

CISCO *Live!*



#CiscoLive



The bridge to possible

Cisco Routing Meraki Access with IPv6 (CRMAv6)

A Practical Guide

Jeffry Handal, Technical Leader
@ipv6pilot
BRKIPV-2751



#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/#BRKIPV-2751>



Agenda

- The Enterprise Today
- CRMAv6
- IPv6-only Management Access
- The Future of the Enterprise

Why are We Here?

The session is a dive into exploring some best practices operating IPv6 with Cisco infrastructure and the Meraki platform. We will examine and demo how to plan, setup, and maintain dual-stack and IPv6-only networks, including practical tips and tricks.

Find the Easter egg





*“IPv6 is a tool for simplification,
innovation, and imagination.”*

Jeffry Handal

Circa 2009

The Enterprise Today



The v6 Enterprise Utopia



Client OS



Enterprise
Network



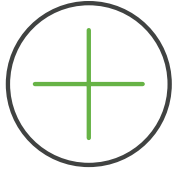
ISP



Internet



IPv6 to Solve Problems



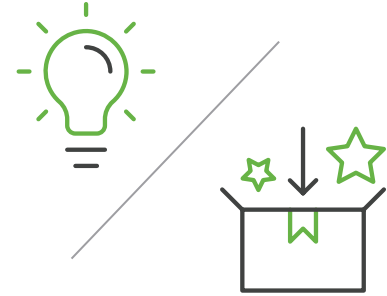
Simpler operations

- Less moving parts (e.g., no DHCP)
- More automation inherit of the protocol
- Avoid headaches caused by NAT and CGNs



Equalizer

- Available to everyone
- Costs less



Future-ready, improved experiences

- Gamification of the workplace
- Industry 4.0
- 5G solutions

How do we make the enterprise take the leap?





CRMAv6

What does CRMAv6 stand for?

Cisco-Routing Meraki-Access with IPv6

What is CRMAv6?

An architecture design that uses Cisco platforms to solve problems with IPv6 as its core enabler.

For the context of this presentation, we will assume the following

- Cisco Routing
 - Edge use case with ASR/ISR
 - Core use case with Catalyst
- Cisco Meraki access
- Cisco Umbrella DNS



Source: IPv6 logo from <https://www.worldipv6launch.org/downloads/>

Design Setup Assumptions – Edge Case

- Native ISP IPv6 availability with DHCPv6-PD
- Client support for all Operating Systems
 - DHCPv6, RA DNS, RA RDNSS option
- Dual stack or IPv6-only for client segments
- Dual stack or IPv6-only management network
- Network services reachable over IPv6:
 - RADIUS, SYSLOG, DHCP, SNMP, SSH, NETCONF
- Transition mechanism leveraged: NAT64/DNS64

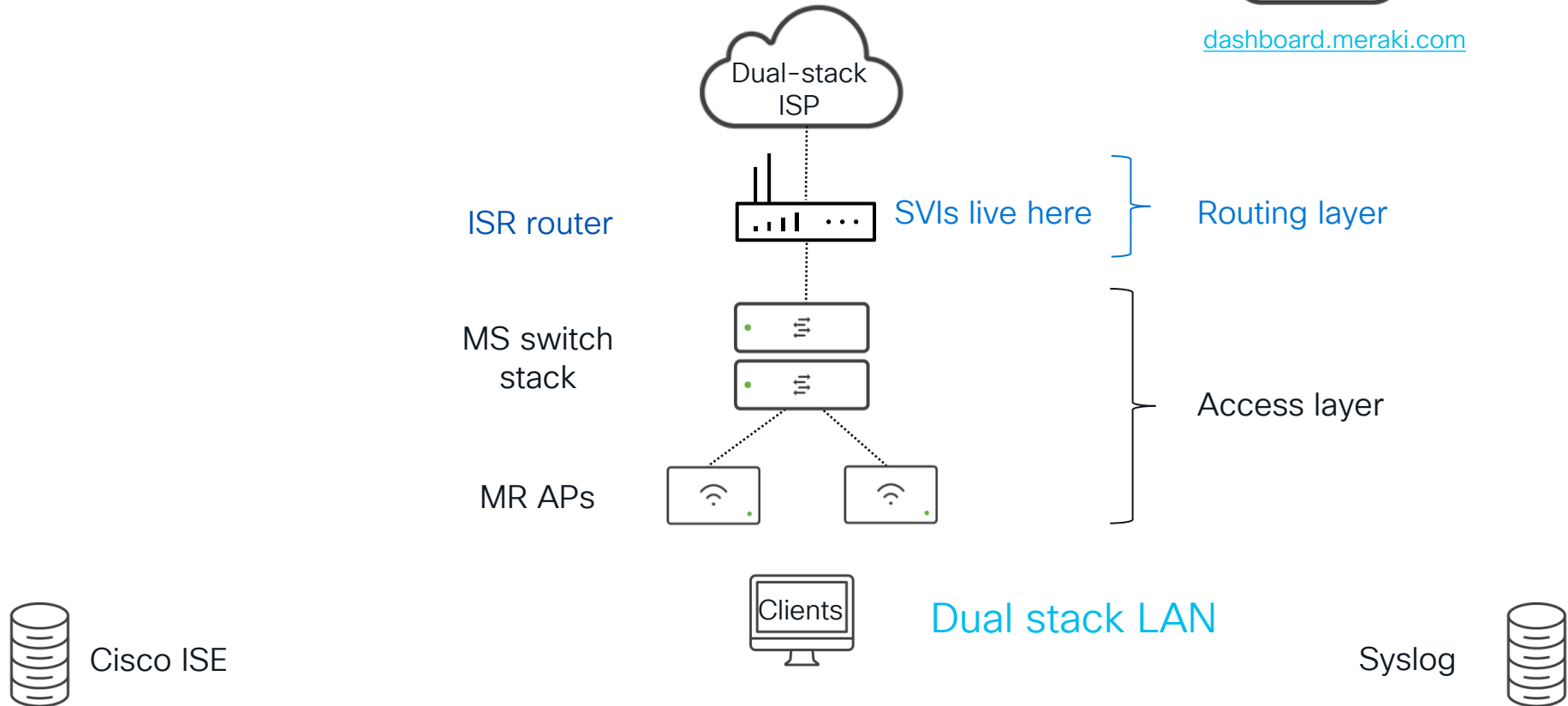


Aim for IPv6-only
where possible

S/M/L Branch Site – Dual Stack



dashboard.meraki.com



Cisco ISE

CISCO *Live!*

Dual Stack VLAN Interface – Cisco IOS

```
interface Vlan10
description CLIENTS
ip address 10.10.10.1 255.255.255.0
ip nat inside
ipv6 address FE80::C15:C010:1 link-local
ipv6 address ISP::2:0:0:0:1/64
ipv6 enable
ipv6 nd reachable-time 1800000
ipv6 nd autoconfig prefix
ipv6 nd autoconfig default-route
ipv6 nd other-config-flag
ipv6 nd router-preference High
ipv6 nd ra lifetime 9000
ipv6 nd ra dns server 2620:119:35::35
ipv6 nd ra dns server 2620:119:53::53
ipv6 dhcp server CLIENTSv6
```

