airheads TECH TALK LIVE

aruba
a Hewlett Packard Enterprise company

Aruba and IPv6

Joe Neville

Sept 19

#ArubaAirheads

Agenda

Do we still need IPv6

IPv6 Crash Course

Watch out for…

Aruba & IPv6

Do we still need IPv6?

- World IPv6 Day 06 June 2012
  - IPv4 address exhaustion headlines have been and gone
- But we still all use IPv4
- Major tech companies (twitter) don't have IPv6
- "No one cares about IPv6" - a guy in Sweden Oct 2018
- My IPv6 videos were youtube kryptonite – lowest views on the channel

Explain this

– My mum watches youtube over IPv6

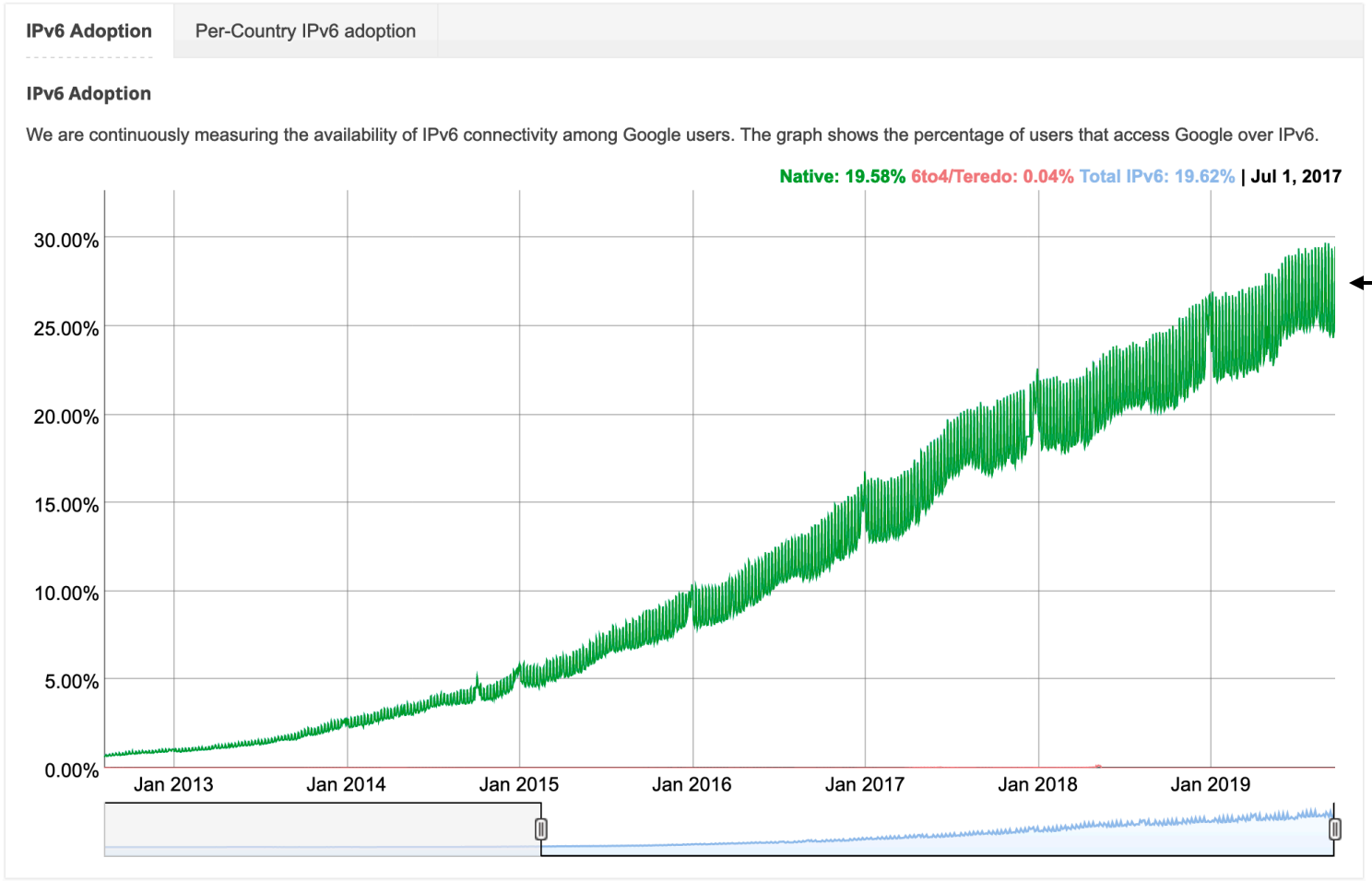
– MSFT tells gamers that IPv6 is preferable over IPv4

What if my Xbox One isn't connected using IPv6?

Your Xbox will work normally without IPv6 connectivity. However, for the best possible experience, we recommend enabling IPv6 on your network. Several Xbox One features already make use of IPv6, and we're building more.

– T-Mobile US is IPv6 only

Lies, damn lies, and statistics



Just shy of 30%

“Livin’ in an IPv6 world”

“Yeah, but that’s not my network!”

–IPv6 in the wild:
  – Home
  – Cloud
  – Mobile
  – Service Provider
  – Content Provider

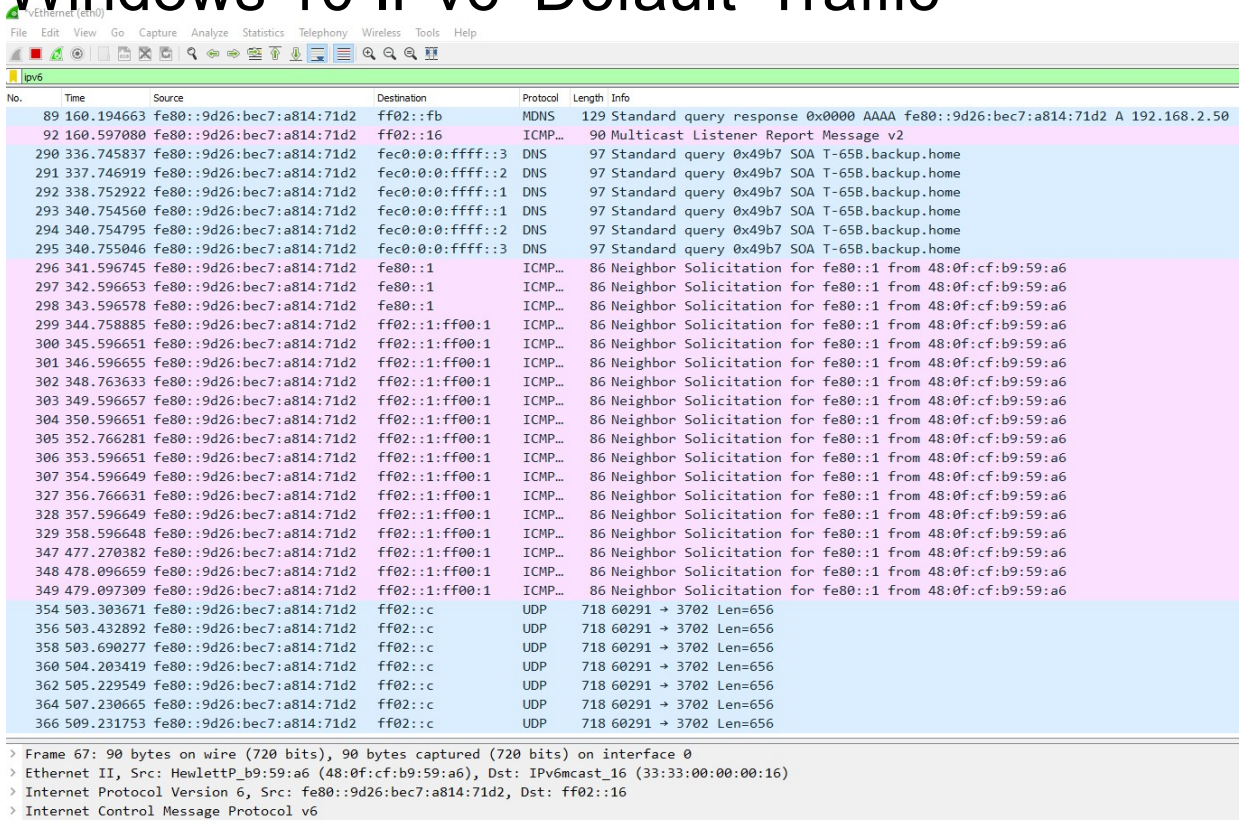
“Yeah but that’s not my network!”

–Don’t be so sure!

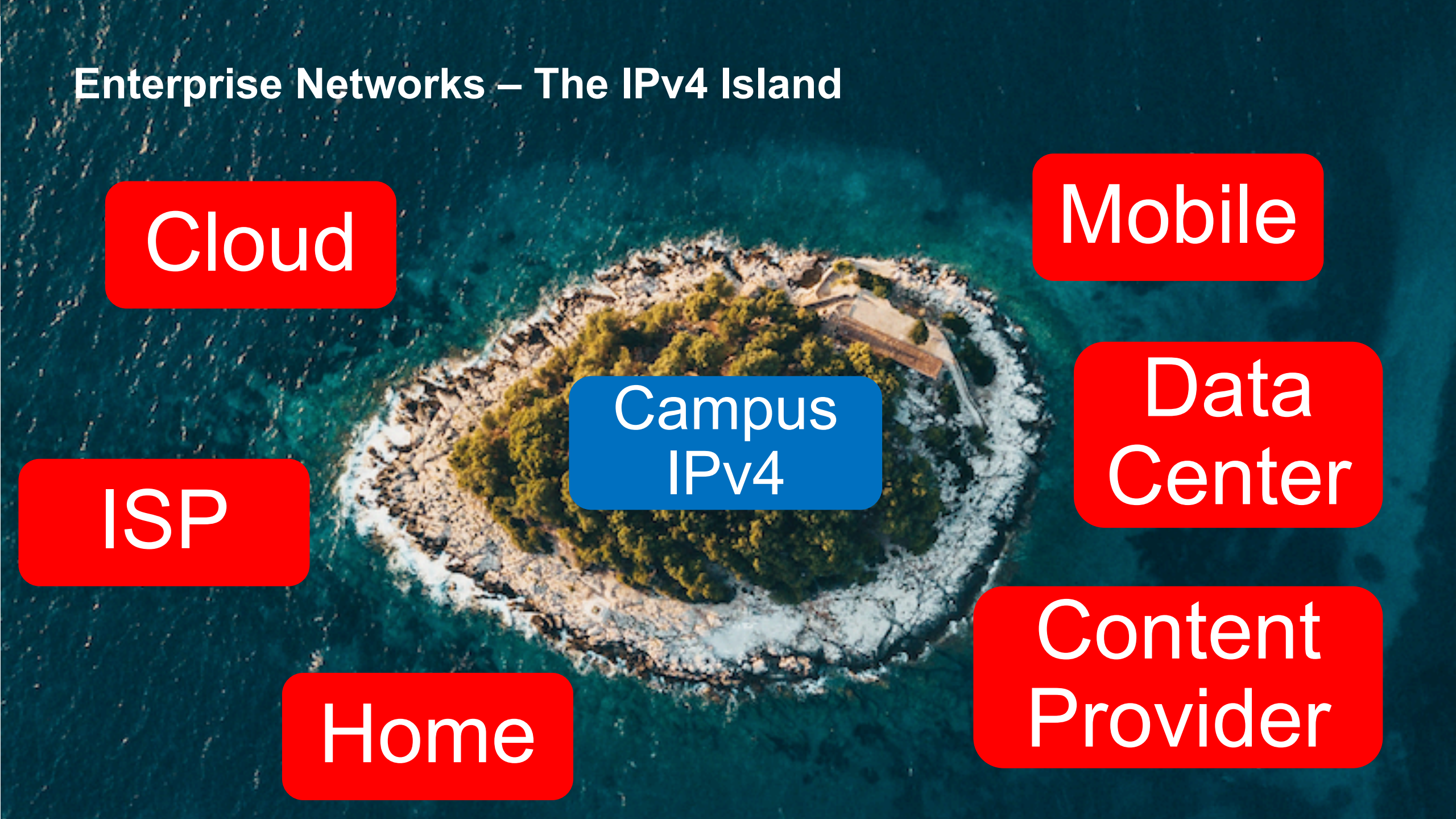
– IPv6 has been the preferred protocol in Windows since Vista.

