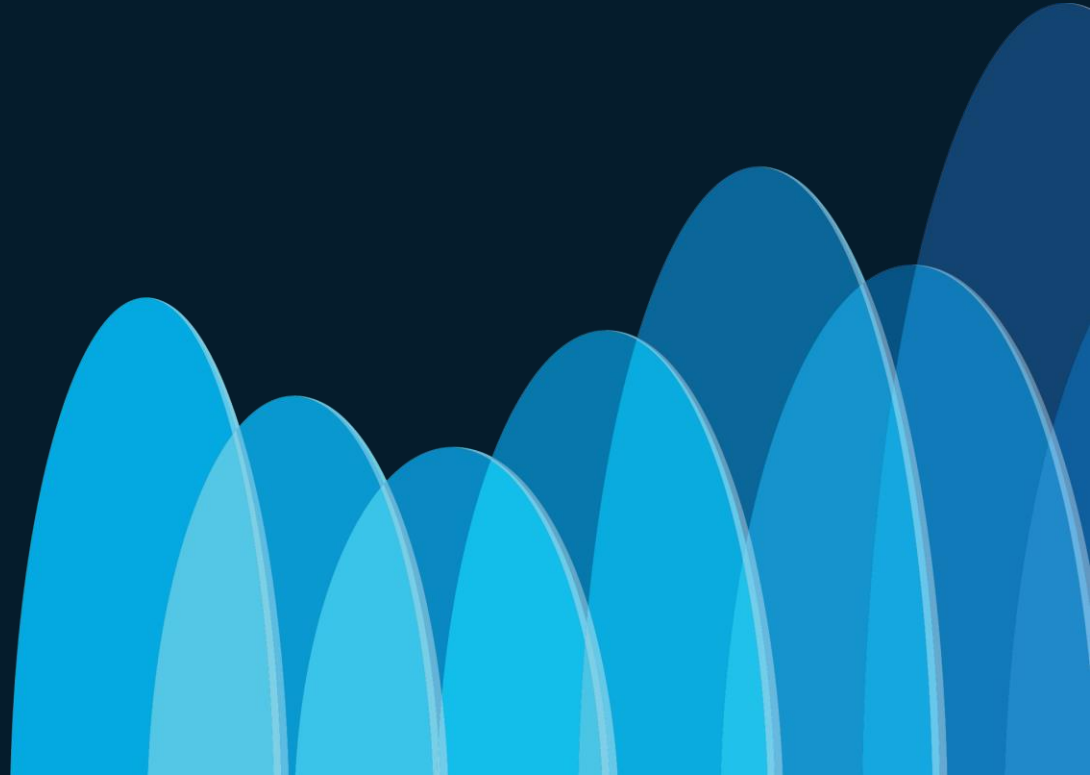


MT Sensor Information



CO2	TVOC	Humidity	Noise	Temperature	Air Quality
859ppm Fair	38µg/m³ Excellent	58% Excellent	62dBA Good	68.3°F 20.17°C	100/100 Excellent