Vanity IP Address

DHCPv6-PD

Umbrella Recursive DNS Servers

DHCPv6

DHCPv6 Options

```
ipv6 dhcp pool CLIENTSv6
```

```
dns-server 2620:119:35::35
```

```
dns-server 2620:119:53::53
```

Vanity IP
Address

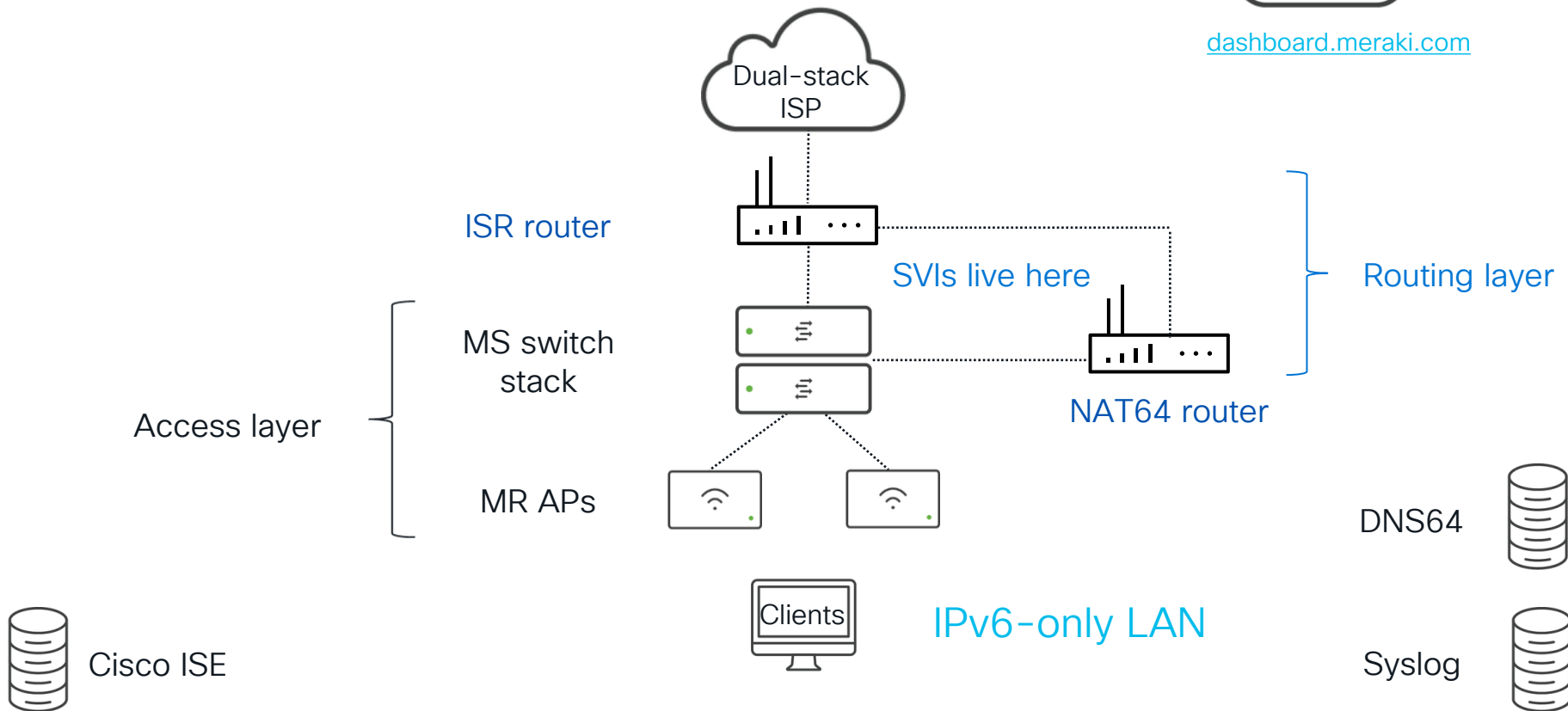
DHCPv6 is supported by all
clients except Android.



S/M/L Branch Site – NAT64/DNS64



dashboard.meraki.com



IPv6-Only VLAN Interface – Cisco IOS NAT64 Example

```
interface Vlan500
description NAT64 v6 SIDE
ipv6 address FE80::C15:C0:500:1 link-local
ipv6 address ISP ::3:0:0:0:1/64
ipv6 enable
ipv6 nd reachable-time 1800000
ipv6 nd autoconfig prefix
ipv6 nd autoconfig default-route
ipv6 nd other-config-flag
ipv6 nd router-preference High
ipv6 nd ra lifetime 9000
ipv6 nd ra dns server 2601:C15:C0:1234::53
ipv6 dhcp server NAT64
```

Vanity IP
Address

Custom DNS64

Cloudflare DNS64:
2606:4700:4700::64
2606:4700:4700::6400

Google DNS64:
2001:4860:4860::6464
2001:4860:4860::64

DNS64 – Bind Example



RFC6147

```
dns64 64:ff9b::/96 {  
    clients {any;};  
    mapped { !10/8; any; };  
    exclude { 0::/3; 4000::/2; 8000::/1; 2001:DB8::/32; };  
    break-dnssec yes;  
};
```

[/etc/bind/named.conf.options](#)

NAT64 Setup

Think:
“Router on a stick setup”

```
ipv6 dhcp pool NAT64  
  dns-server 2601:1234:1234:ABCD::53
```

```
nat64 prefix stateful 2601:2C2:1111:B6::/64  
nat64 v4 pool NAT64POOL 10.22.22.11 10.22.22.14  
nat64 v6v4 list NAT64 pool NAT64POOL overload
```

```
ipv6 access-list NAT64  
  sequence 30 permit ipv6 2601::/20 any
```

```
Interface XXXX  
  nat64 enable
```

Issue command on an
IPv6 and IPv4 interface.