– There are no IPv4 only networks, you have v6 traffic, you just aren't aware.

Windows 10 IPv6 ‘Default’ Traffic



Enterprise Networks – The IPv4 Island

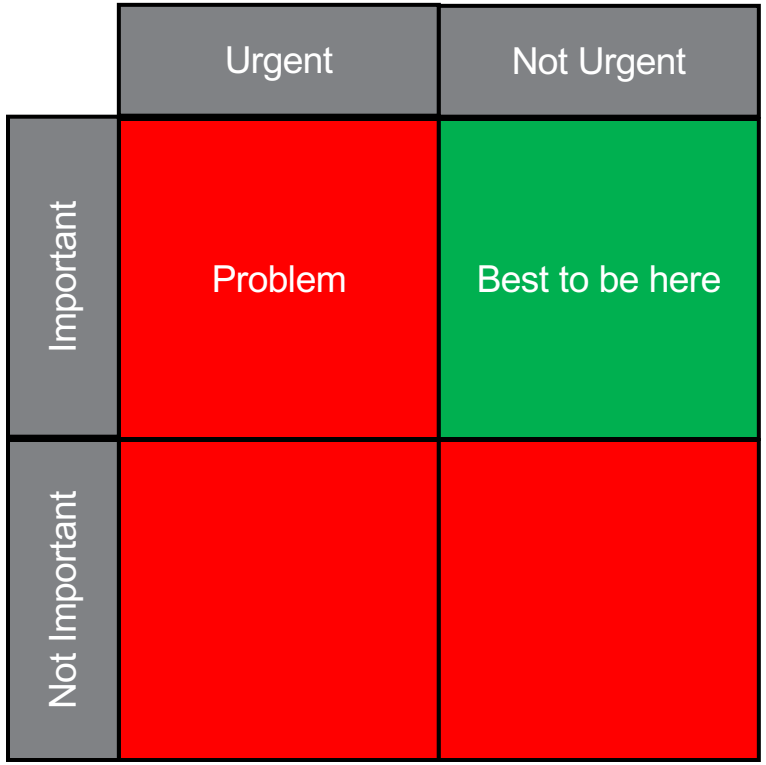


IPv6 Is Unevenly Distributed

- ‘Early’ Adopters:
  - V Large Scale – facing RFC1918 exhaustion
  - Universities – Students need the latest technology in CS Dept, rolls out across campus
  - Industrial – car industry & anyone dealing with IoT at all!

  - This is changing – ***many*** more requests inbound
  - Companies needing to formulate an IPv6 strategy
  - MSFT IPv6 Corp Network project – provides a use case

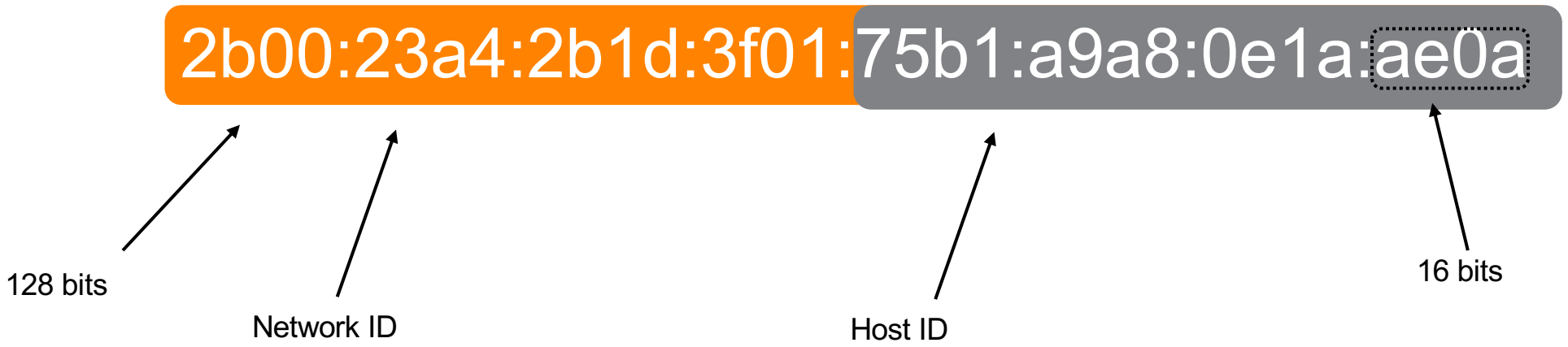
Best time to get into IPv6 is yesterday



- **Companies**
  - Still benefit from being late adopter (let others work out bugs)
  - That time is coming to an end
  - Certain industries no benefit because must be active (cloud, IoT)
- **Engineers**
  - No benefit in waiting
  - Increased demand, shortage of skills, higher salary offers (usually).

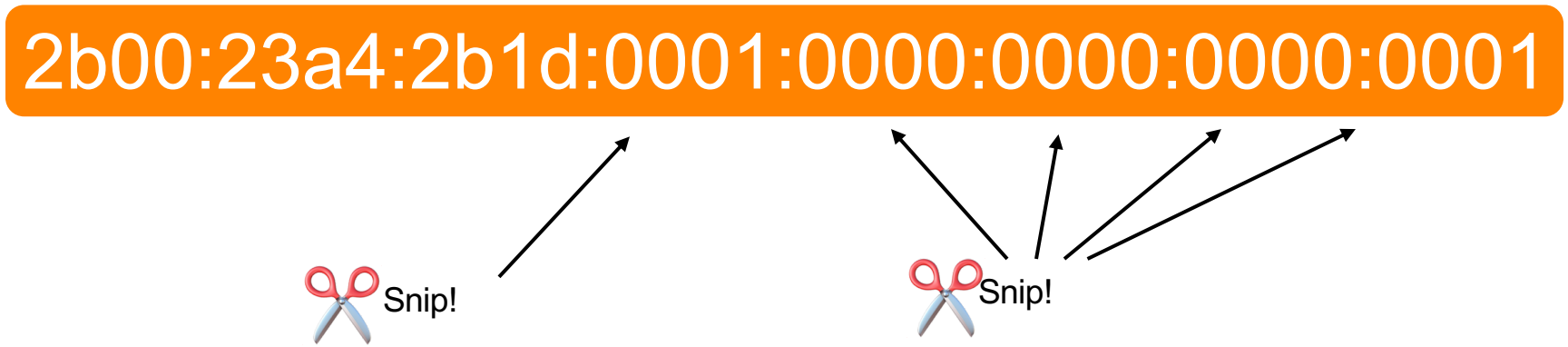
IPv6 Crash Course

– 128-bits of address space vs. 32 for IPv4



IPv6 Crash Course

– Leading zeros and all zero 16-bits can be abbreviated:



IPv6 Crash Course

– Leading zeros and all zero 16-bits can be abbreviated:

2b00:23a4:2b1d:1::1

Not so ugly!

IPv6 Crash Course

– Address planning is very different:

– /64 is the LAN subnet, required for SLAAC

– That's 18,446,744,073,709,551,616 IPv6 addresses per interface!