Physical Guest Experience



Meraki IoT

INFRASTRUCTURE MONITORING

MT10

Temperature and humidity



MT12

Water leaks



MT20

Door open/close



POWER

MT40

Smart power controller



INDOOR AIR QUALITY

MT14

Indoor air quality



MT15

Indoor air quality + CO2



COLD STORAGE

MT11

Temperature probe



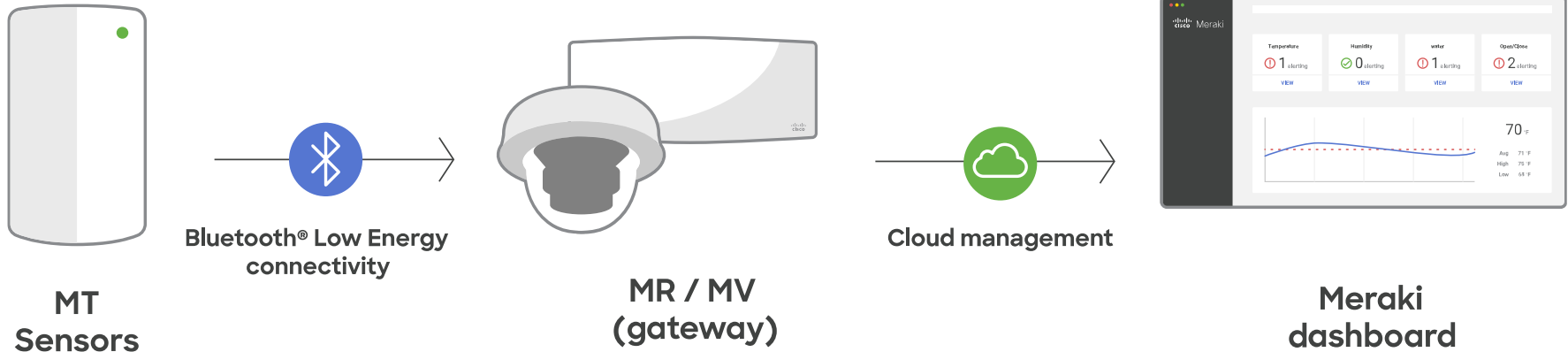
AUTOMATION

MT30

Automation button



Meraki IoT

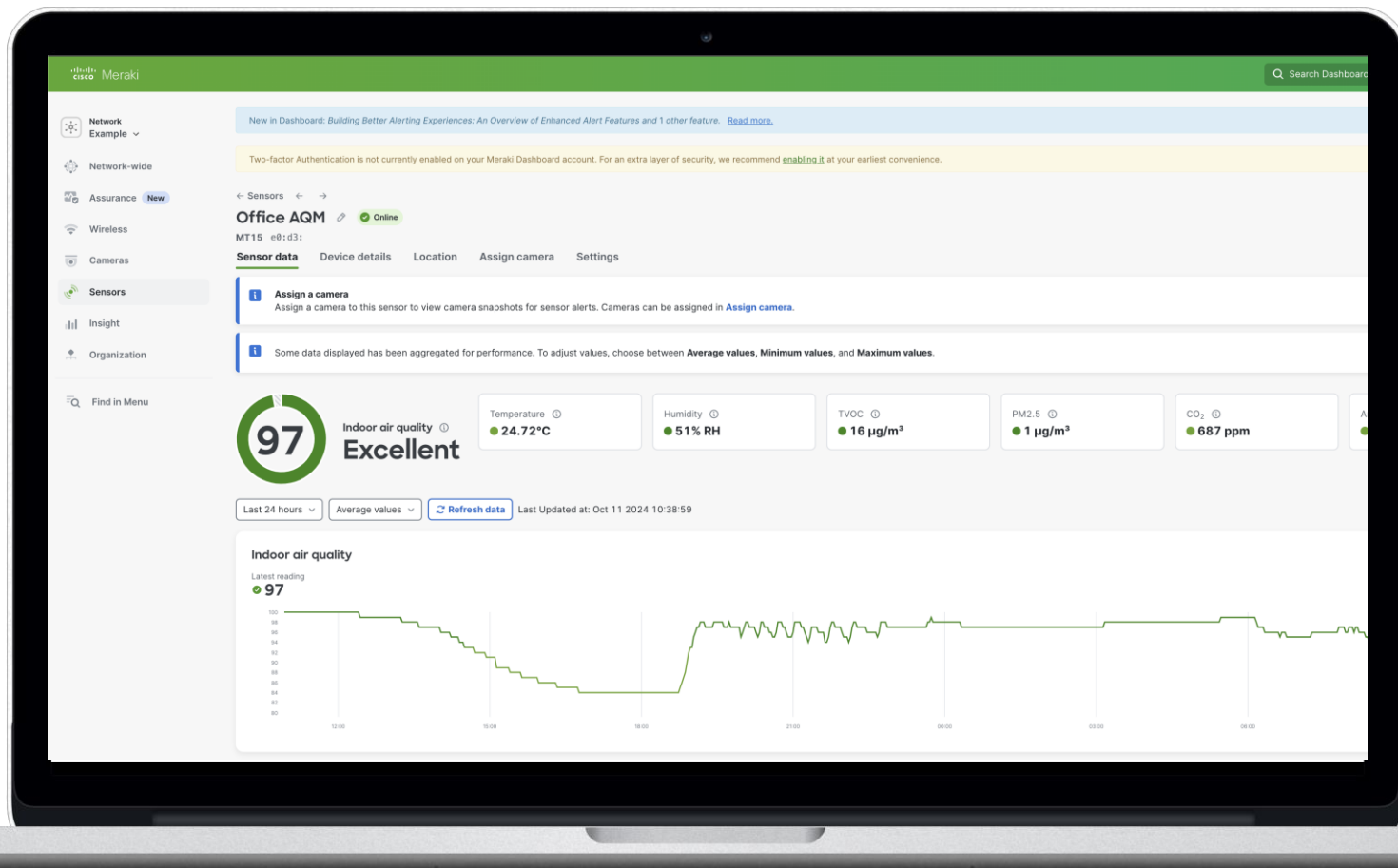


Meraki MT15

Indoor air quality and carbon dioxide sensor

- CO2
- Total Volatile Organic Compounds
- Particulate Matter (PM2.5)
- Temperature and Humidity
- Ambient Noise
- Vape Detection



