

CISCO *Live!*



#CiscoLive



The bridge to possible

Wi-Fi Personal Network (WPN)

The At-Home Experience in Enterprise Networks

James Sands, Technical Solutions Architect, Cisco Meraki

BRKMER-2000



#CiscoLive

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 June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKMER-2000>



Agenda

- The At-Home Experience – Why Does it Matter?
- Multicast-Based Discovery Protocols on Shared Networks
- User Segmentation on a Shared Network
- The Meraki Wi-Fi Personal Network
- User Self-Service and Automation
- Demonstrations

The At-Home Experience

Why Does it Matter?



Hospitality

“By recent surveys...65% of guests want to stream their content to the TV.”

<https://beyondtv.com/>



<https://beyondtv.com/>

Multi-Dwelling

“More tenants demand high-tech options, like free Wi-Fi in all rental units...”

<https://ipropertymanagement.com/research/property-management-industry-statistics>



<https://ipropertymanagement.com/research/property-management-industry-statistics>



Campus Housing

“...ranked among the Top 10 College Dorms nationally...from the comforts of home...”

<https://www.stevenson.edu/student-life/living-on-campus/housing-selection/>



<https://www.fivestarseniorliving.com/living-options/independent-living>

Senior Living

In 2021, 75% of adults 65+ years old use the Internet.

<https://www.pewresearch.org/internet/fact-sheet/internet-broadband/>

At-Home Wi-Fi User Experience

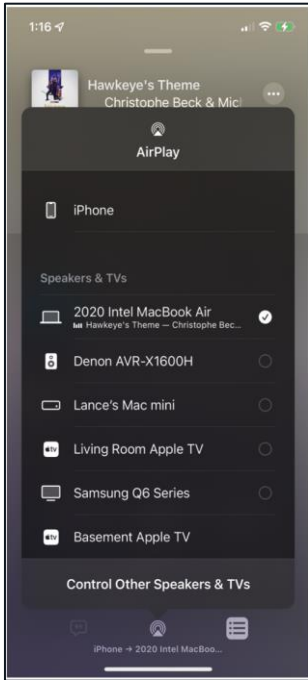
Device Discovery and Shared Networks



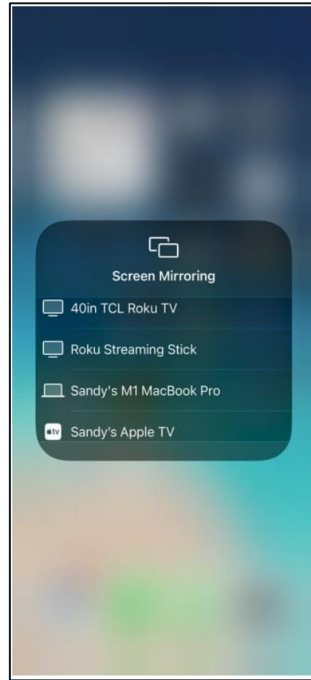
<https://gifimage.net/wp-content/uploads/2017/10/moving-eyes-gif-3.gif>

At-Home Wi-Fi User Experience

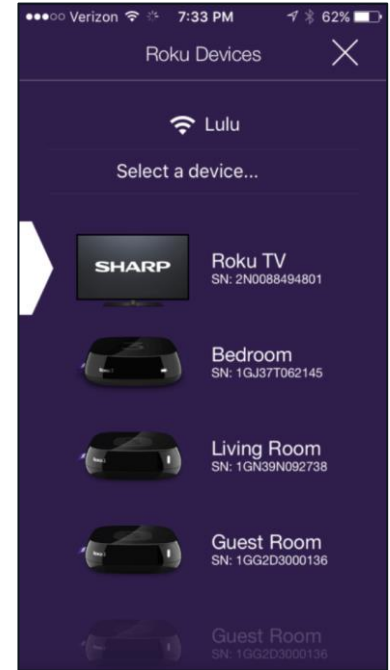
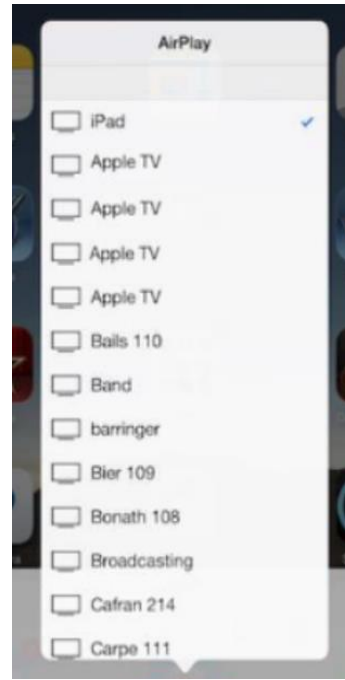
Device Discovery and Shared Networks