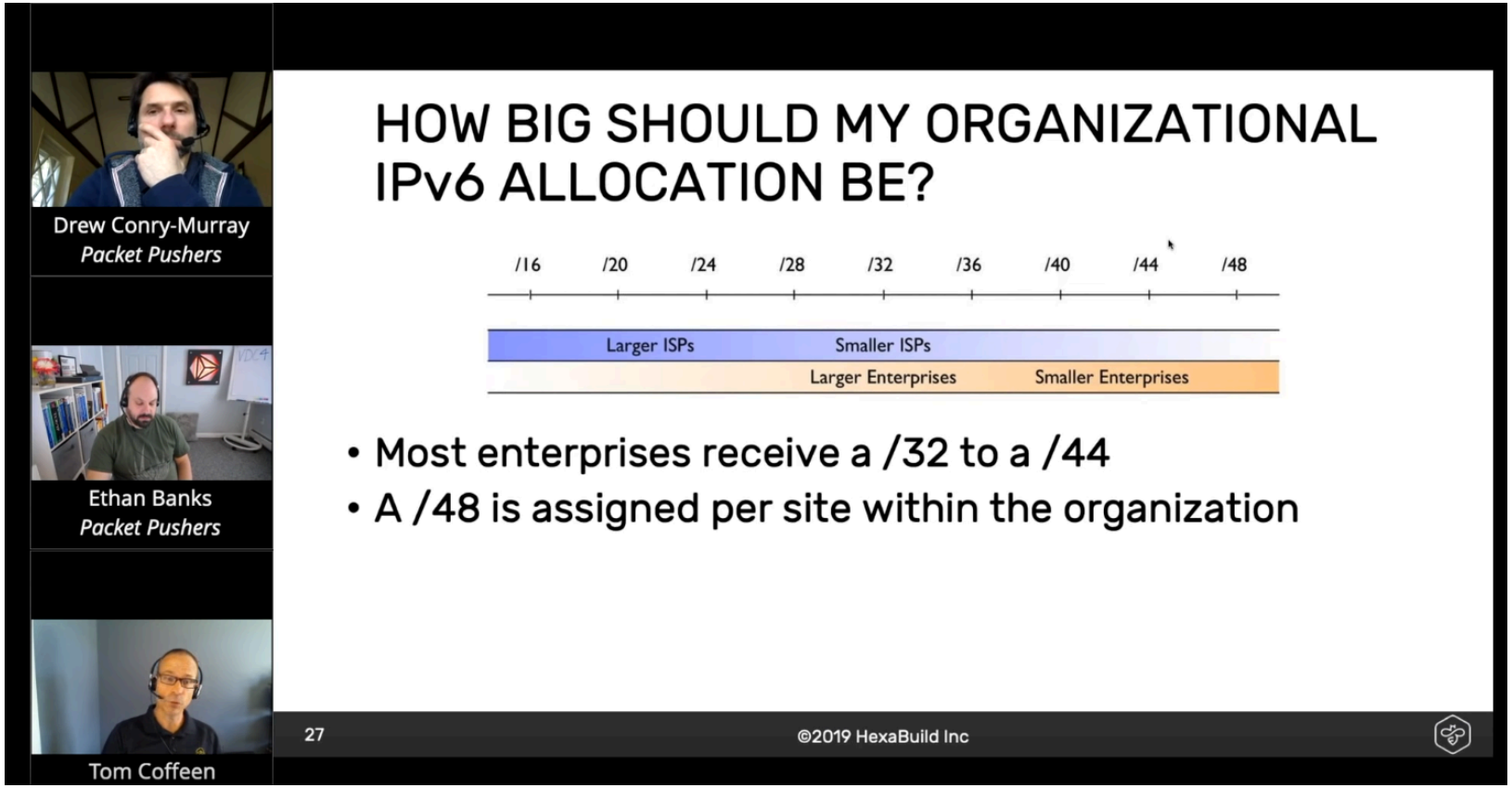
IPv4 World

IPv6 World

IPv6 Crash Course

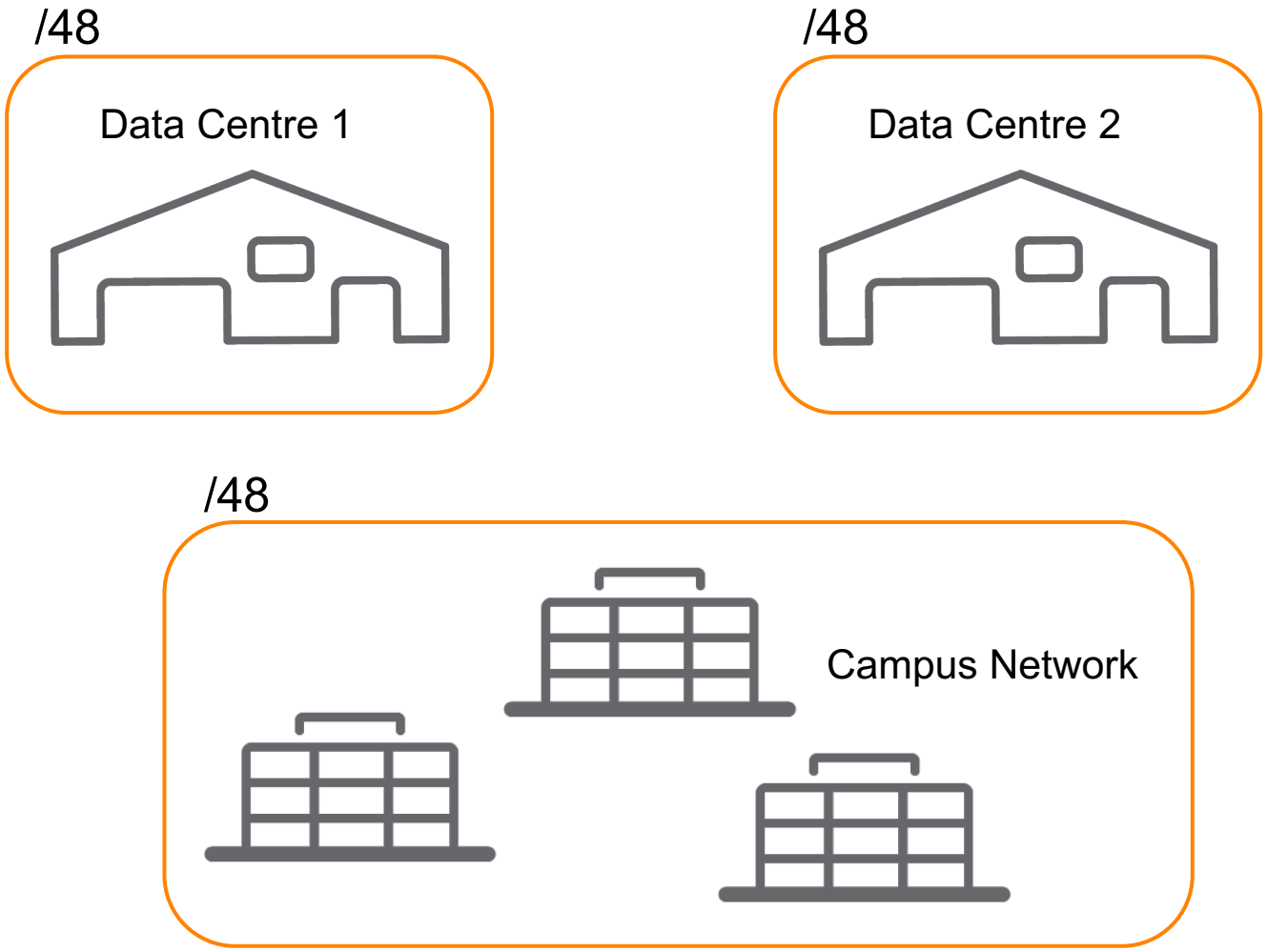
https://www.youtube.com/watch?v=fuGe7P-LsuQ

- Recommendation is to **GO BIG!**
- Home networks have a /56 (256 subnets)
- Small enterprise = /40 - /48
- /48 = 65,536 LANs!



IPv6 Crash Course

- Assign a /48 per site
- Site being a logical entity in your network.

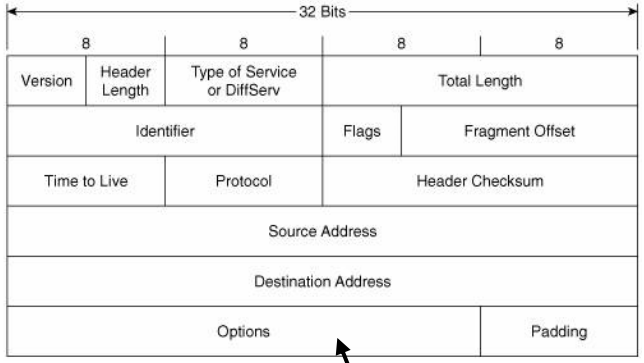


IPv6 Crash Course

More major differences:

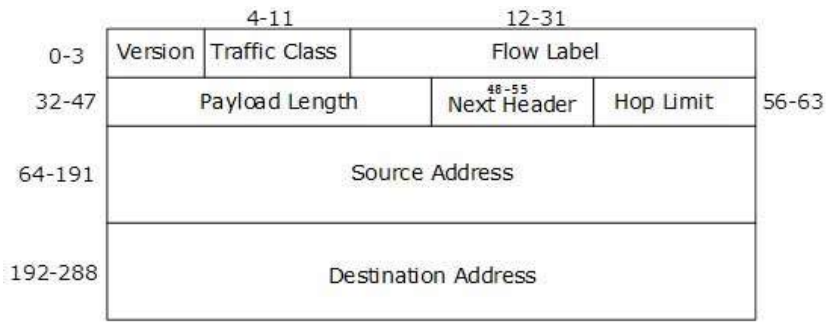
– All-new header

IPv4: 20 – 60 bytes



What is this anyway?

IPv6 – fixed 40 bytes



IPv6 Crash Course

More major differences:

– Extension Headers

Extension Header	Type	Description
Hop-by-Hop Options	0	Options that need to be examined by all devices on the path.
Destination Options (before routing header)	60	Options that need to be examined only by the destination of the packet.
Routing	43	Methods to specify the route for a datagram (used with Mobile IPv6).
Fragment	44	Contains parameters for fragmentation of datagrams.
Authentication Header (AH)	51	Contains information used to verify the authenticity of most parts of the packet.
Encapsulating Security Payload (ESP)	50	Carries encrypted data for secure communication.
Destination Options (before upper-layer header)	60	Options that need to be examined only by the destination of the packet.
Mobility (currently without upper-layer header)	135	Parameters used with Mobile IPv6.
Host Identity Protocol	139	Used for Host Identity Protocol version 2 (HIPv2).[11]
Shim6 Protocol	140	Used for Shim6.[12]
Reserved	253	Used for experimentation and testing.[13][4]
Reserved	254	Used for experimentation and testing.[13][4]

Source: https://en.wikipedia.org/wiki/IPv6_packet

IPv6 Crash Course

More major differences:

– No more ARP!

– Neighbor Discovery Protocol

Router Solicitation (Type 133)

Hosts inquire with Router Solicitation messages to locate routers on an attached link.[3] Routers which forward packets not addressed to them generate Router Advertisements immediately upon receipt of this message rather than at their next scheduled time.

Router Advertisement (Type 134)

Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message.

Neighbor Solicitation (Type 135)

Neighbor solicitations are used by nodes to determine the link layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link layer address.

Neighbor Advertisement (Type 136)

Neighbor advertisements are used by nodes to respond to a Neighbor Solicitation message.

Redirect (Type 137)

Routers may inform hosts of a better first hop router for a destination.

Source: https://en.wikipedia.org/wiki/Neighbor_Discovery_Protocol

IPv6 Crash Course

More major differences:

– Forget 1 interface = 1 address

– Multiple addresses per interface are encouraged!

  – Link-local

  – Global Unicast

  – Privacy Extensions

  – ULA (?)