Demo

Meraki

Search Dashboard

Network

Network-wide

Security & SD-WAN

Switch

Insight

Organization

Health

Clients

all for the last day

1.6 Mb/s

1.2 Mb/s

0.8 Mb/s

0.4 Mb/s

0 Mb/s

Policy Forget Search...

Add client Download As

<input type="checkbox"/>	Status	Description	Usage	Device type, OS	IPv4 address	MAC address	User	
--------------------------	--------	-------------	-------	-----------------	--------------	-------------	------	--

Last login
about 1 hour ago from 3.88.26.134 Ashburn, VA

Current session started
42 minutes ago

Data for this organization is hosted in North America

© 2022 Cisco Systems, Inc.
Privacy - Terms

Give your feedback

Sending request to bam-cell.nr-data.net...

Design Setup Assumptions – Core Case

- Native ISP IPv6 availability up through edge device
- L3 routing is handled at the core/distribution level
- Client support for all Operating Systems
 - DHCPv6, RA DNS, RA RDNSS option
- Dual stack or IPv6-only for client segments
- Dual stack or IPv6-only management network
- Network services reachable over IPv6:
 - RADIUS, SYSLOG, DHCP, SNMP, SSH, NETCONF
- Transition mechanism leveraged: NAT64/DNS64

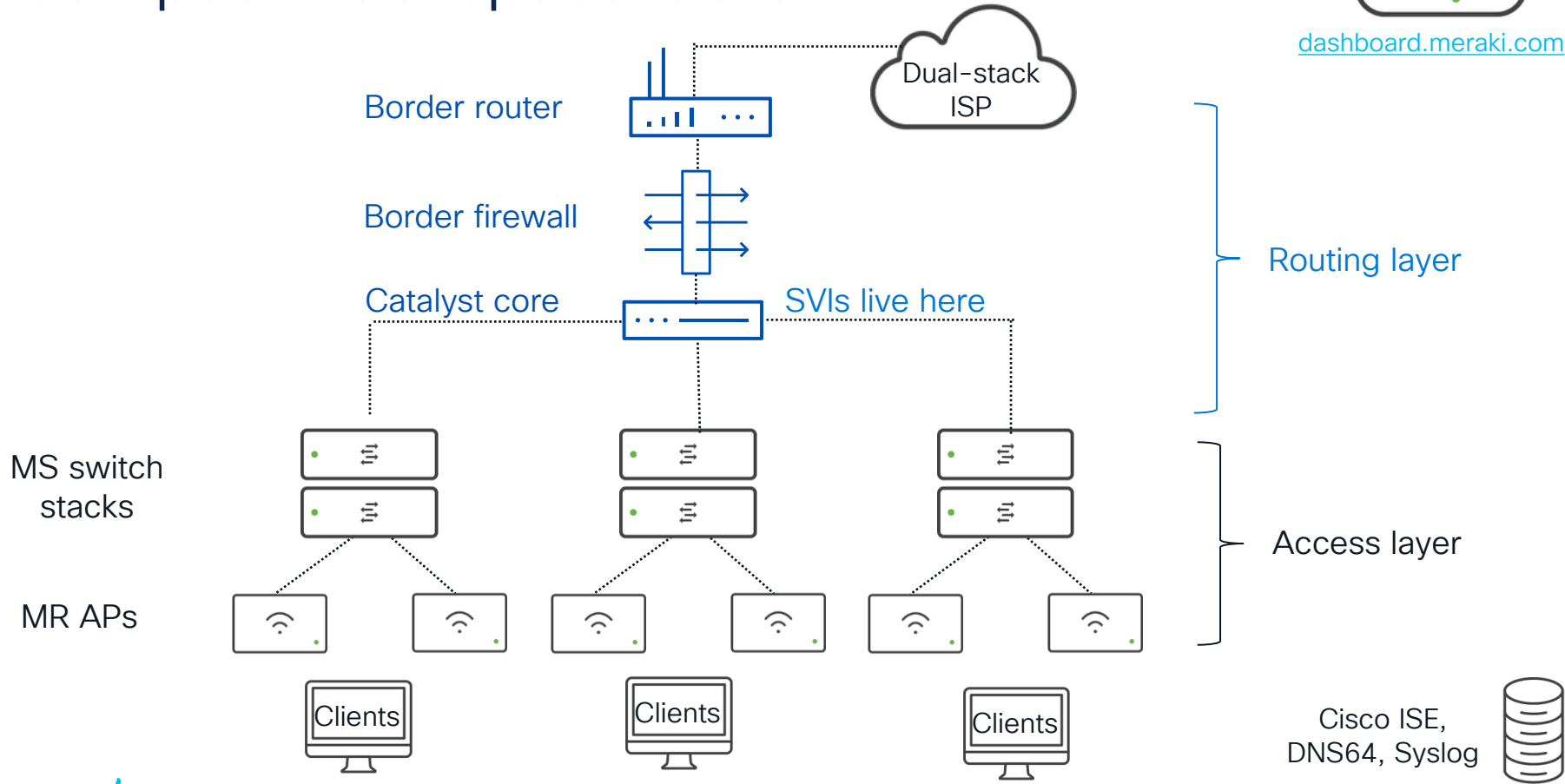


Aim for IPv6-only
where possible

Campus – Collapsed Core



dashboard.meraki.com



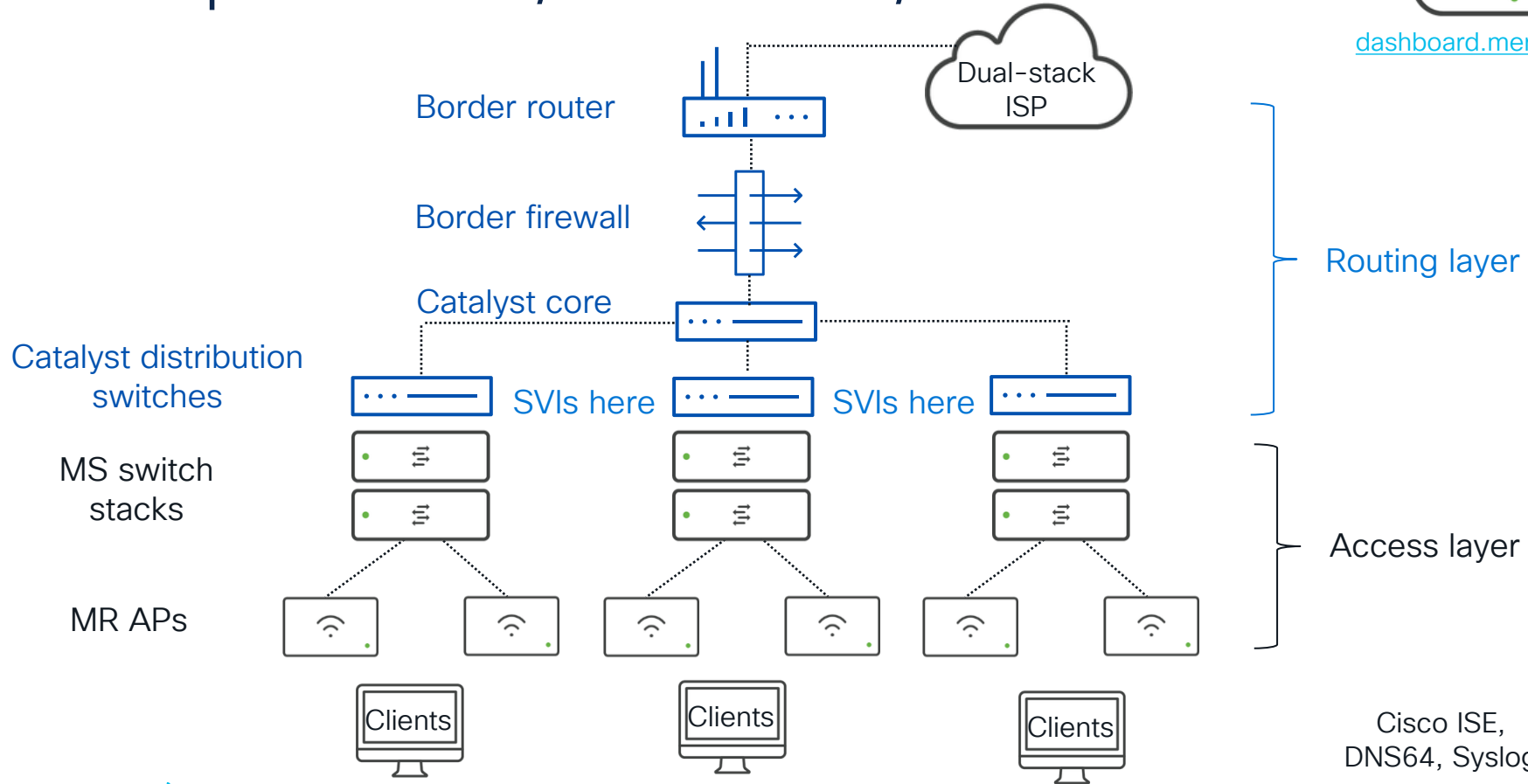
Cisco ISE,
DNS64, Syslog



Campus – Core/Distribution/Access



dashboard.meraki.com



Cisco ISE,
DNS64, Syslog



Meraki Management for Catalyst

#1 in cloud
managed
networks



#1 in
networking

Campus Lessons Learned

Service



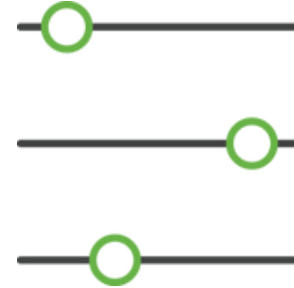
Intended functionality
to enable for end
users

RA origination



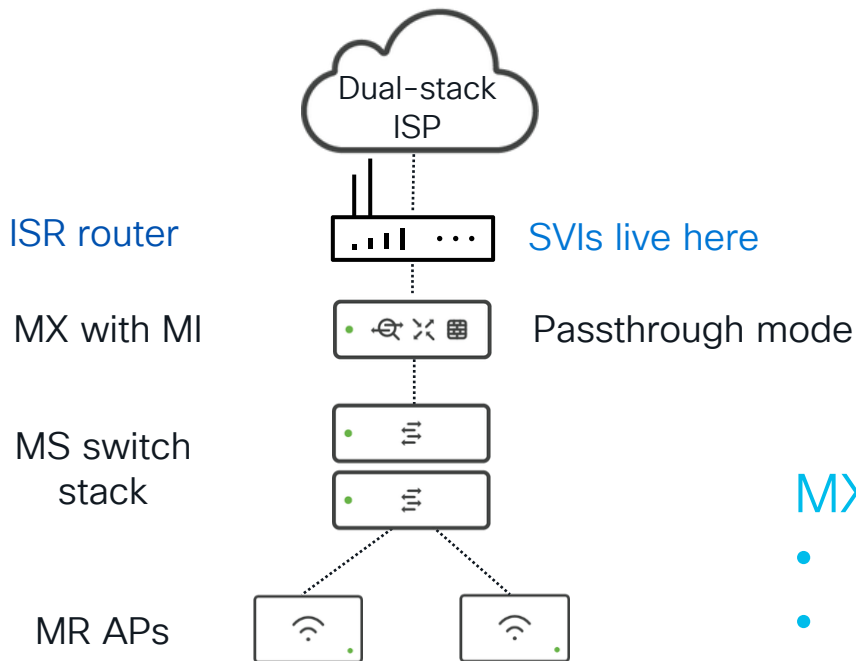
SVI location in the
grand scheme

Policers



Be aware of broadcast and
multicast policers on the
network path

Bonus – MX-as-a-Sensor



MX in this setup offers IPv6:

- Visibility
- Performance metrics
- L3/L7 security options



Cisco ISE

Syslog



IPv6-only Management Access

Is IPv6-only
management with
Cisco Meraki possible?