<https://www.pcmag.com/how-to/airplay-stream-screen-mirror-audio-video-ipad-phone-mac-appletv>



<https://www.digitaltrends.com/computing/how-to-use-airplay-stream-mirror-screen/>



https://blog.roku.com/wp-content/uploads/2015/08/Roku-Mobile-App-iOS_switch-device.png

Meraki Wi-Fi Personal Network (WPN)

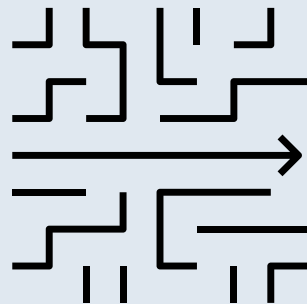
Simple, Secure and Scalable Solution



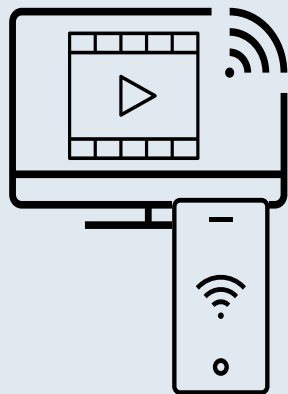
Multicast-Based Discovery Protocols on Shared Networks



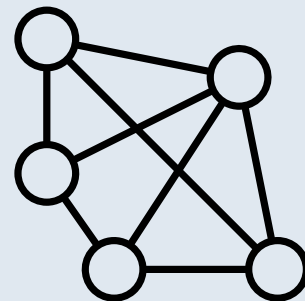
Multiple smart
devices per person



Interoperability



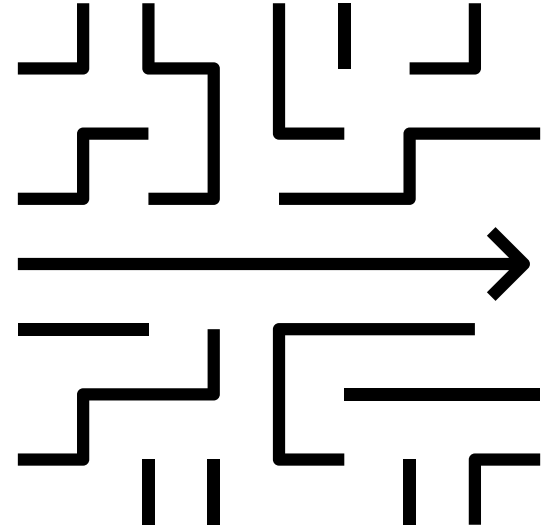
Zero Configuration
Networking



Multicast-Based Discovery Protocols

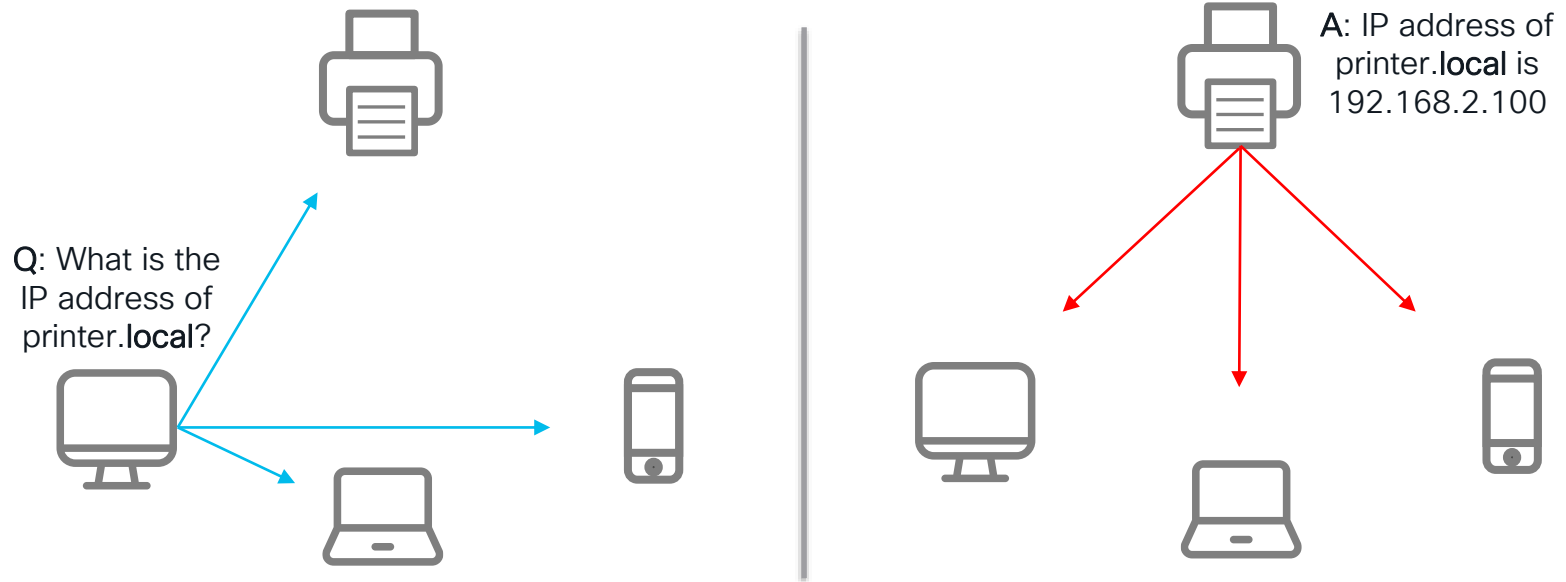
Zero Configuration Networking

- Automatically Creates a Functional Network:
 - Address Assignment
 - Host Name Resolution
 - Service Discovery



Multicast-Based Discovery Protocols

Name Resolution Without a Name Server



¹ <https://datatracker.ietf.org/doc/html/rfc6762>

² <https://en.wikipedia.org/wiki/Multicast> (diagram)

Multicast-Based Discovery Protocols

Name Resolution and Service Discovery

- Multicast DNS (mDNS) – RFC 6762
 - Bonjour Services
- Simple Service Discovery Protocol (SSDP)
 - Universal Plug and Play (UPnP)
 - Digital Living Network Alliance (DLNA)
- Etcetera

mDNS

- 224.0.0.251
- FF02::FB

SSDP

- 239.255.255.250
- FF02::c

2 – link local scope is the most common

User Segmentation: Easier Said than Done



User Segmentation on a Shared Network

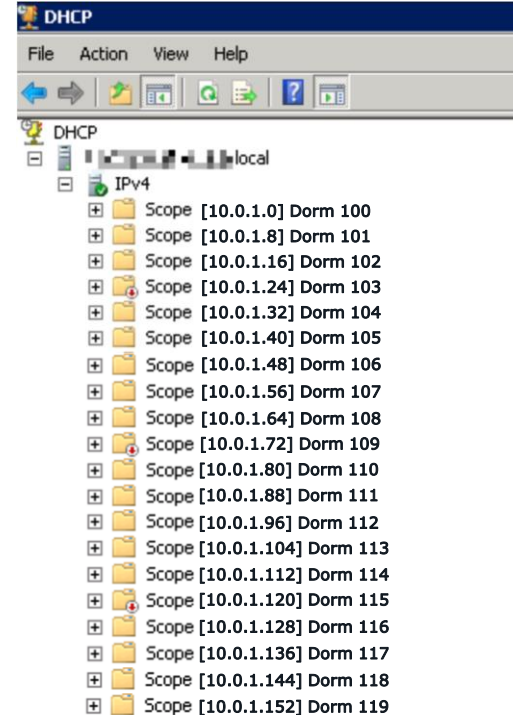
Traditional Method is Complex and Does Not Scale Well