IPv6 - Four to remember

Key points:

1. Address Allocation
2. WLAN IPv6 Deployment
3. Dual-stack hardware exhaustion
4. First Hop Security

1. IPv6 Address Allocation – Many Moving Parts

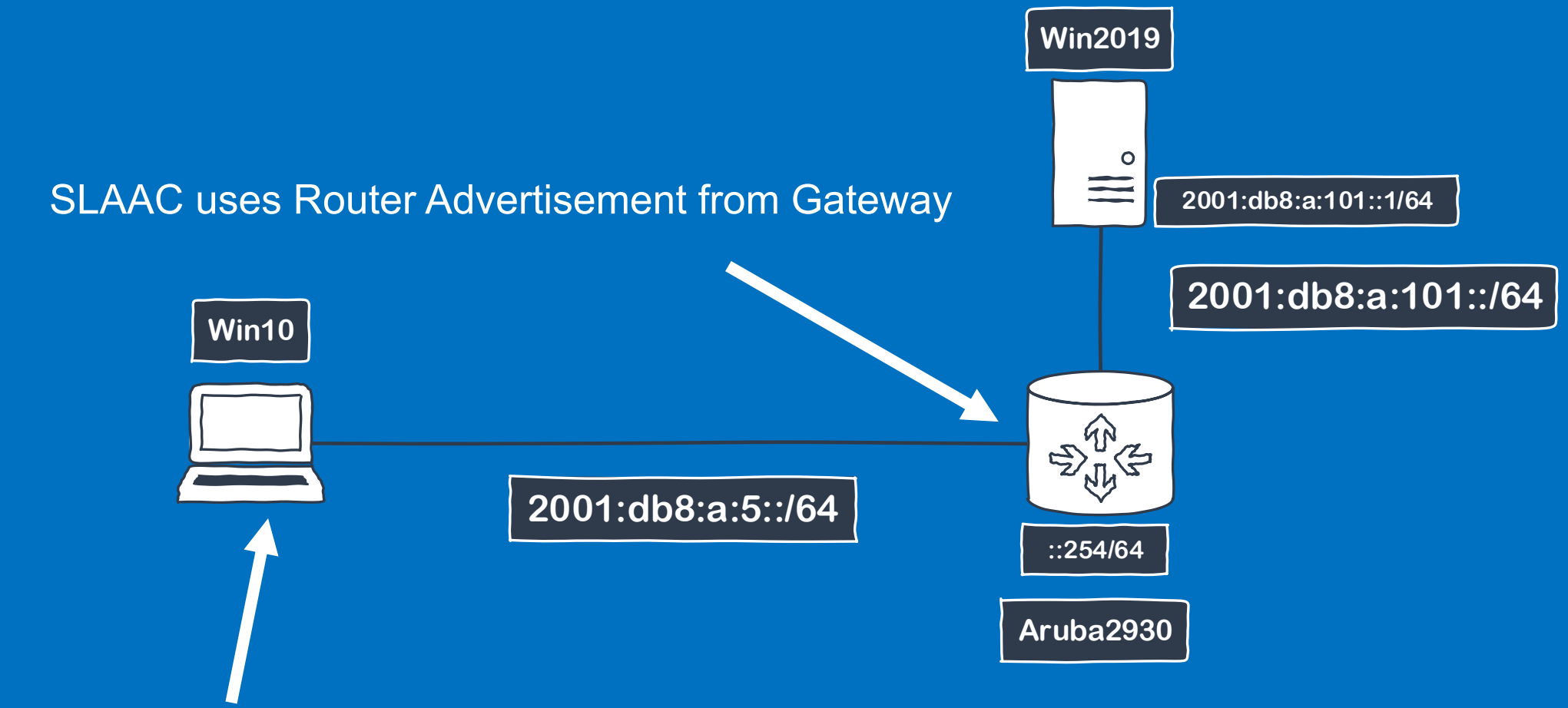
IPv4:

1. Static & DHCPv4
2. DHCPv4 options contain DNS servers and Default Gateway

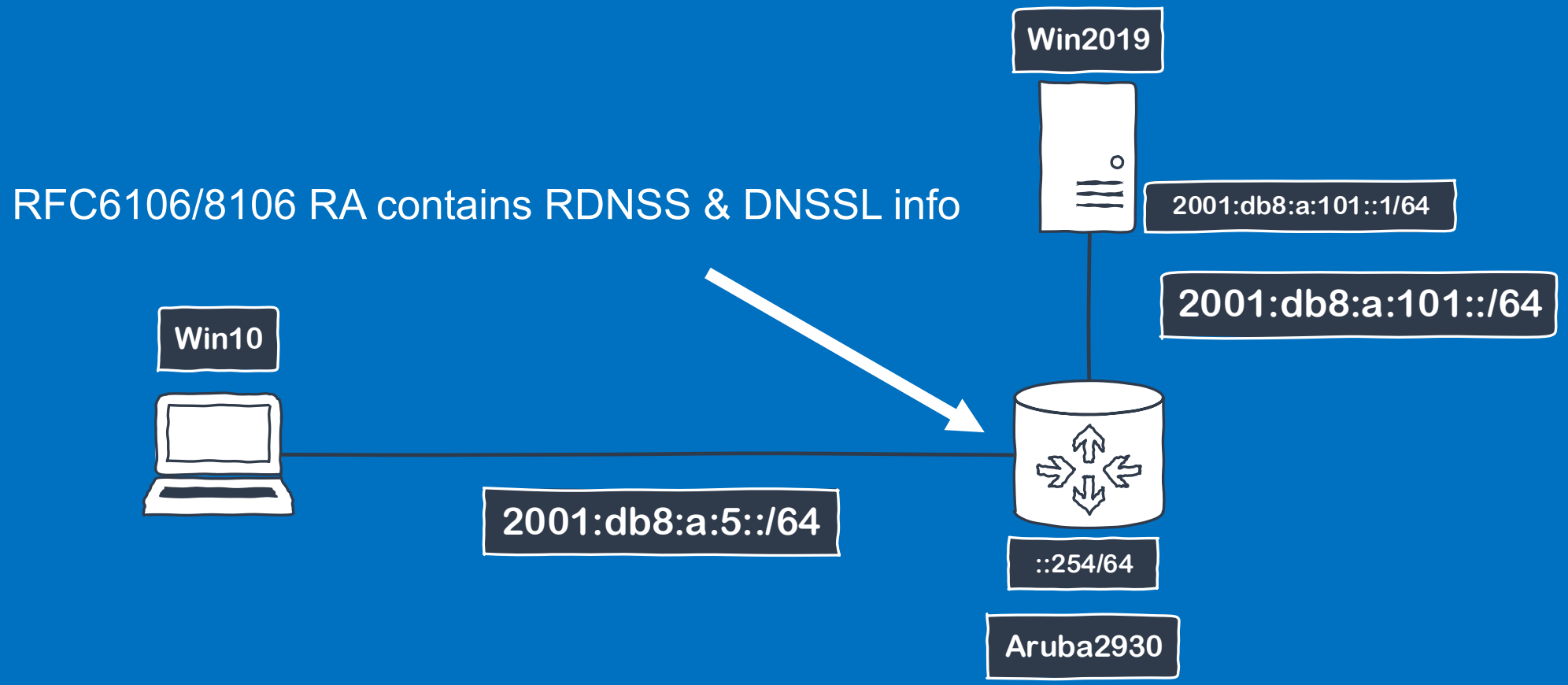
IPv6:

1. Stateless AutoConfiguration – SLAAC
2. DHCPv6 Stateful – Address and Other info (DNS)
3. DHCPv6 Stateless – Address from SLAAC, other info from DHCPv6 server
4. Static

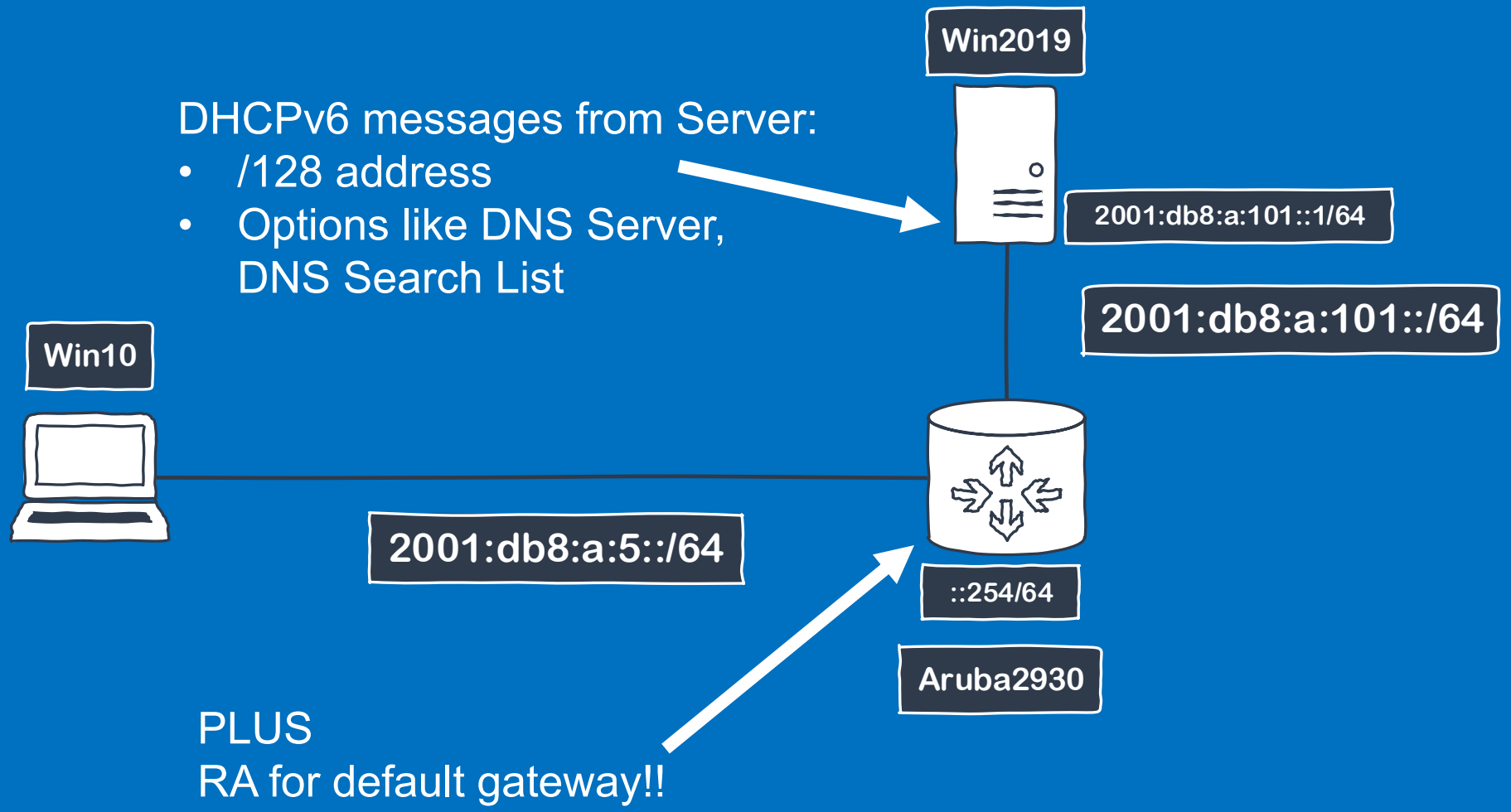
SLAAC


SLAAC uses Router Advertisement from Gateway
Win2019
2001:db8:a:101::1/64
2001:db8:a:101::/64
Win10
2001:db8:a:5::/64
::254/64
Aruba2930
Client generates the host ID 64-bits