IPv6 Addressing

Product Family	IPv6 Address	SLAAC	RDNSS	Static Assignment	DHCPv6	LSP* Reachability	LSP* Assignment
MR	Yes	Yes	Yes	Yes	No	Yes	Yes
MS	Yes	Yes	Yes	Yes	No	Yes	Yes

*LSP: Local status page

Only two IPv6 addresses expected: GUA/ULA and link-local

IPv6 Addressing – Local Status Page (LSP)



The screenshot shows the Meraki Local Status Page (LSP) in a web browser. The browser address bar shows the URL [2601:2c3:8881:b5:3656:feff:feb0:3ae2]/#connection. The page header displays the Cisco Meraki logo. A large green checkmark icon is centered on the page, with the word "Healthy" below it and the text "This switch is functioning normally". Below this, there are four tabs: "Connection", "Uplink configuration", "Switch ports status", and "Switch ports configuration". The "Connection" tab is selected. Under the heading "Your client connection", there is a table with the following data:

Client IP	2601:2c3:8881:b5:3656:feff:feb0:3ae2
Client MAC	70:69:5a:8d:55:74
VLAN	500
Port	10

The screenshot shows the "Uplink configuration" page in the Meraki GUI. The page title is "Uplink configuration" and the subtitle is "Configure the uplink Internet connection on this switch." Below this, there is a section for "IP configuration". The "IP assignment" is set to "DHCP". The "VLAN" is set to "500". The "IPv6 assignment" is set to "Static" (with "Auto" also visible). The "IPv6 Static VLAN" is set to "500". The "Address/Prefix Len" is set to ":: / 64". The "Gateway" is set to "::". The "DNS server 1" is set to "::". The "DNS server 2" is set to "::".

Address assignment via LSP

LSP => GUI-based console

IPv6 Addressing – Dashboard View



MR

<input type="checkbox"/>	#	Status	Name	MAC address	Model	Connectivity	Public IP	Local IP	
<input type="checkbox"/>	1	●	KIAH-PATIO-MR70	e0:cb:bc:b9:73:1f	MR70		2601:2c0:3001:100:0a10:00ff:fe59:731f	0.0.0.0	
<input type="checkbox"/>	2	●	KIAH-MR46	98:18:88:fc:1e:5a	MR46		2601:2c0:3001:100:0a10:00ff:fe5a:1e5a	10.11.11.198	
<input type="checkbox"/>	3	●	KIAH-MR30H	e0:55:3d:ee:3f:33	MR30H		2601:2c0:3001:100:0a10:00ff:fe3f:3333		

LAN IPV6
VIA AUTOCONF
2601:2c0:3001:100:0a10:00ff:fe59:731f

VLAN
0

GATEWAY
fe80::c15:c0:100:1

DNS
2620:119:35::35
2620:119:53::53

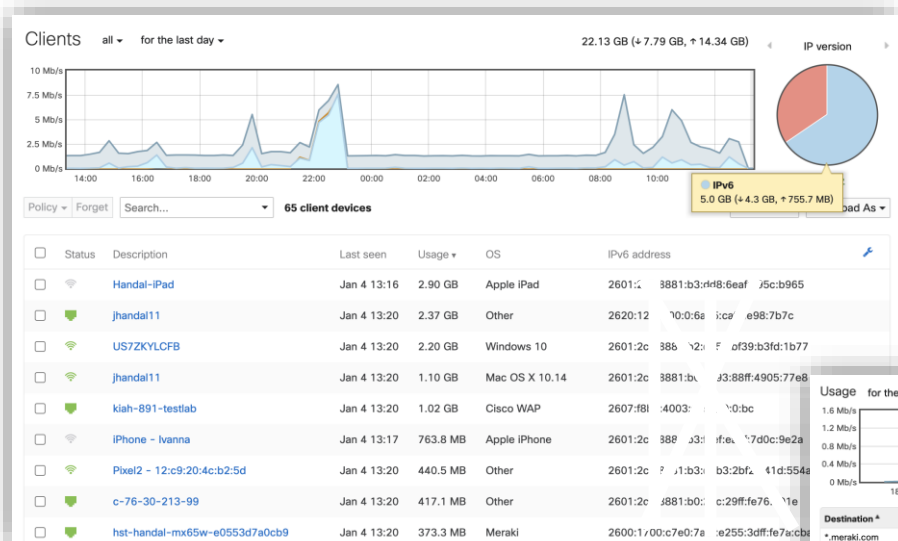
MS

<input type="checkbox"/>	#	Status	Name	MAC address	Model	Connectivity	Public IP	Local IP	
<input type="checkbox"/>	1	●	KIAH-MS220-8P-ASW-2	88:15:44:01:5a:10	MS220-8P		2601:2c0:3001:100:0a15:44ff:fe01:5a10	10.11.11.253	
<input type="checkbox"/>	2	●	KIAH-MS220-8P-ASW-1	00:18:0a:88:44:28	MS220-8P		2601:2c0:3001:100:0a18:0aff:fe03:4428	10.11.11.161	
<input type="checkbox"/>	3	●	KIAH-MS210-24P-ASW-3	98:18:88:7e:f5:29	MS210-24P		2601:2c0:3001:100:0a18:00ff:fe7e:f529	10.11.11.250	
<input type="checkbox"/>	4	●	KIAH-MS120-8LP-ASW-4	0c:8d:db:03:c0:1f	MS120-8LP		2601:2c0:3001:100:0c8d:dbff:fc03:c01f	10.11.11.169	

IPv6 Monitoring and Troubleshooting (M&T)

Product Family	Traffic Analytics	Syslog	Netflow	SNMP	RADIUS	Scanning API
MR	Yes	Yes	No	Yes	Yes	Yes
MS	Yes	No	No	Yes	Yes	N/A