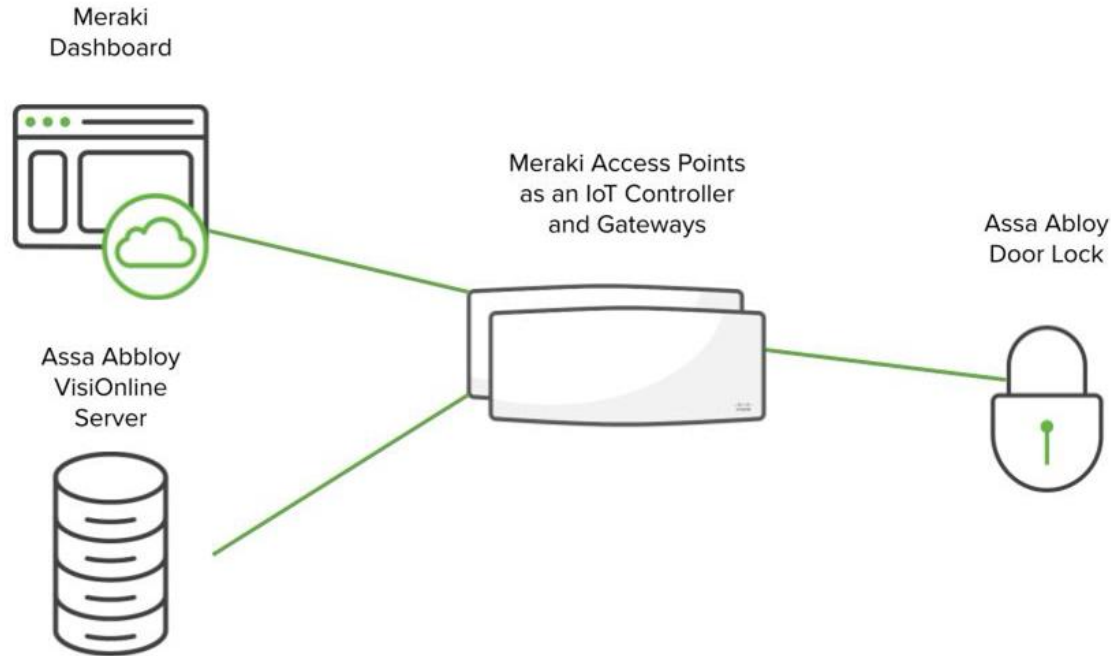




A background image showing two hands in business attire holding a small white card. The image is overlaid with a dark blue semi-transparent banner containing the text "EXTEND BEYOND MERAKI IOT".

EXTEND BEYOND MERAKI IOT

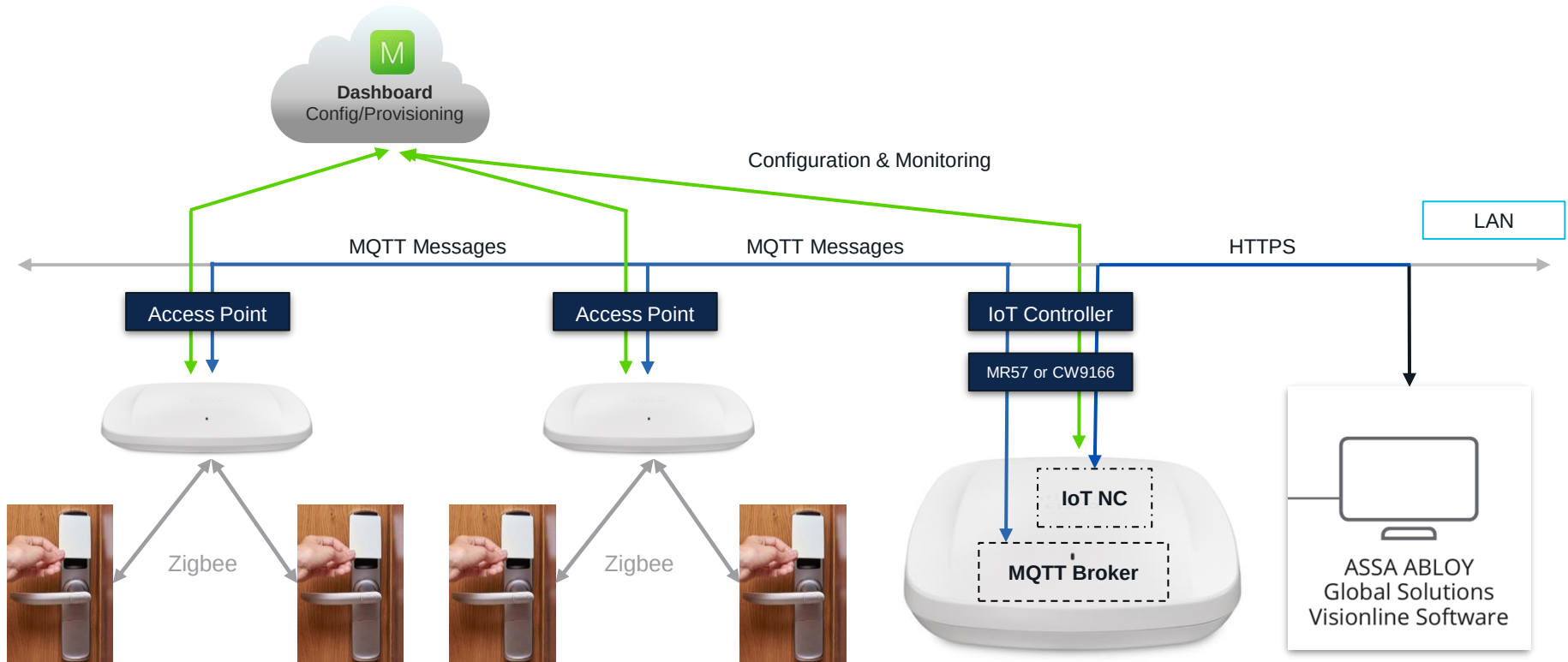
Meraki Wireless + Assa Abloy Door Locks



Meraki Wireless + Assa Abloy Door Locks

- No dedicated overlay network or additional hardware required
- IoT radio in Meraki AP functions as a Zigbee Gateway
- Visibility and Insight into connected gateway and online status of locks in Meraki Dashboard

Detailed Architecture



Supported Hardware

IOT Controller

MR57



CW9166



ZigBee Gateways

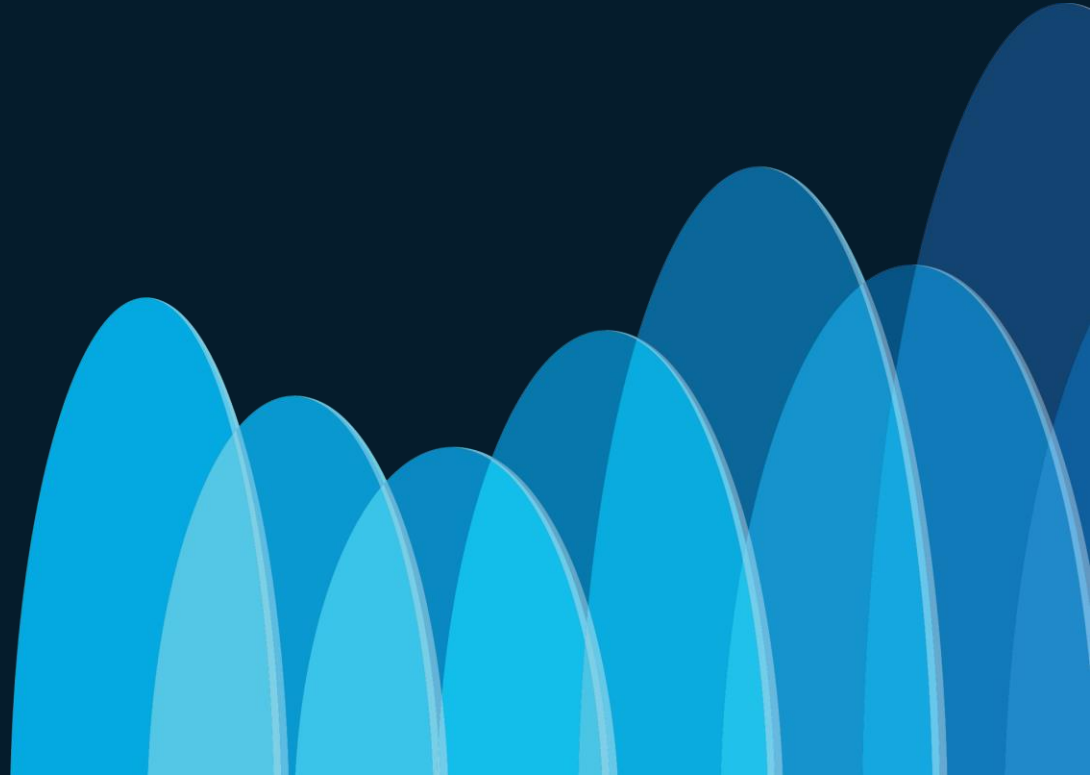
All Wi-Fi 6 / 6E APs
(16x Models)



Currently in Private Beta

Reach out to Travis Schlafke tschlafk@cisco.com
or your local account team.

CONCLUSION



Agenda

- The need for compelling guest experiences
- iPSK and Wireless Personal Network (WPN)
- Beyond the Wi-Fi domain
 - Meraki IoT for healthy and sustainable guest experiences
 - Assa Abloy Door Lock Integration
- Conclusion

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