SLAAC


RFC6106/8106 RA contains RDNSS & DNSSL info
Win2019
2001:db8:a:101::1/64
2001:db8:a:101::/64
Win10
2001:db8:a:5::/64
::254/64
Aruba2930

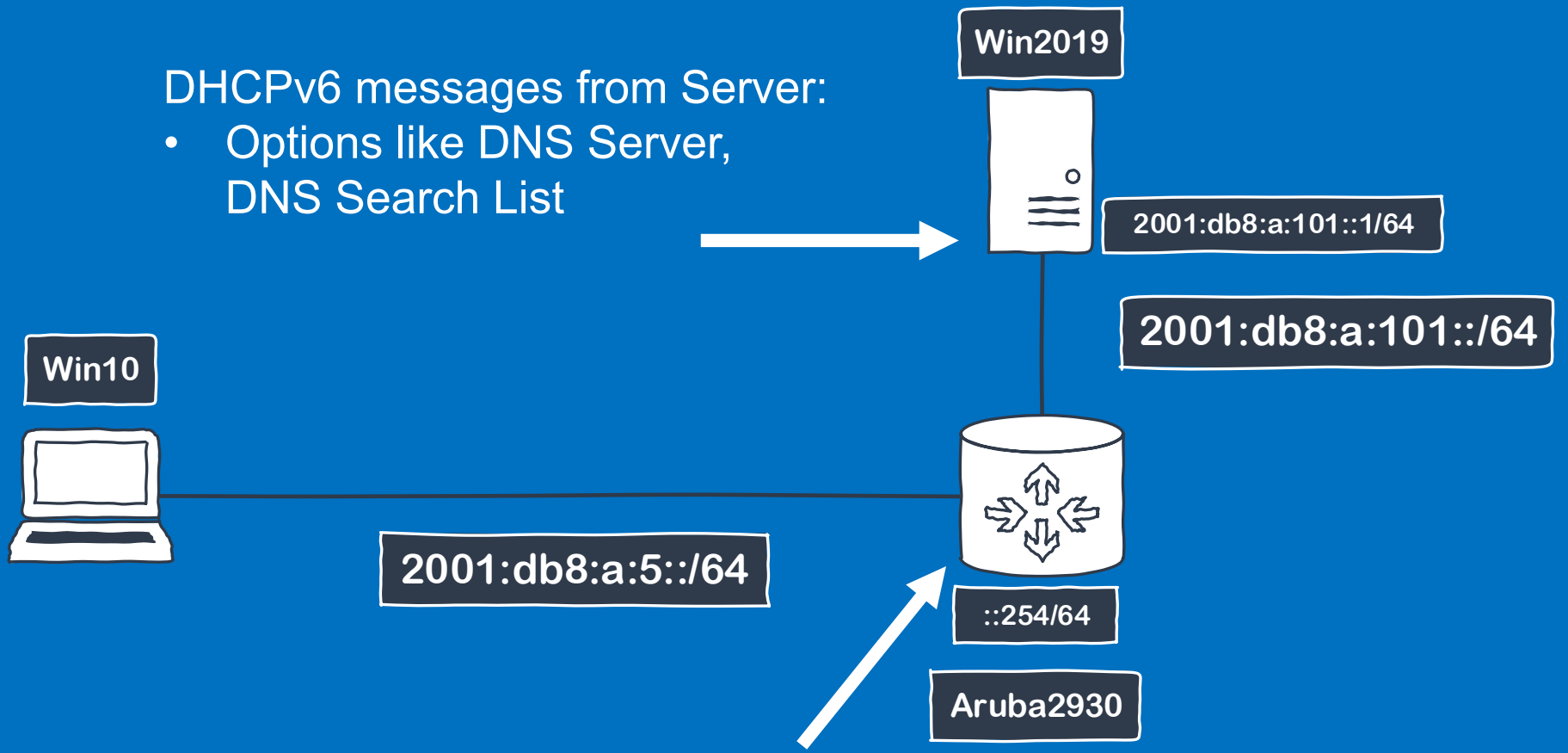
DHCPv6 Stateful



DHCPv6 Stateless

DHCPv6 messages from Server:

- Options like DNS Server, DNS Search List



2. Aruba AP Deployment & IPv6

WLAN & IPv6 Address Allocation – *Even More* Moving Parts

IPv6:

1. Stateless AutoConfiguration – SLAAC
2. DHCPv6 Stateful Address and Other info (DNS)
3. DHCPv6 Stateless – Address from SLAAC, other info from DHCPv6 server
4. Static

X

AP Controller Discovery

1. ADP
2. DNS Options
3. CAPWAP-AC-V6 Option

WLAN & IPv6 Address Allocation – *Even More* Moving Parts

Currently Supported

IPv6:

1. DHCPv6 Stateful Address and Other info (DNS)
2. DHCPv6 Stateless – Address from SLAAC, other info from DHCPv6 server

AP Controller Discovery

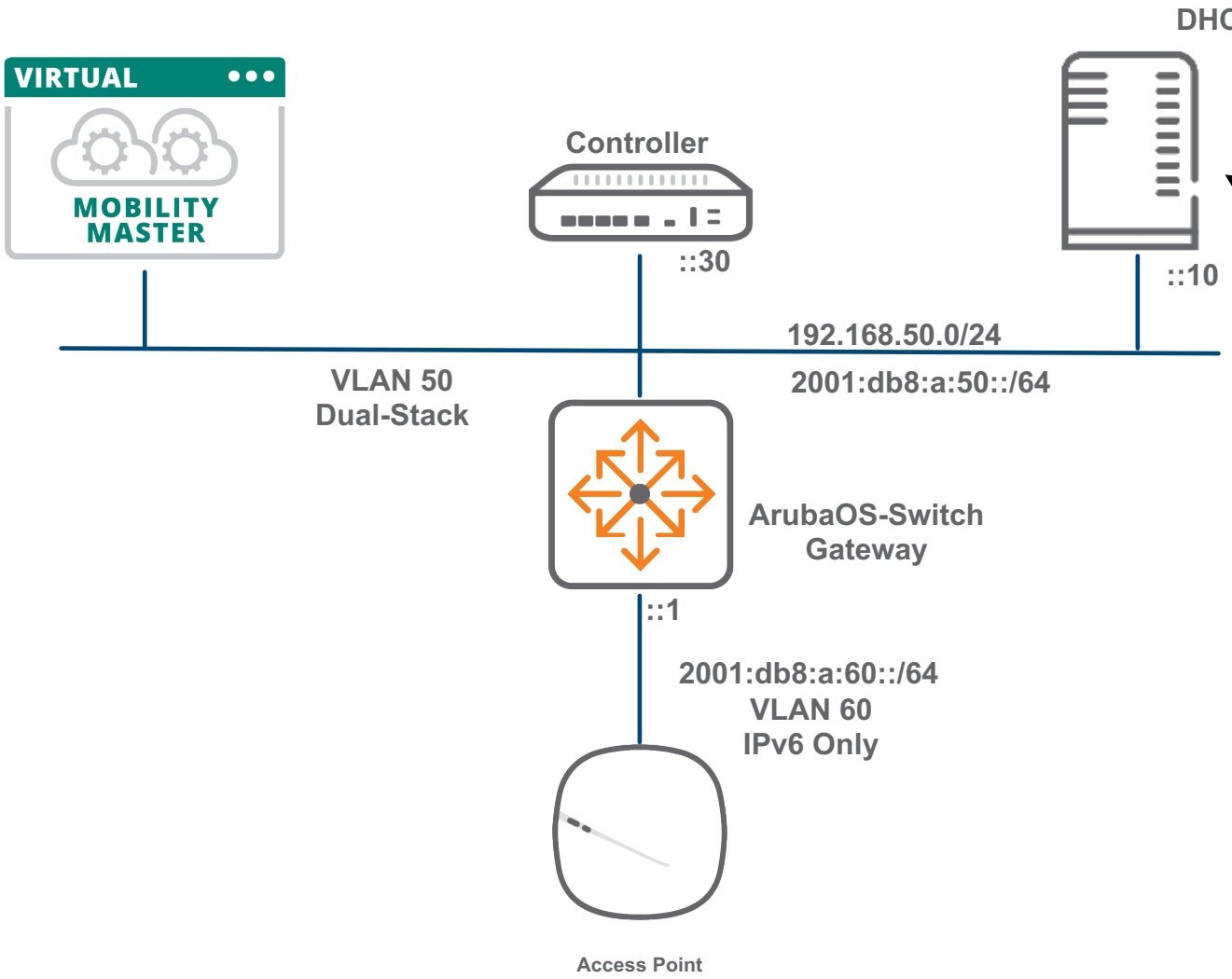
1. DNS Options
2. CAPWAP-AC-V6 Option

AP Controller Discovery Process

Requirements

- **IP Address** → To source the query traffic
- **DNS Server** → To send the aruba-master query
- **DNS Search-List** → FQDN for query
- **Controller Address** → To build IPSEC tunnel