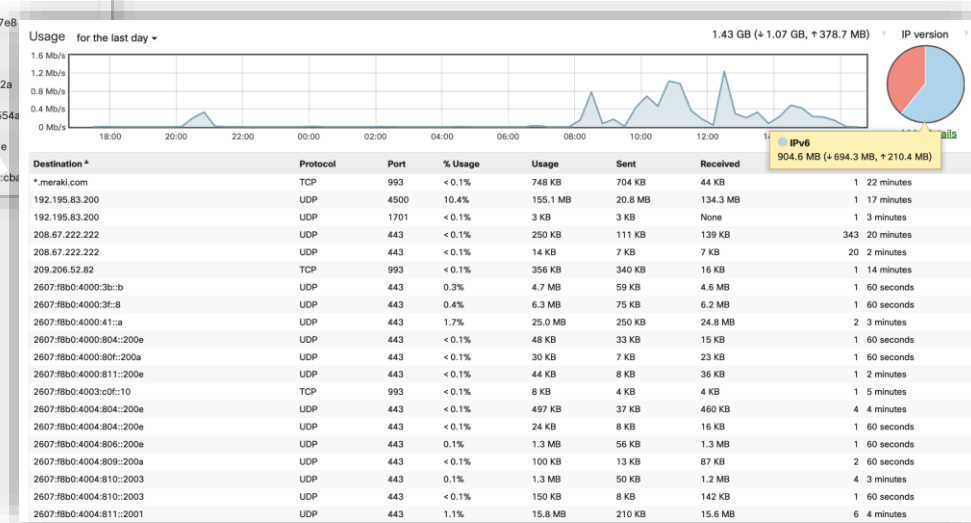
IPv6 M&T- Traffic Analytics



Network-wide -> Clients

Visibility for both IP protocols!

Specific client page details



IPv6 M&T – Address History




Network-wide -> Clients -> specific client

CLIENTS

MININT-74K1CS6 


Overview **Connections** Performance History

Status  associated since Jan 10 11:28


SSID JETNETv6

Access point [KIAH-NAT64-MR36 topology](#)

Splash N/A

Signal  59dB (channel 108)

User miles (802.1X login)

Device type Intel Windows 10 

Capabilities 802.11ac - 2.4 and 5 GHz [details](#)

[event log](#) [packet capture](#)

Network

IPv4 address: 169.254.78.194

IPv6 address: 2601:2cc:ccc1:b6:3443:d5a9:fcf5:9947

IPv6 address (link-local): fe80:0:0:0:adc2:1c8f:fd6b:4ec2

MAC address: 00:28:f8:70:22:c7

IPv6 Address log

Export 

<input type="checkbox"/> First connected at ▼	Address	Type	Time connected
<input type="checkbox"/> Dec 2 17:07	fe80:0:0:0:adc2:1c8f:fd6b:4ec2	Link-Local	38d 18h 33m 37s

IPv6 M&T – Connection Path



Device type MR30H

LAN IP 10.11.11.157 (via DHCP)

LAN IPv6 2601:203:555:1:50:e255:501:fee:3f33 (via Autoconf)

Channel quality on 5 GHz radio for the past 2 hours

2.9% channel utilization

2 current connected clients

Usage on 5 GHz radio (Ch 40) for the past 2 hours

1.2 Kbps usage

[View more details](#)

Ping Packet capture

Hybrid architecture:
ISR at the edge example

Meraki Management
for Catalyst too!

Network-wide -> Clients -> specific client

IPv6 M&T – SNMP



SNMP

SNMP access

- ☐ Disable SNMP on access points in this network
- ☒ Allow SNMP v1/v2c access using the following community name:
- ☐ Allow SNMP v3 access using usernames and passphrases

There are no SNMP users for this network

[Add an SNMP user](#)

Network-wide -> General

```
snmpwalk -v2c -t 10 -c meraki12345 udp6:[2601:2c3:c15:c0:3350::ff:feb0:aaaa]:161
```

Snippet Output

```
SNMPv2-MIB::sysDescr.0 = STRING: Meraki MS120-8FP Cloud Managed PoE Switch
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.29671.2.340
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10394196) 1 day, 4:52:21.96
SNMPv2-MIB::sysName.0 = STRING: KIAH-MS120-8FP-ASW-5
SNMPv2-MIB::sysLocation.0 = STRING: Unknown
SNMPv2-MIB::sysORID.1 = OID: SNMPv2-MIB::snmpMIB
```

IPv6 M&T – Syslog



Logging

Syslog servers

Server IP	Port	Roles	Actions
10.11.11.125	5145	<div>Flows x URLs x</div> <div>Wireless event log x</div>	x
2601:2c3:8661:b5:e255:3dfffec0:3c90:1	5145	<div>Air Marshal events x</div> <div>Flows x URLs x</div> <div>Wireless event log x</div>	x

[Add a syslog server](#)

Network-wide -> General

Wireless network
only option (for now)

Sample
Output

```
Dec 30 16:10:16 2601:2c3:8661:b5:e255:3dfffec0:3c90:1 1609366217.028192575  
KIAH_IPV6ONLY_MR52 airmarshal_events type=rogue_ssid_detected ssid=""  
bssid='DE:CB:AC:B9:73:1F' src='DE:CB:AC:B9:73:1F' dst='FF:FF:FF:FF:FF:FF'  
wired_mac='E0:CB:BC:B9:73:1F' vlan_id='25600' channel='161' rssi='23' fc_type='0' fc_subtype='8'
```


IPv6 M&T – MR Scanning API



Location and scanning ⓘ

Analytics

Scanning API

Validator ⓘ

Post URLs ⓘ

Status ⓘ	Post URL	Secret	API Version	Radio Type		
●	<input type="text" value="https://location.dnspaces.io/notifications/Meraki/jeffryhai"/>	<input type="text"/> Show secret	V3 (beta) <input type="button" value="v"/>	WiFi <input type="button" value="v"/>	<input type="button" value="Validate"/>	<input type="button" value="X"/>
●	<input type="text" value="https://location.dnspaces.io/notifications/Meraki/jeffryhai"/>	<input type="text"/> Show secret	V3 (beta) <input type="button" value="v"/>	Bluetooth <input type="button" value="v"/>	<input type="button" value="Validate"/>	<input type="button" value="X"/>
●	<input type="text" value="https://macdb.uk/jehandal/events.php"/>	<input type="text"/> Show secret	V2 <input type="button" value="v"/>	Bluetooth <input type="button" value="v"/>	<input type="button" value="Validate"/>	<input type="button" value="X"/>
●	<input type="text" value="https://macdb.uk/jehandal/events.php"/>	<input type="text"/> Show secret	V2 <input type="button" value="v"/>	WiFi <input type="button" value="v"/>	<input type="button" value="Validate"/>	<input type="button" value="X"/>

[Add a Post URL](#)

Network-wide -> General

Sample
Output

```
"seenTime":"2018-01-06T06:02:45Z", "ssid":"NAT64", "os":null, "clientMac":"40:4e:36:89:fc:5b", "seenEpoch":1515218565, "rssi":48, "ipv6":"/2601:2c3:887f:5f73::c6b6:69c3:116c:d670", "manufacturer":"HTC"]}]}}
```

IPv6 Security



Product Family	Access Control List	RA Guard	DHCPv6 Guard	802.1x	LSP Access
MR	Yes	Yes ¹	Beta	Yes	Yes
MS	Yes	No	Partial ²	Yes	Yes

¹ RA guard on by default.