VLANs

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

Subnets

DHCP
Scopes



User Segmentation on a Shared Network

Difficult to Manage, Doesn't Scale Well

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-to-Peer Blocking

L2 Isolation



SSID per user or group of users

User Segmentation on a Shared Network

Existing solutions are Costly and Complex

- Complex network designs
- Disparate management interfaces
- Client App for onboarding
- Cumbersome onboarding workflows



http://b.vimeocdn.com/ts/123/631/123631397_640.jpg

The Meraki WiFi Personal Network (WPN)



Meraki Wi-Fi Personal Network (WPN)

Built on Identity Pre-Shared Key (IPSK) *without* RADIUS

Basic info

SSID (name) ← SSID

SSID status Enabled Disabled

☐ Hide SSID

Identity PSK without RADIUS ←

Devices are assigned a group policy based on its passphrase

WiFi Personal Network (WPN) ⓘ ←

Enabled




Disabled

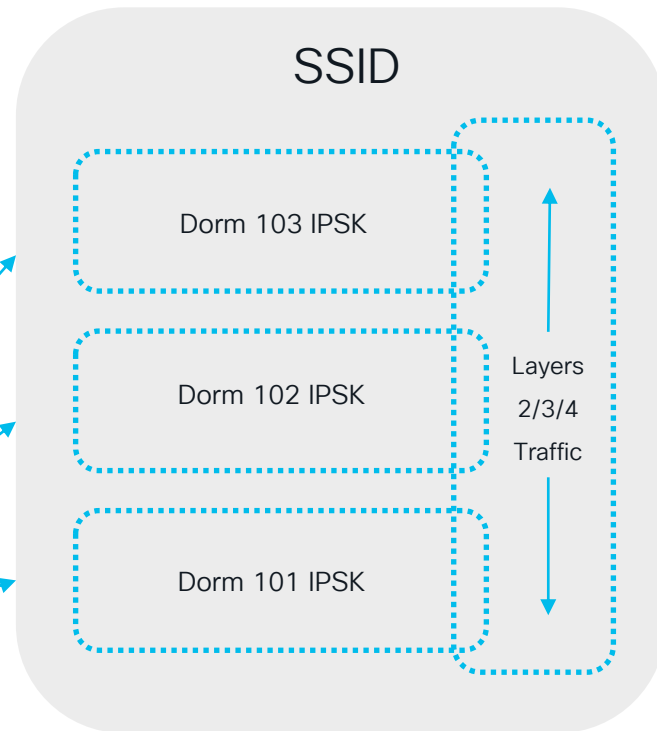
Add

Delete

Search Identity PSKs...

3 Identity PSKs

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



Meraki Wi-Fi Personal Network (WPN)

WPN, One Click Segmentation

Basic info

SSID (name)

SSID status

☐ Hide SSID

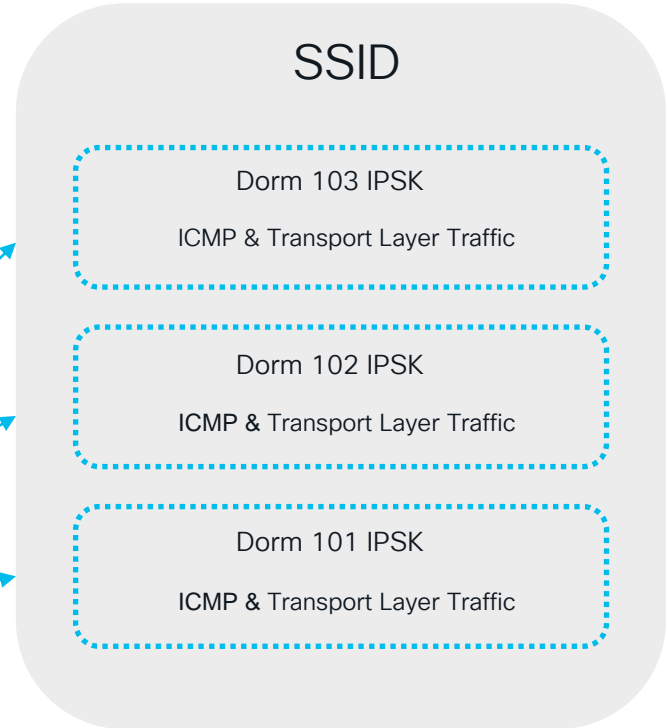
☒ Identity PSK without RADIUS
Devices are assigned a group policy based on its passphrase

WiFi Personal Network (WPN)

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

3 Identity PSKs

<input type="checkbox"/>	Name ▲	Pre-Shared Key	Group Policy
<input type="checkbox"/>	Dorm 103 <input type="button" value="eye"/>	Dorm-103-WPN-GP
<input type="checkbox"/>	Dorm 102 <input type="button" value="eye"/>	Dorm-102-WPN-GP
<input type="checkbox"/>	Dorm 101 <input type="button" value="eye"/>	Dorm-101-WPN-GP



Up to 5000 IPSKs per SSID with WPN enabled

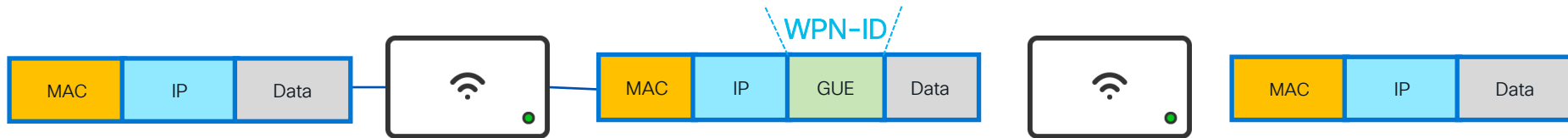
CISCO *Live!*

Wireless > Configure > Access Control

Meraki Wi-Fi Personal Network

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

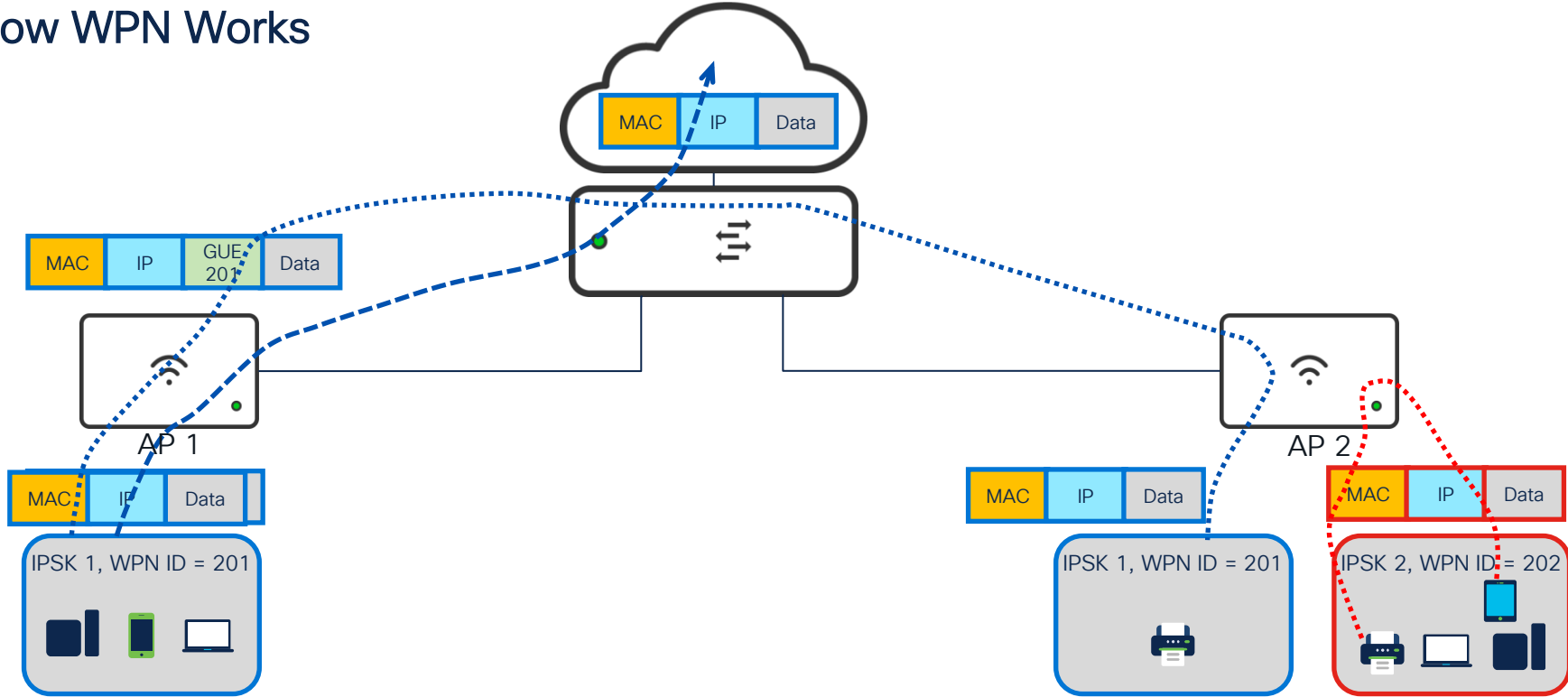


Destination AP strips the GUE header

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

Meraki Wi-Fi Personal Network

How WPN Works




Meraki Wi-Fi Personal Network

Meraki Group Policy Identifies User Devices

Health

WIRELESS

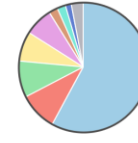
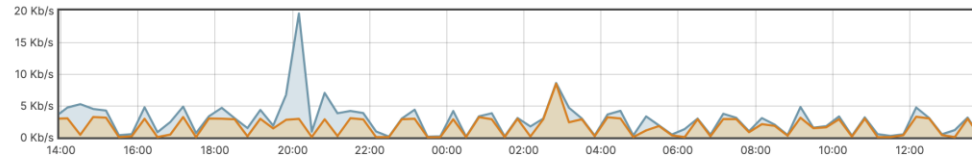
 2/2 healthy







Clients

all ▾ for the last day ▾

29.5 MB (↓ 25.4 MB, ↑ 4 MB)

Applications ▾



Policy ▾		Search...		5 client devices		Add client ▾		Download As ▾	
<input type="checkbox"/>	Status	Description	Connected To	802.1X policy	MAC address	Last seen	Usage ▾	IPv4 address	
<input type="checkbox"/>		Entertainment-Room	Basement 36-1	Dorm-101-WPN-GP	34:fd:6a:03:66:14	May 2 13:57	18.2 MB	192.168.2.20	
<input type="checkbox"/>		X0160029A4YA	Basement 36-1	Dorm-102-WPN-GP	20:ef:bd:5a:76:48	May 2 13:57	5.5 MB	192.168.2.18	
<input type="checkbox"/>		Jims-iPhone-2	Basement 36-1	Dorm-102-WPN-GP	4a:d4:3a:a2:37:10	May 2 13:57	3.5 MB	192.168.2.30	
<input type="checkbox"/>		Jims-work-iPhone	Basement 36-1	Dorm-103-WPN-GP	6a:2e:2e:f0:c7:77	May 2 13:57	2.9 MB	192.168.2.38	
<input type="checkbox"/>		iPad	Basement 36H-2	Dorm-101-WPN-GP	3a:a7:77:41:31:4f	May 2 13:56	132 KB	192.168.2.32	

Click on the wrench to add the '802.1X Policy' column

Network-wide > Monitor > Clients

WPN Requirements

- MR29+
- Wi-Fi 5 Wave 2 APs and later
- Standard Feature, no additional license required
- Bridge Mode
- New Version of 'Access Control' page



User Self-Service and Automation



User Self-Service and Automation

Improving the User Experience and IT Efficiency



splashaccess.

Our Wi-Fi

Please enter your details below

Email Address

First Name

Last Name

☐ I agree to the Terms and Conditions.

☐ Yes, I would like to receive news and offers via email.

Continue

Or please enter your voucher code

Voucher code:

☐ I agree to the Terms and Conditions.

Continue

Manage WPA2 Portal


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

User Self-Service and Automation

Improving the User Experience and IT Efficiency




Identity Pre-share Key + 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

<input type="checkbox"/> Name ▲	Pre-Shared Key	Group Policy
<input type="checkbox"/> Dorm 103	<input type="password" value="....."/> 	Dorm-103-WPN-GP
<input type="checkbox"/> Dorm 102	<input type="password" value="....."/> 	Dorm-102-WPN-GP
<input type="checkbox"/> 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](#)

User Self-Service and Automation

The Meraki Dashboard API

Update Network

Operation ID: updateNetwork

Description: Update a network

PUT /networks/{networkId}

Request Parameters

Path

networkId * | String

No Description

Body

updateNetwork | Object

No Description

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/>

 **Meraki Marketplace**

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



<https://github.com/meraki>

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

Session Recap

- An 'at-home' user experience offers a competitive advantage
- Device discovery on a shared network creates confusion and is insecure
- Multicast-based discovery protocols on shared networks are the crux of the problem
- Traditional means of segmenting user traffic is difficult and costly
- WPN is secure, scalable, easy to implement, and does not require a license
- IPSK is required and provides access to an SSID using multiple PSKs
- Meraki Dashboard API enables automation, improves the user experience and simplifies IT administration

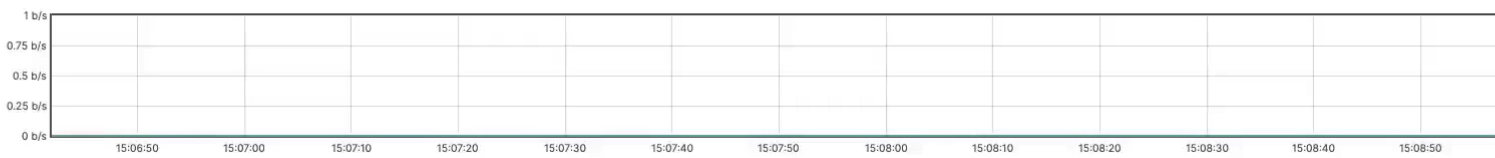
Wi-Fi Personal Network (WPN) Demonstration

Meraki has recently updated our list of subprocessors. See the [Meraki subprocessors page](#) to learn more.

Health

Clients

allfor the last day



Policy

Search...

No clients have used this network in the specified time span.

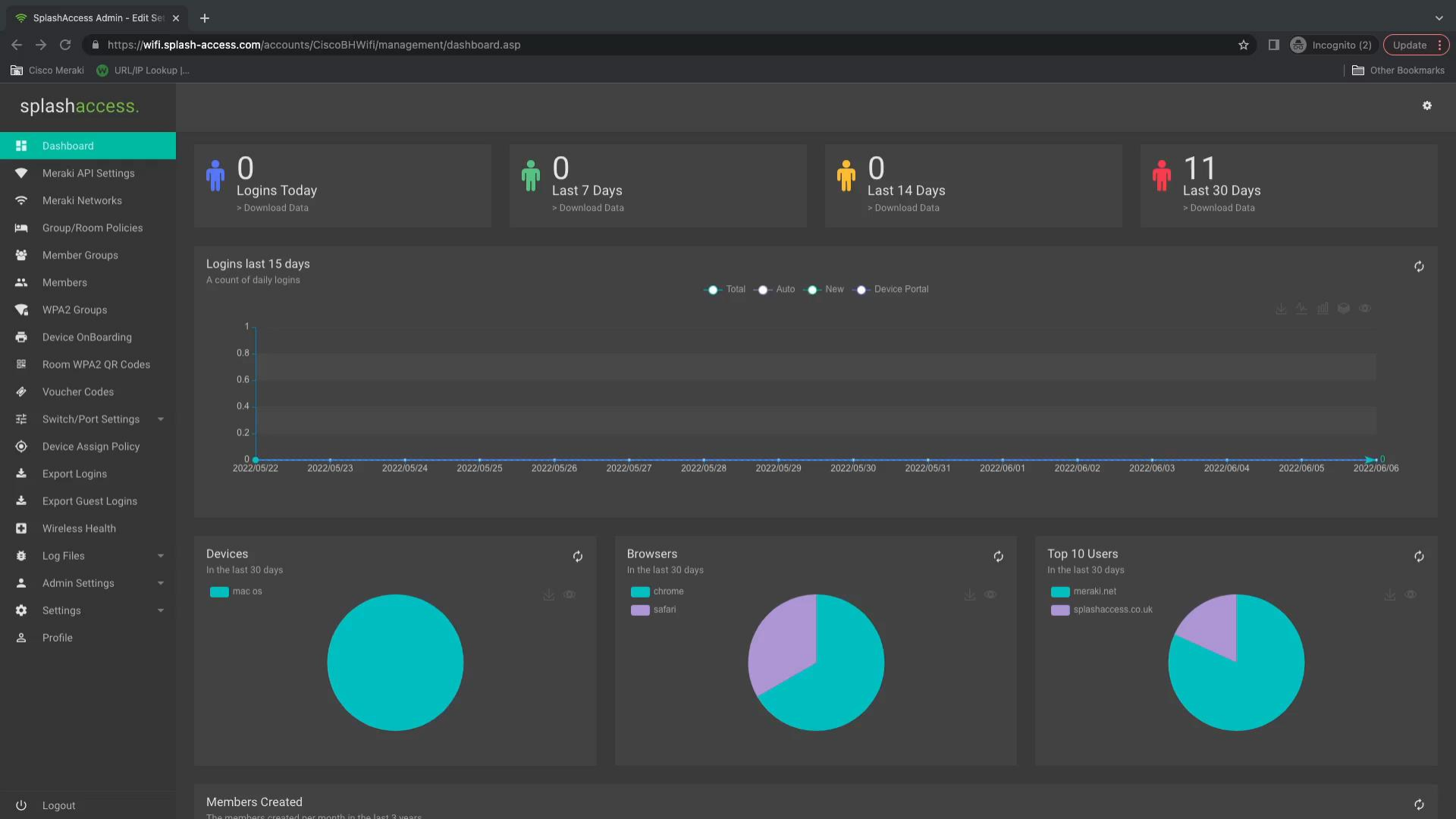
Applications

[More](#)

Add client

Download As

SplashAccess Demonstration



Call to Action

Start a Free Trial



Contact your Cisco or Meraki
sales rep



The bridge to possible

Thank you

Appendix

Caveats

- WPN supports wireless traffic only (i.e., wired traffic on the same L2 domain is not supported today)
- WPA3 is not supported upon initial release
- Devices on different VLANs can reach wireless devices via L3 routing
- NAT mode is not supported on the SSID using WPN (Bridge Mode only)
- WPN does not support the wired ports on MR30H and MR36H at initial release
- Users can roam and access their own devices if they are on the same VLAN and Meraki Network

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.



Learn

Cisco U.

IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology, and certification training

Cisco Modeling Labs

Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network

Resource community portal for certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product, technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups

180-day certification prep program with learning and support

Cisco Continuing Education Program

Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

CISCO *Live!*



#CiscoLive