Stateful DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



Configure DHCPv6:
- v6 address
- RDNSS & DNSSL

Configure DNS:
- AAAA for aruba-master

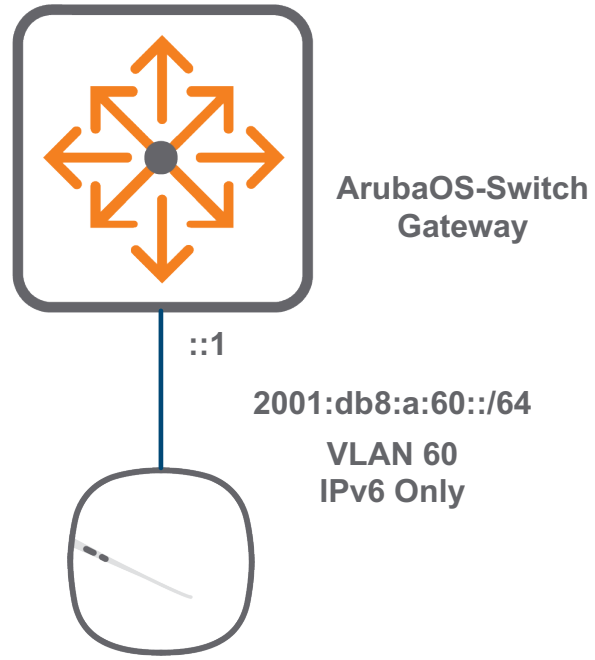
Stateful DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24 Gateway Config

```
ipv6 unicast-routing
vlan 50
  ipv6 enable
  ipv6 address fe80::1 link-local
  ipv6 address 2001:db8:a:50::1/64
  ipv6 nd ra managed-config-flag
  ipv6 nd ra prefix 2001:db8:a:50::/64 infinite no-autoconfig
  ipv6 helper-address unicast 2001:db8:a:50::1
```

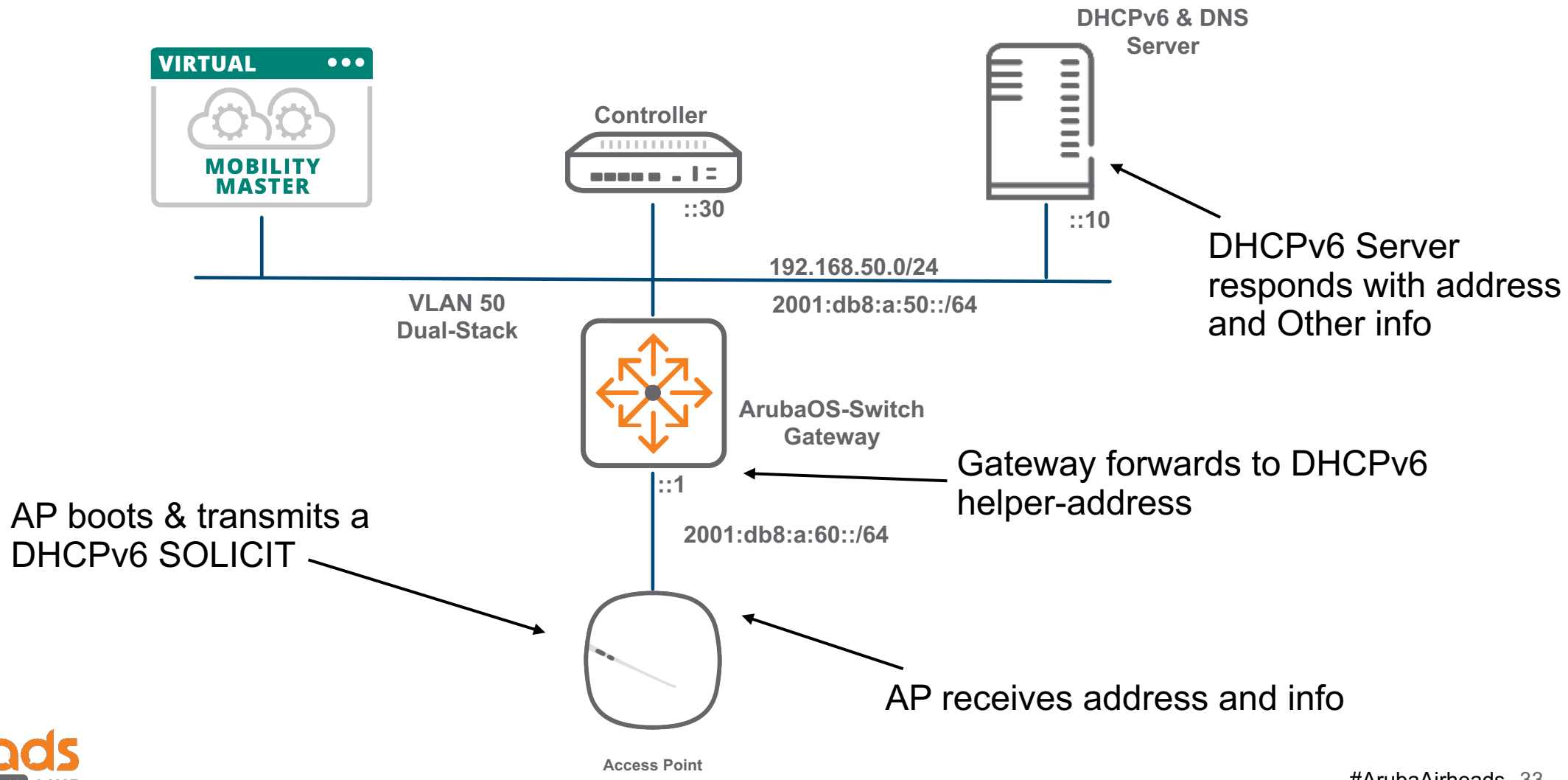
M flag set – Get Address and Other info from DHCPv6

Prefix sent with L flag on and A flag off

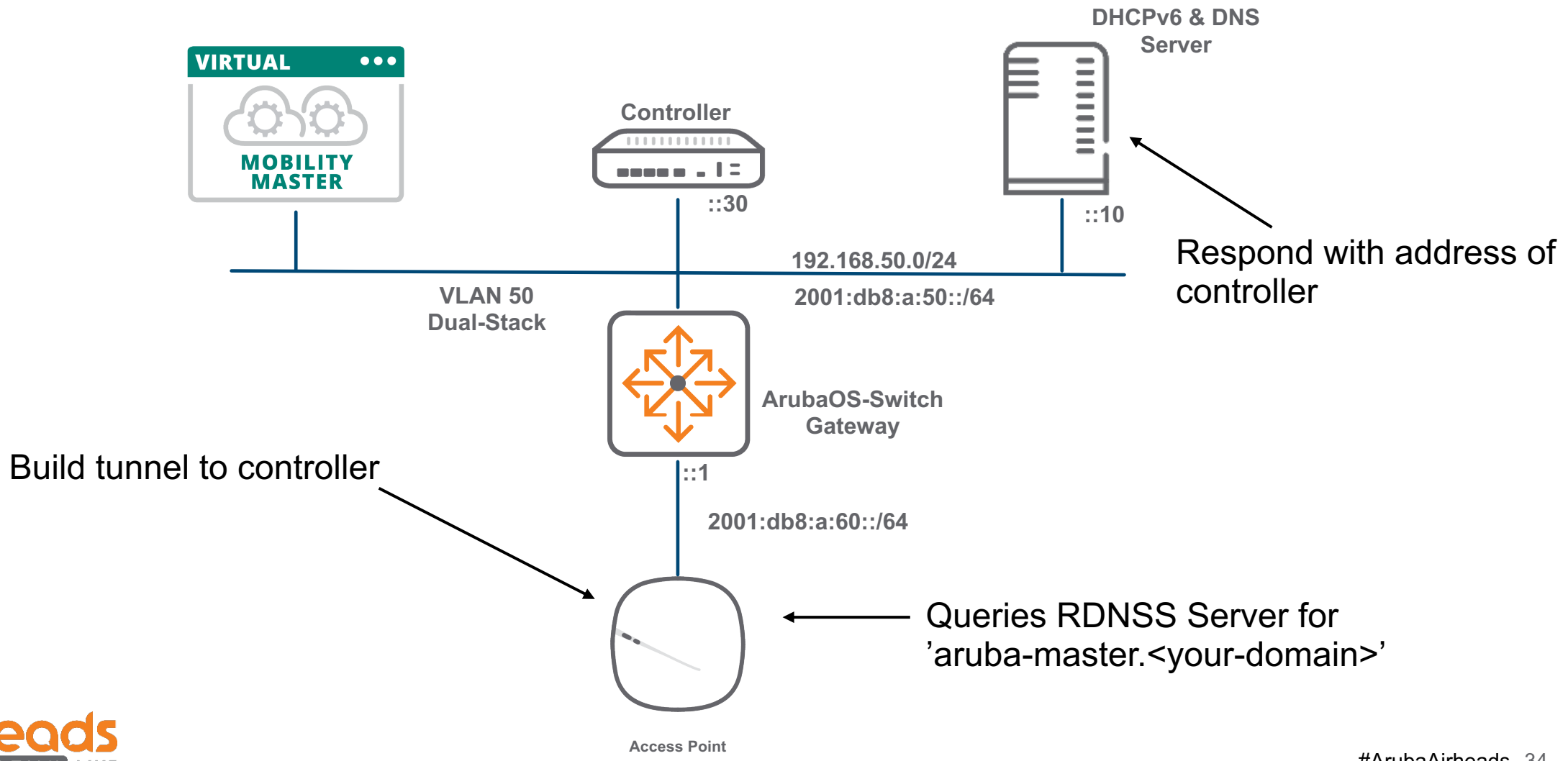
DHCPv6 helper address



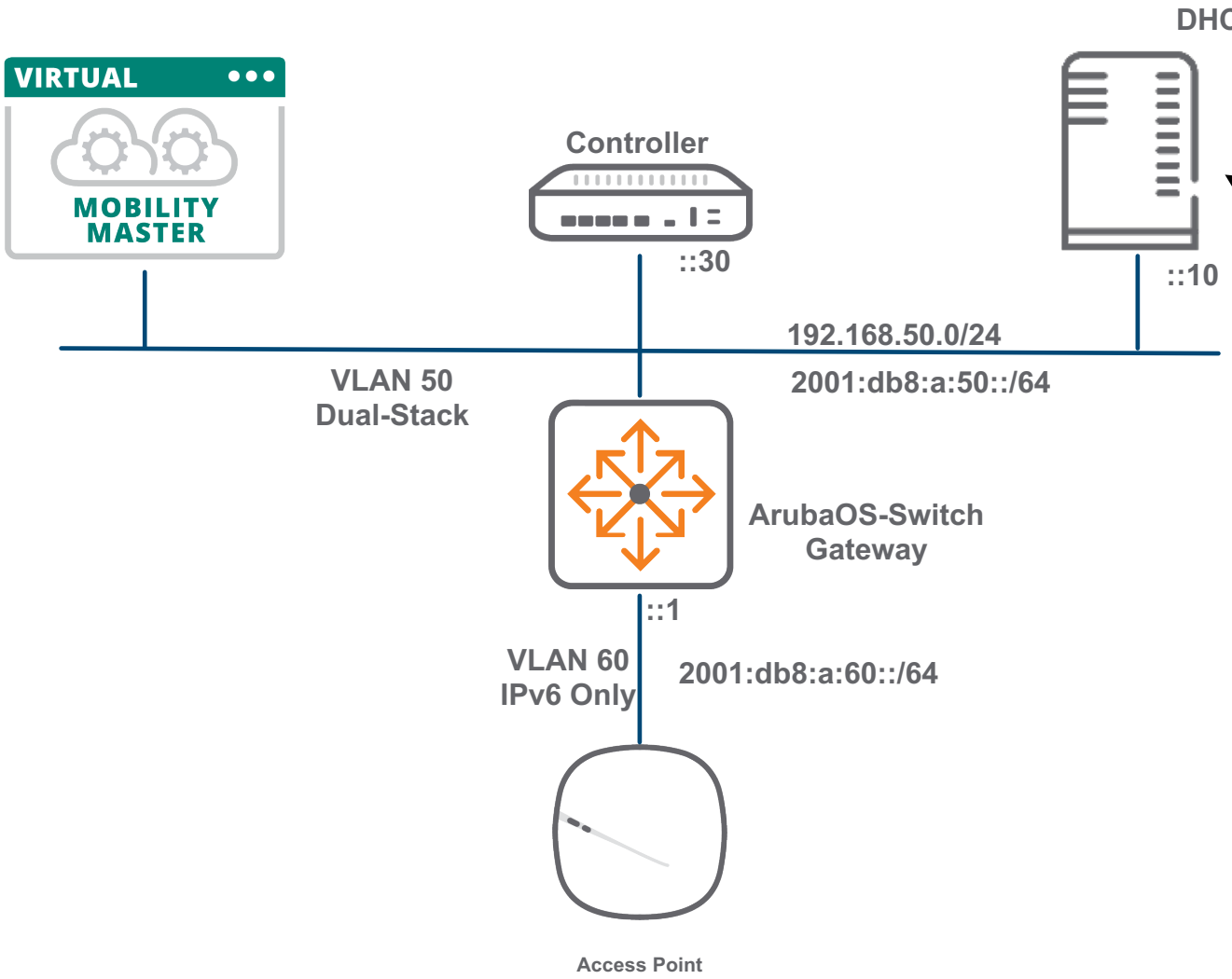
Stateful DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



Stateful DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



Stateless DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



Configure DHCPv6:

- RDNSS & DNSSL

Configure DNS:

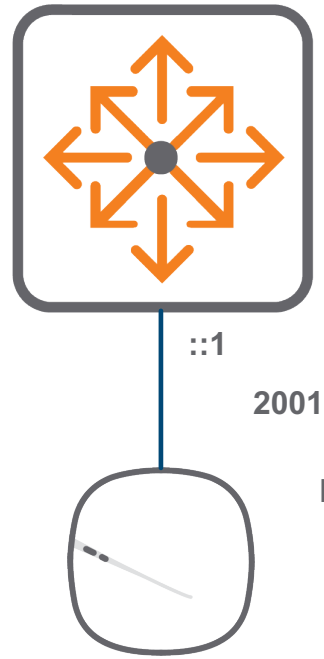
- AAAA for aruba-master

Stateless DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24 Gateway Config

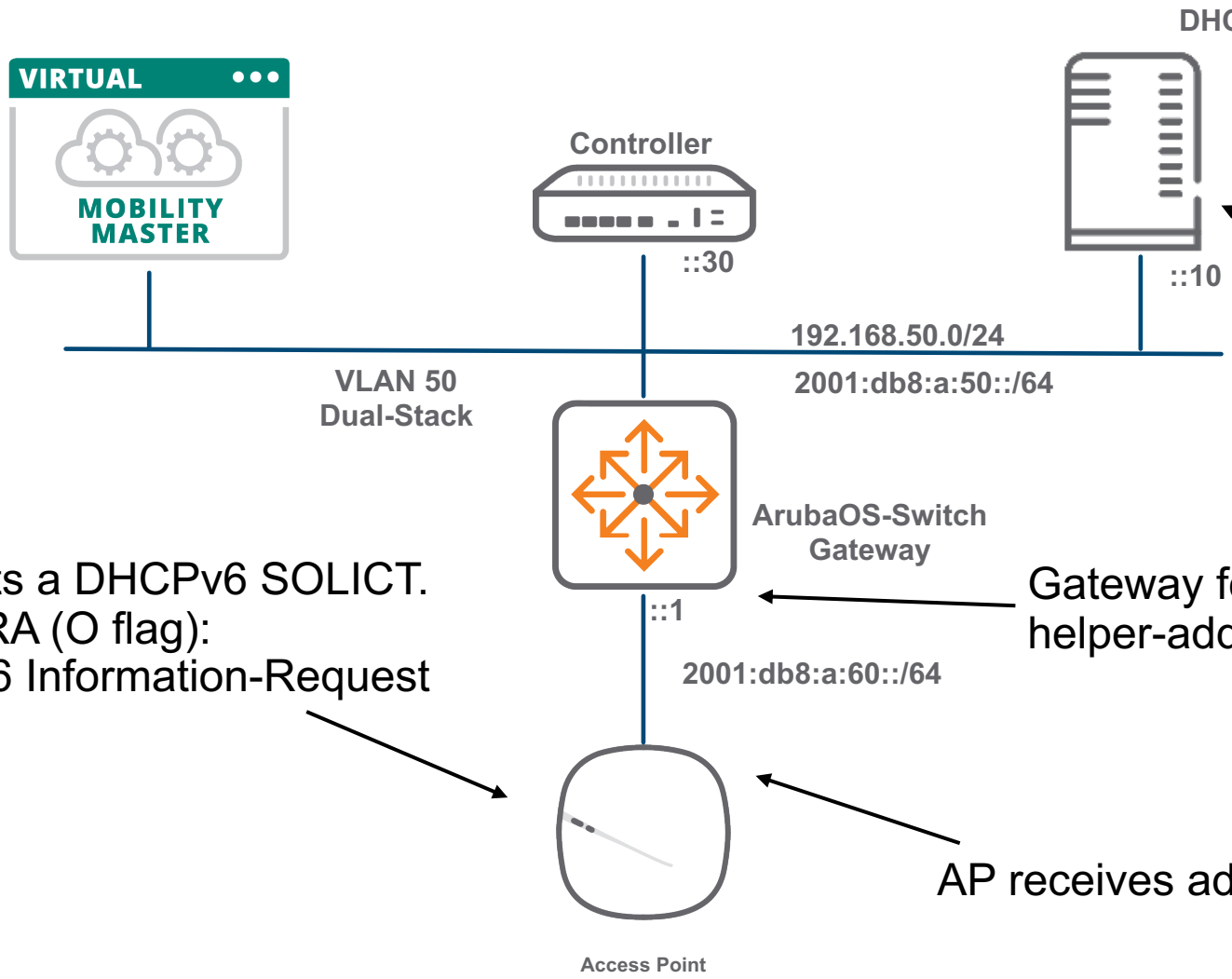
```
ipv6 unicast-routing
vlan 50
  ipv6 enable
  ipv6 address fe80::1 link-local
  ipv6 address 2001:db8:a:50::1/64
  ipv6 nd ra other-config-flag
  ipv6 helper-address unicast 2001:db8:a:50::1
```

Prefix sent with L flag on and A flag ON. /64 = SLAAC!

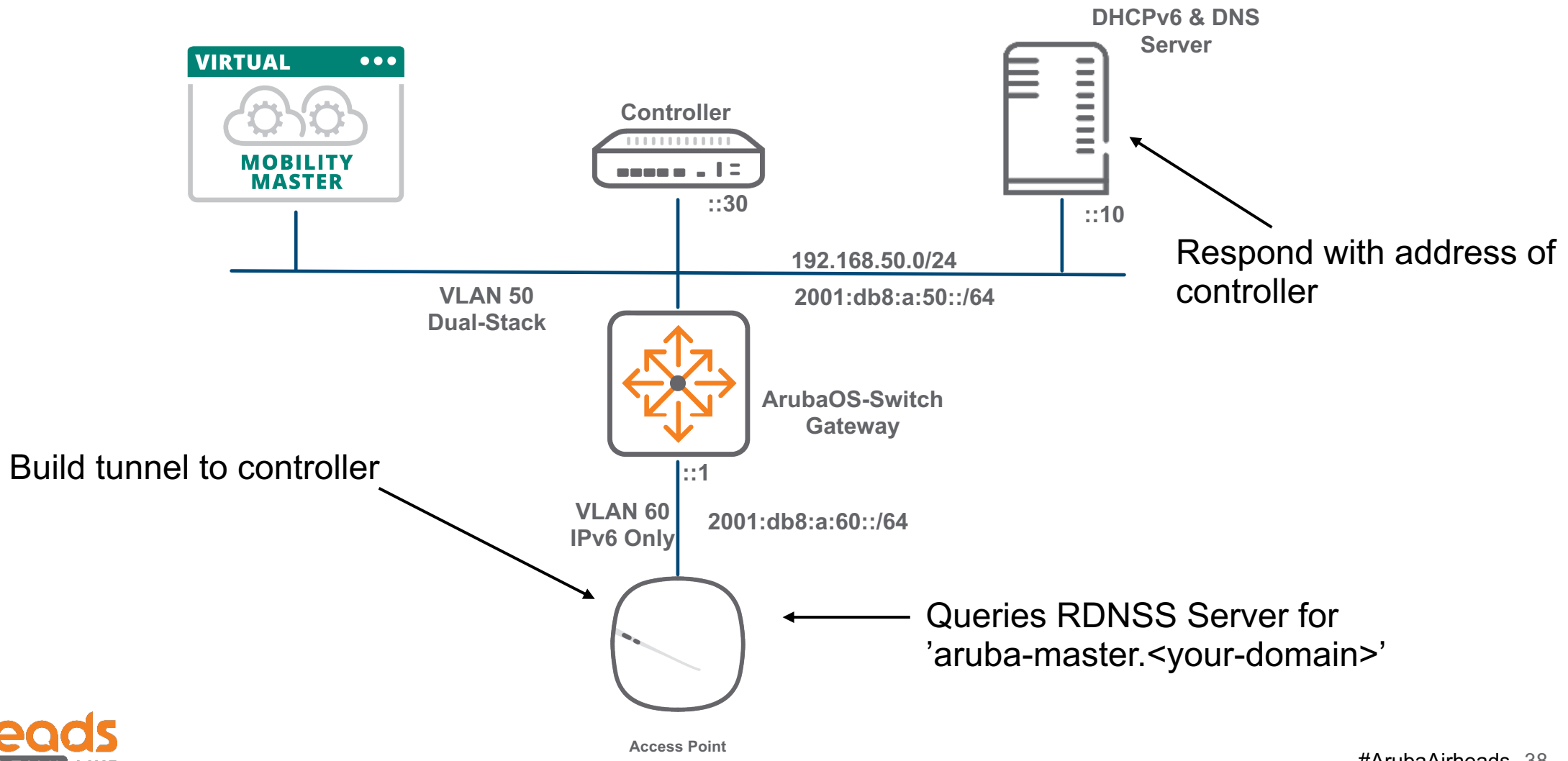
Other flag on



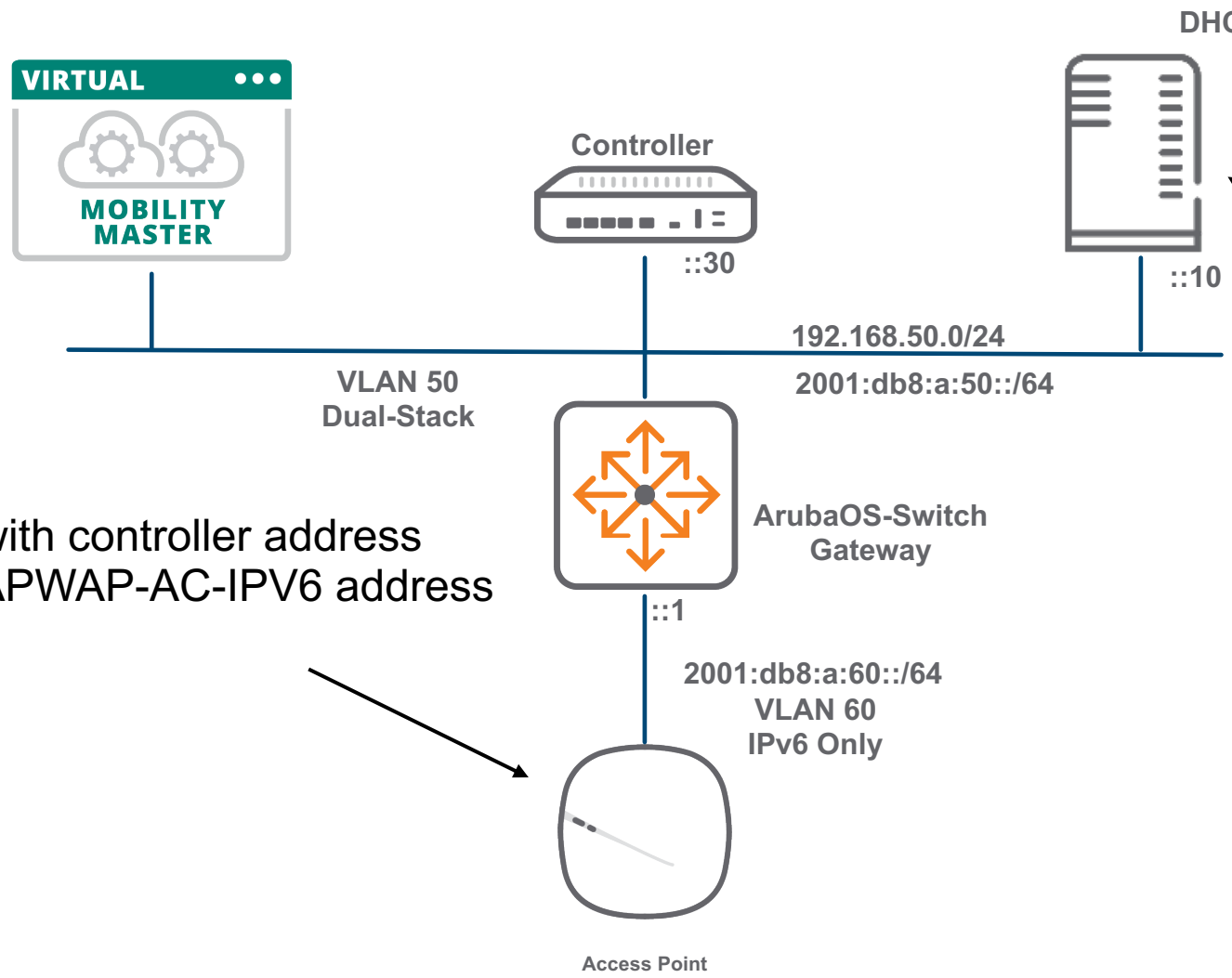
Stateless DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



Stateless DHCPv6 with DHCP Options RDNSS 23 & DNSSL 24



DHCPv6 with DHCP Options CAPWAP-AC-IPV6 52



- AP boots
- DHCPv6 SOLICIT
- Receives REPLY with controller address
- Builds tunnel to CAPWAP-AC-IPV6 address

Configure DHCPv6:

- v6 address
- CAPWAP-AC-IPV6 52

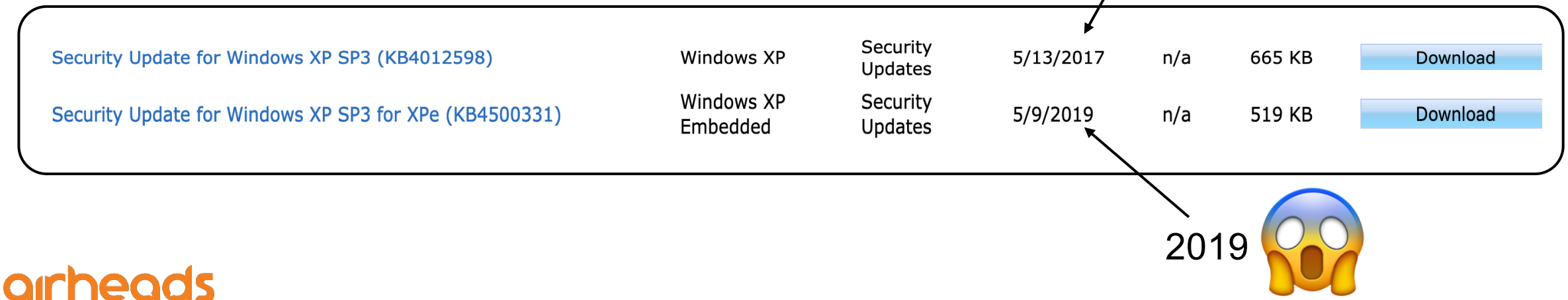
IPv6 Address Allocation Issues!

SLAAC Issues:

– RFC6106 support is not universal.

– Windows Creator Update and later (1703).

Sidenote – 2018 People told me of WinsXP client on their network



IPv6 Address Allocation Issues!

DHCPv6 NOT SUPPORTED ON ANDROID

- This is by design
- Issue tracker opened June 2012: https://issuetracker.google.com/issues/36949085
- 277 comments, no change
- Impacts address allocation – many go with SLAAC & DHCPv6

That leads us on to the next point

3. Dual-stack hardware exhaustion

IPv4:

1. Usually one address per host

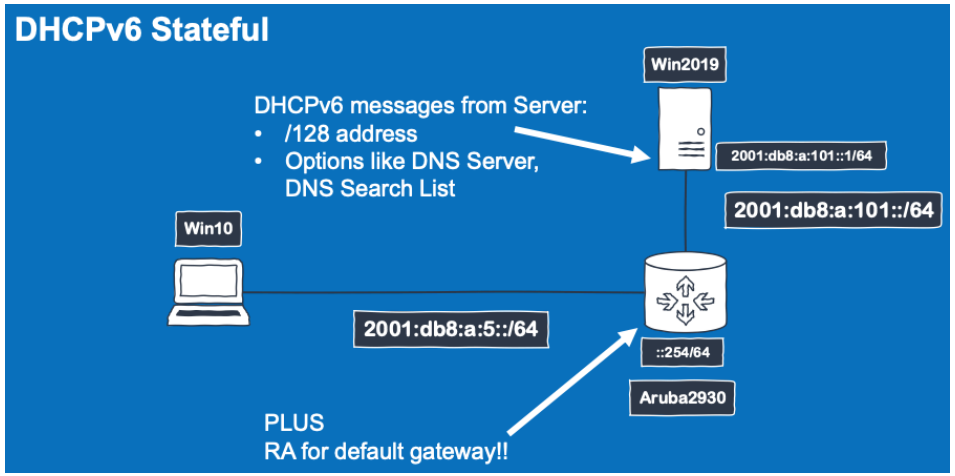
IPv6:

1. Multiple prefixes per interface by design
2. DHCPv6 = 2 prefixes, 1 link-local, 1 GUA
3. SLAAC = 3 prefixes, 1 link-local, 2 GUA
4. Mixed OS environment: 4 prefixes or more!
5. IPv6 addresses take up more resources!

Impacts the networking hardware resources, only have finite routing and IPv6 neighbour tables.

Dual-stack makes this even worse!

4. First Hop Security



New Attack Vectors

- All those options, packets and the whole new NDP create new opportunities for exploits.
- Spoofing DHCPv6 and NDP pkts for man-in-the-middle & DoS attacks.
- RA is like the crown jewels of the LAN network – crucial because it controls addressing and the default gateway!

Mitigation tools like RA Guard are fundamental requirements.

As is a IPv6 specific security plan.

Understanding IPv6 is vital to understanding how to secure it!

Aruba & IPv6

IPv6 Open for Business

- Good support on AOS-Switch, Layer 3 Gateway support on ArubaOS-CX
- Dual-stack supported on AOS8 & Aruba Instant. APs can boot and discover MD in IPv6 only network.
- Mgmt and Provisioning needs work. We are aware and working on this. Watch this space.

Aruba & IPv6

IPv6 Open for Business

- Live IPv6 deployments across the globe, airheads ‘pink’ series focused on Wins and v6 wired.
- Working with PLM & Aruba CTO office to plug v6 gaps in Aruba portfolio.
- AOS8 & Instant IPv6 write-up:

  https://github.com/Joe-Neville/aos-ipv6/blob/master/aruba-ap-ipv6-deployment.md

aruba
a Hewlett Packard
Enterprise company

airheads

TECH TALK LIVE