² “DHCPv6 guard” via ACL for now.

IPv6 Security – MS ACLs and FHS

- “Manual” First Hop Security (FHS) for DHCPv6 only
- Centralized for all switches in network

User-defined rules

	#	Policy	IP Version	Protocol	Source	Src port	Destination	Dst port	Vlan	Comment	
II	1	Deny ▾	IPv6 ▾	UDP ▾	Any	547	Any	546	Any	Block DHCPv6	✕
II	2	Deny ▾	IPv6 ▾	Any ▾	Any	Any	2607:f2f8:ab30::2/128	Any	Any	Block jeffryh	✕
		Allow	Any	Any	Any	Any	Any	Any	Any	Default rule	

Block DHCPv6

Switch -> ACL

IPv6 Security – MR ACLs and FHS

Learn more about FHP:
[BRKENT-3002](#)

RA Guard on by default!

Block IPs and ports

Layer 2 LAN isolation Disabled (bridge mode only)

DHCP guard Disabled

RA guard Enabled

RA allowed routers
one IP6 address per line

Wireless ->
Firewall & traffic
shaping

Outbound rules



Search...

Add new

<input type="checkbox"/>	#	Policy	IP Version	Protocol	Destination	Dst port	Rule description	Actions
II	<input type="checkbox"/>	1 Deny	IPv6	ICMPv4	2a03:2880:f134:183:face:b00c:0:25de/128	Any	FACEBOOK PING BLOCK	...
II	<input type="checkbox"/>	2 Deny	IPv6	TCP	2a03:2880::/29	Any	FACEBOOK ALL BLOCK	...

IPv6 Security – 802.1x



MS

Switch -> Access policies

Access policies

Name: RADIUSv6

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions
1	2600:1f18:44c:bb10	9173	*****	Test

[Add a server](#)

RADIUS testing: RADIUS testing enabled

RADIUS CoA support: RADIUS CoA disabled

RADIUS accounting: RADIUS accounting enabled

RADIUS accounting servers

#	Host	Port	Secret
1	2600:1f18:44c:bb10	9173	*****

[Add a server](#)

Host Mode: Single-Host

Access policy type: 802.1x

Guest VLAN:

Voice VLAN clients: Bypass authentication

Completed testing to "2600:1f18:44c:bb10:1::1:9173 for miles"

Total switches: 1
Switches passed: 1
Switches failed: 0
Switches unreachable: 0

All switches successfully contacted the RADIUS

MR

Completed testing to "2600:1f18:44c:bb10:1::1:9173 for miles"

Total APs: 3
APs passed: 1
APs failed: 0
APs unreachable: 2

All online access points successfully contacted the RADIUS server, however 2 access points were offline and could not be tested.

RADIUS attributes used:

RADIUS attributes unused:
User-Name:miles
cisco-avpair:cts:security-group-tag=0002-00

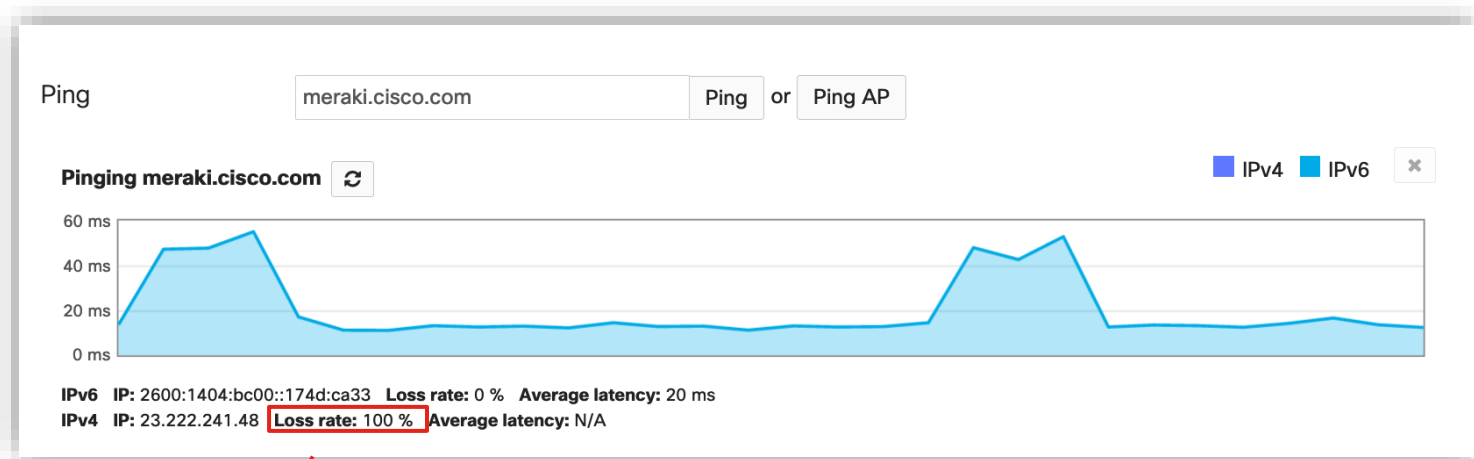
[Retry](#) or [close](#)

Wireless -> Access control

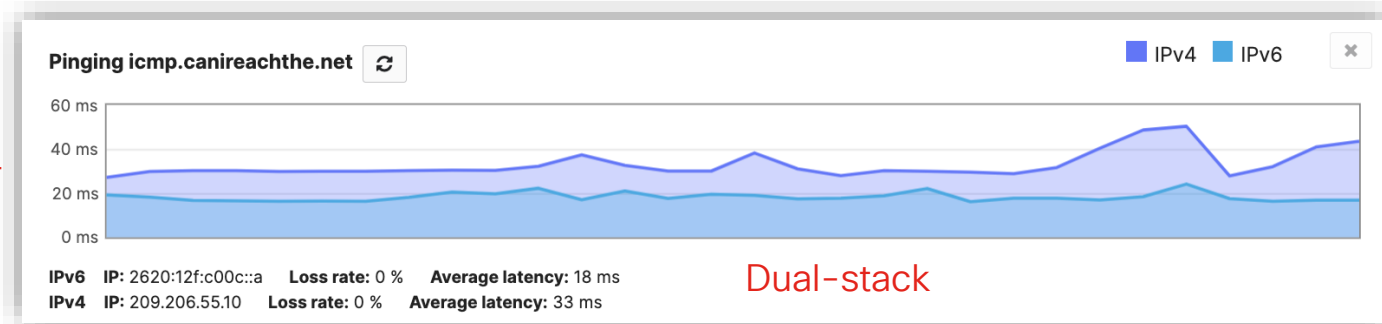
IPv6 Dashboard Tools

Product Family	Ping	Traceroute	MTR
MR	Yes	Yes	N/A
MS	Yes	N/A	Yes

IPv6 Dashboard Tools – Ping



Due to the nature
of NAT64 when using IPv4
instead of DNS name



Dual-stack

Demo

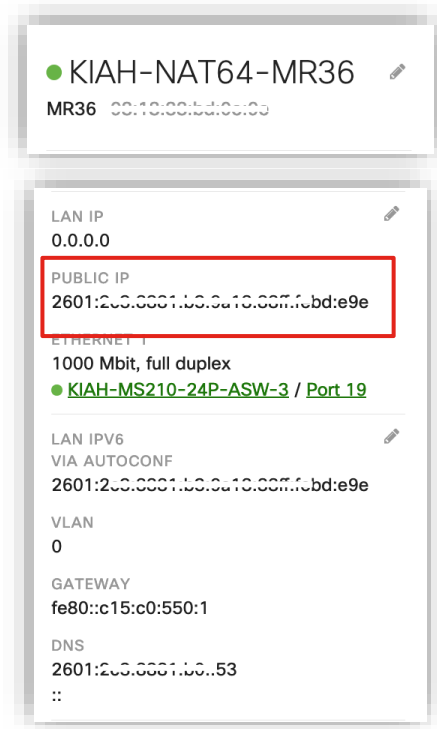
Is IPv6-only
management with
Cisco Meraki possible?



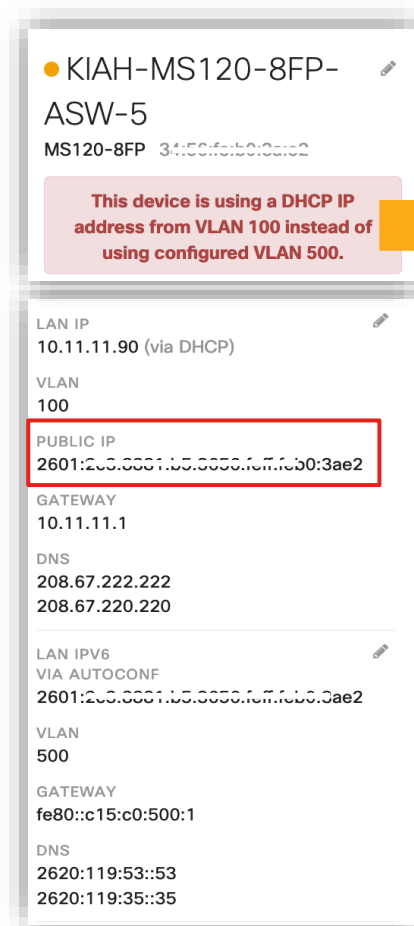
YES!

IPv6-Only Management

MR



MS

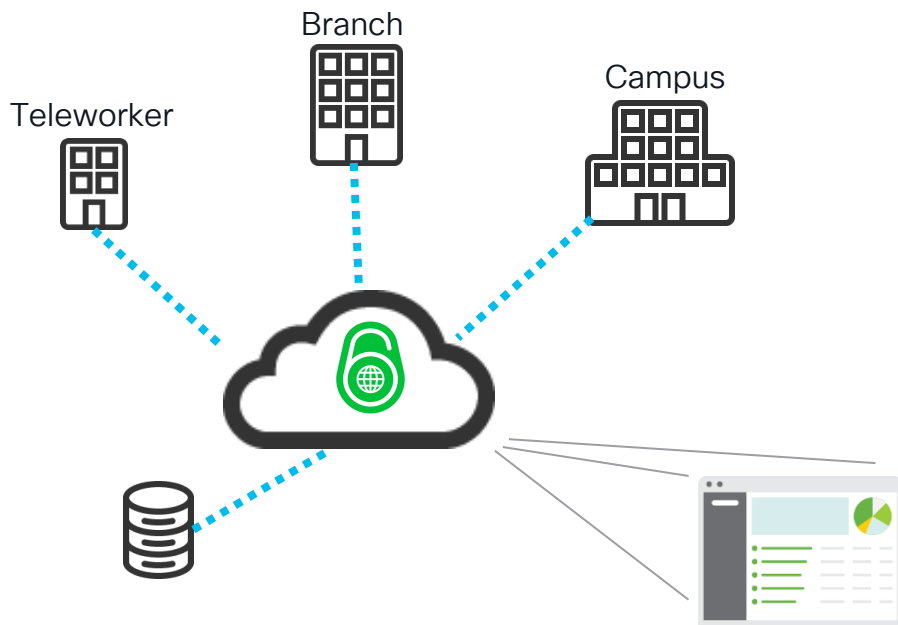


To be corrected soon.
Still seeks an IPv4 address, but it does not use it to communicate to dashboard.

The Future of the Enterprise



A v6-Centric Future



Cisco-routing Meraki-access deliver the ability to:

- Manage your network over IPv6-only.
- Allow client traffic to reach the entire Internet.

With a touch of simpler operations.

Cisco: Your Companion on the Journey to IPv6

What will happen when we enable IPv6 at the enterprise?



A new universe opens up!

Resources

- [Monitor IPv6 Adoption \(Cisco\)](#)
- [Umbrella IPv6 DNS Servers](#)
- [Cisco Meraki Community on IPv6](#)
- [Cisco Press: IPv6 for Enterprise Networks](#)

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



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive