
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Goodbye Legacy,

the move to an IPv6-Only Enterprise

David Prall Systems Architect
@pralldc

BRKENT-2008

Cisco Webex App

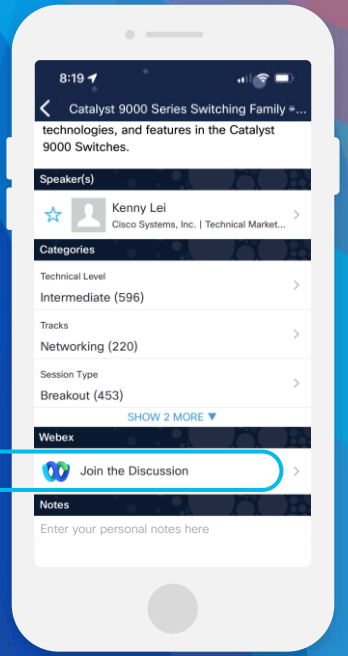
Questions?

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 9, 2023.

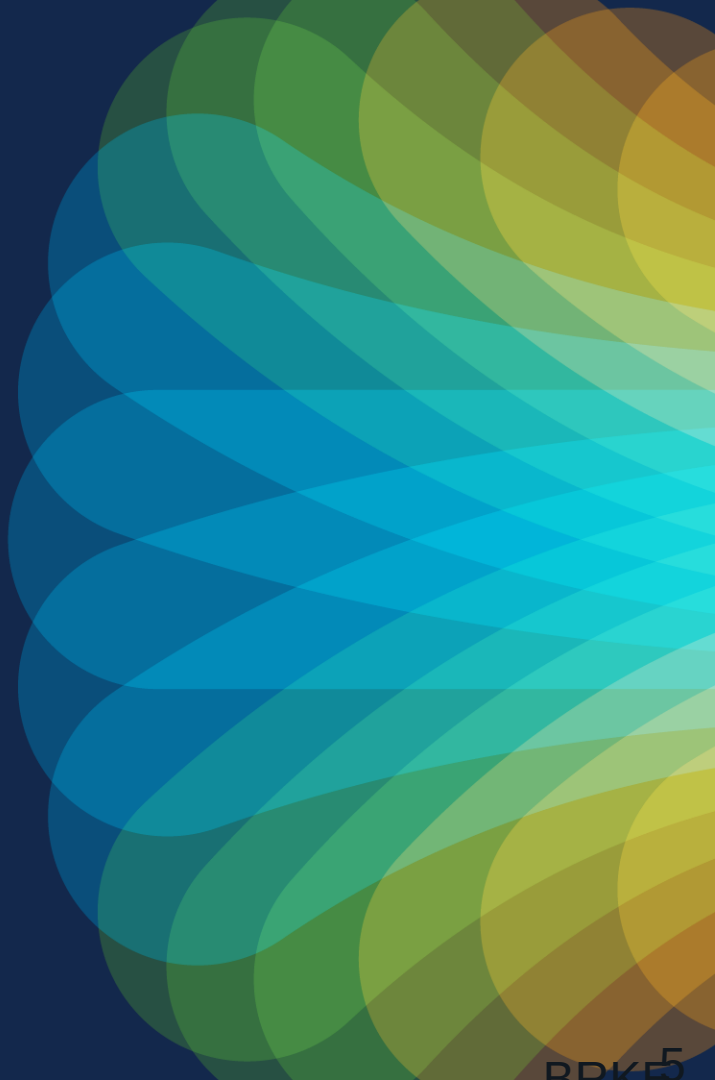


https://ciscolive.ciscoevents.com/ciscolivebot/#BRKENT-2008

Agenda

- Introduction
- Our Dual Stacked Network
- IPv4 vs IPv6
- NAT64/DNS64
- IPv6-Only
- Additional Learning
- Conclusion

Introduction



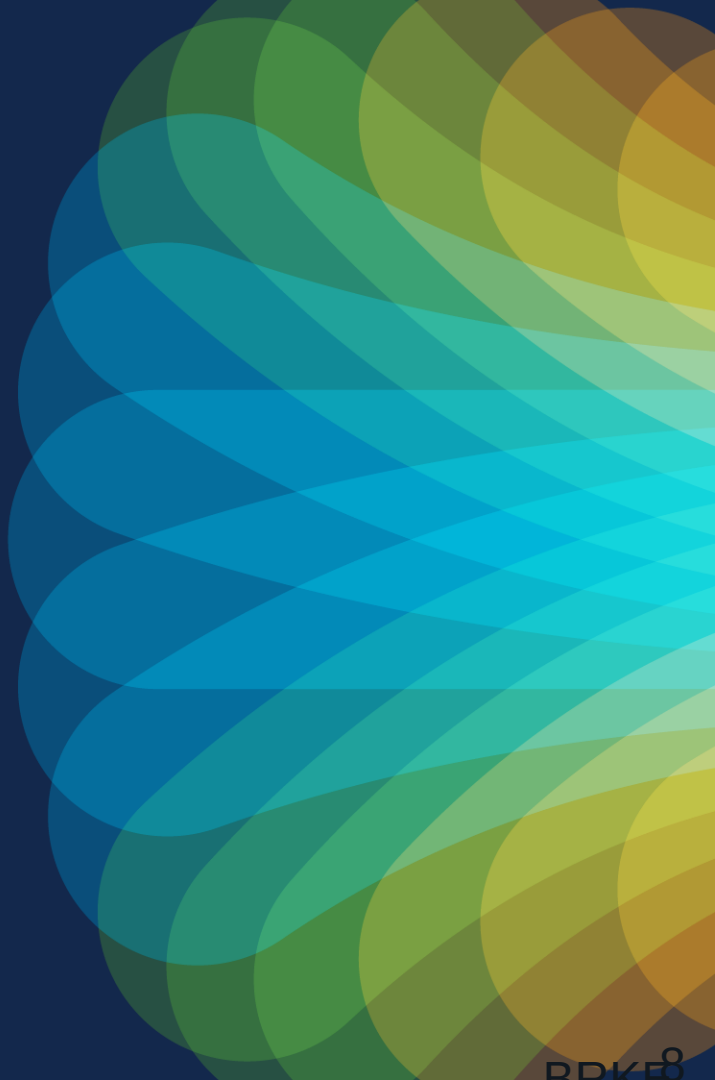
Your speaker

- David Prall
- Systems Architect
- US Federal NSD Operation
- dprall@cisco.com
- CCIE 6508 (R&S/SP/Security)
- 22 Years at Cisco
- Washington, DC
- House Dual-Stacked since September 2007

IPv6-Only is the Future

- RFC1883 - December 1995
  - Updated RFC8200 (STD86) - July 2017
- US Government Memorandum M-21-07, Completing the Transition to Internet Protocol Version 6 (IPv6) – November 2020
  - September 2025 for 80% IPv6-Only completion
  - US Government Memorandum M-05-22, Transition Planning for Internet Protocol Version 6 (IPv6) – August 2005
  - Transition to IPv6 – September 2010
- Germany Defense, China, and others have released 2030 dates for IPv6-Only completion

Our Dual Stacked Network



Our Dual Stacked Network

- IPv4 and IPv6 are both available for use
- How did my Web Browser Connect
- NetFlow shows us what is being utilized

IPv4 and IPv6 are both available for use

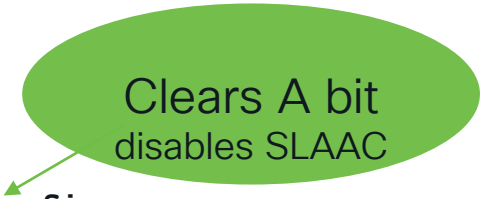
```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001db8:8000:103::190
   Link-local IPv6 Address . . . . . : fe80::12a8:6d5:b492:dd26%12
   IPv4 Address. . . . . . . . . . . : 192.168.124.190
   Subnet Mask . . . . . . . . . . . : 255.255.255.192
   Default Gateway . . . . . . . . . : 2001:db8:8000:103::1
                                       fe80::272:78ff:fe55:15d%12
                                       192.168.124.129
```

```
$ ifconfig en0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=400<CHANNEL_IO>
ether 88:66:5a:4b:a2:38
inet6 fe80::c5:d6d9:3a53:5bb3%en0 prefixlen 64 secured scopeid 0x6
inet 192.168.141.108 netmask 0xfffffe00 broadcast 192.168.141.255
inet6 2001:db8:8000:140:58d:6787:27f2:9aab prefixlen 64 dynamic
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
```

Are you sure both are available?

- Android doesn't support DHCPv6

```
show run interface vlan 150
<snip>
 ipv6 nd prefix default 2592000 604800 no-autoconfig
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:DB8::100
<snip>
```

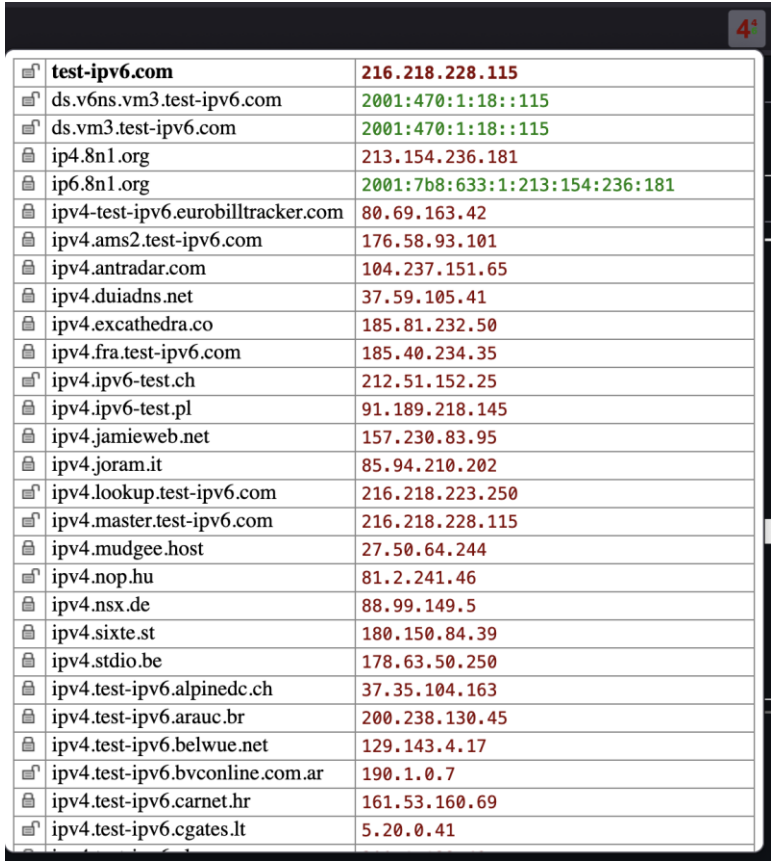


- For Android we must leave SLAAC enabled and provide DNS

```
conf t
int vlan 150
 no ipv6 nd prefix default
 ipv6 nd ra dns server 2001:DB8::111
 ipv6 nd ra dns server 2001:DB8::112
end
```

How did my Web Browser Connect

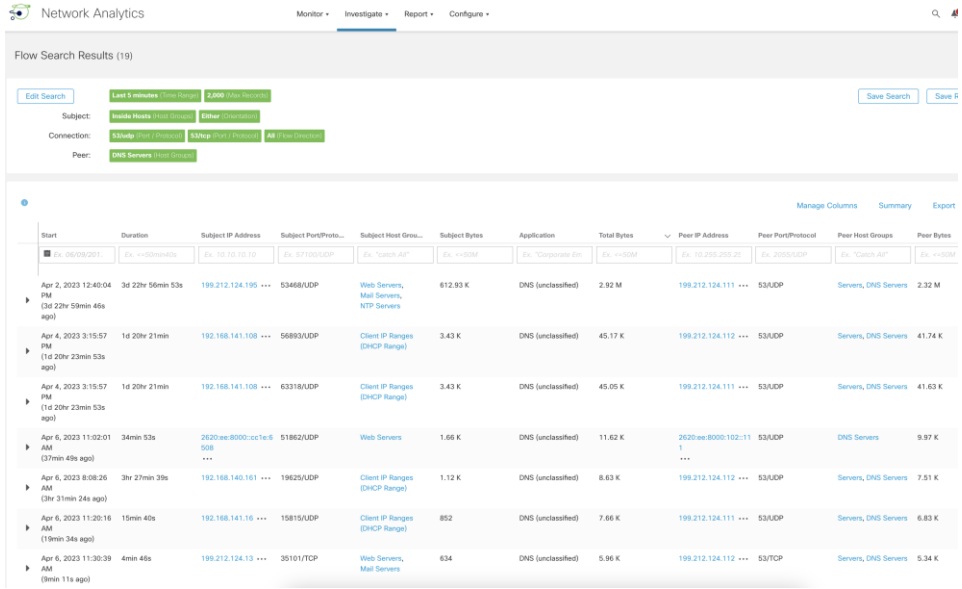
- IPvFoo
  - Extension for Firefox and Chrome
  - Can be added to Edge enabling “Allow extensions from other stores.”



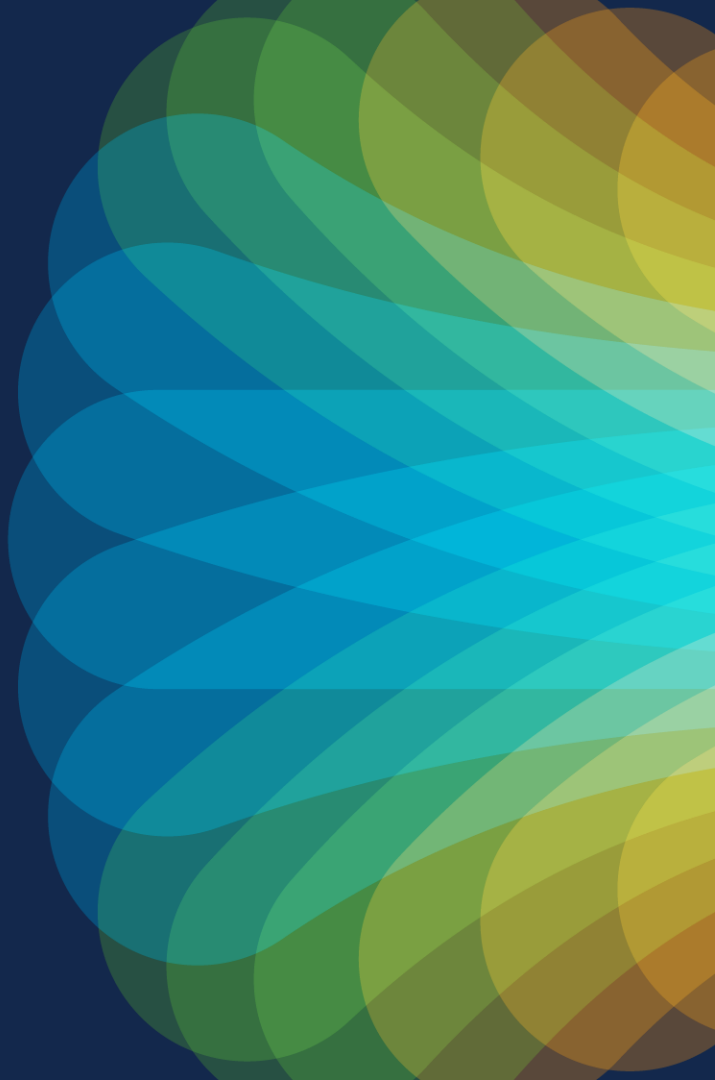
test-ipv6.com	**216.218.228.115**
ds.v6ns.vm3.test-ipv6.com	2001:470:1:18::115
ds.vm3.test-ipv6.com	2001:470:1:18::115
ip4.8n1.org	213.154.236.181
ip6.8n1.org	2001:7b8:633:1:213:154:236:181
ipv4-test-ipv6.eurobilltracker.com	80.69.163.42
ipv4.ams2.test-ipv6.com	176.58.93.101
ipv4.antradar.com	104.237.151.65
ipv4.duiadns.net	37.59.105.41
ipv4.excathedra.co	185.81.232.50
ipv4.fra.test-ipv6.com	185.40.234.35
ipv4.ipv6-test.ch	212.51.152.25
ipv4.ipv6-test.pl	91.189.218.145
ipv4.jamieweb.net	157.230.83.95
ipv4.joram.it	85.94.210.202
ipv4.lookup.test-ipv6.com	216.218.223.250
ipv4.master.test-ipv6.com	216.218.228.115
ipv4.mudgee.host	27.50.64.244
ipv4.nop.hu	81.2.241.46
ipv4.nsx.de	88.99.149.5
ipv4.sixte.st	180.150.84.39
ipv4.stdio.be	178.63.50.250
ipv4.test-ipv6.alpinedc.ch	37.35.104.163
ipv4.test-ipv6.arauc.br	200.238.130.45
ipv4.test-ipv6.belwue.net	129.143.4.17
ipv4.test-ipv6.bvconline.com.ar	190.1.0.7
ipv4.test-ipv6.carnet.hr	161.53.160.69
ipv4.test-ipv6.cgates.lt	5.20.0.41

NetFlow shows us what is being utilized

- NetFlow allows the network operator to see what is flowing on the network.
  - Secure Network Analytics / StealthWatch
  - DNA Center Assurance
  - Other Third Party
- What is using IPv4 still?
  - Internal or External?
- Why is it using IPv4 still?
  - Focus on Internal.



IPv4 vs IPv6



IPv4 vs IPv6

- Address Selection
- Happy Eyeballs RFC6555/8305 – Users are happy
- IPv6 is Faster

Address Selection

- RFC6724 Default Address Selection for IPv6
- Globally Unique Addresses (GUA) are the only option
- Unique Local Addresses (ULA) are of limited use
  - Not the same as RFC1918
  - There is no NATv6
  - NPTv6 as defined changes only the prefix
  - As of RFC6724 IPv4 is preferred over IPv6 ULA
    - Unless IPv6 ULA to IPv6 ULA

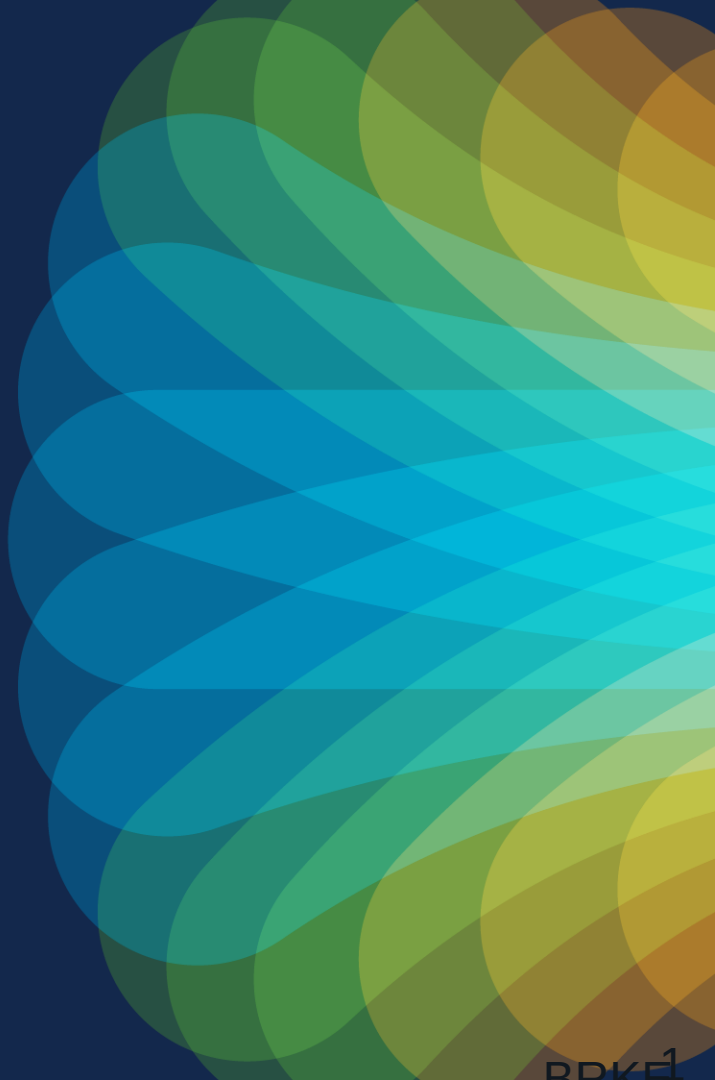
Happy Eyeballs RFC6555/8305

- On a dual-stacked system give IPv6 the edge but start an IPv4 session and see which is fastest.
- Before Happy Eyeballs dual-stacked systems would start an IPv6 session and if it didn't work after several attempts. Possibly fallback to IPv4.
- Typically, only needed when a site is advertising an IPv6 AAAA but not functioning. Or when Cogent (AS174) and Hurricane Electric (AS6939) are involved.

IPv6 is Faster

- “Several years ago, Facebook decided to move early and migrate to IPv6. We’ve observed that accessing Facebook can be 10-15 percent faster over IPv6. We believe other developers will see similar advantages from migrating.” IPv6: It’s time to get on board
- “Akamai’s customer AbemaTV did a case study in 2019, which showed that IPv6 improved the throughput by 38% on average when compared with connections via IPv4.” 10 Years Since World IPv6 Launch

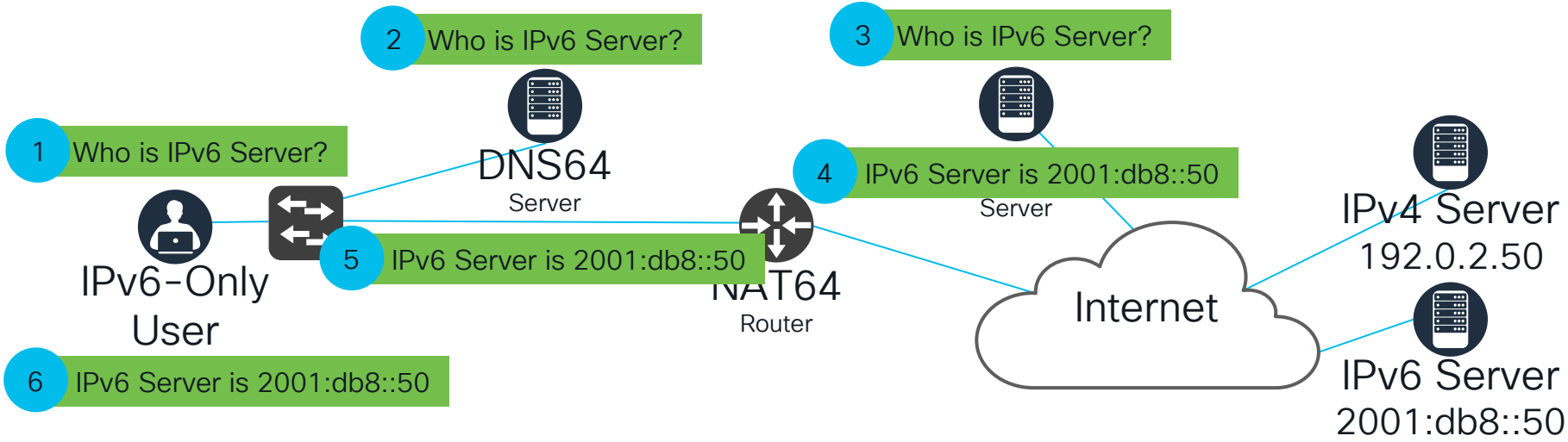
NAT64/DNS64



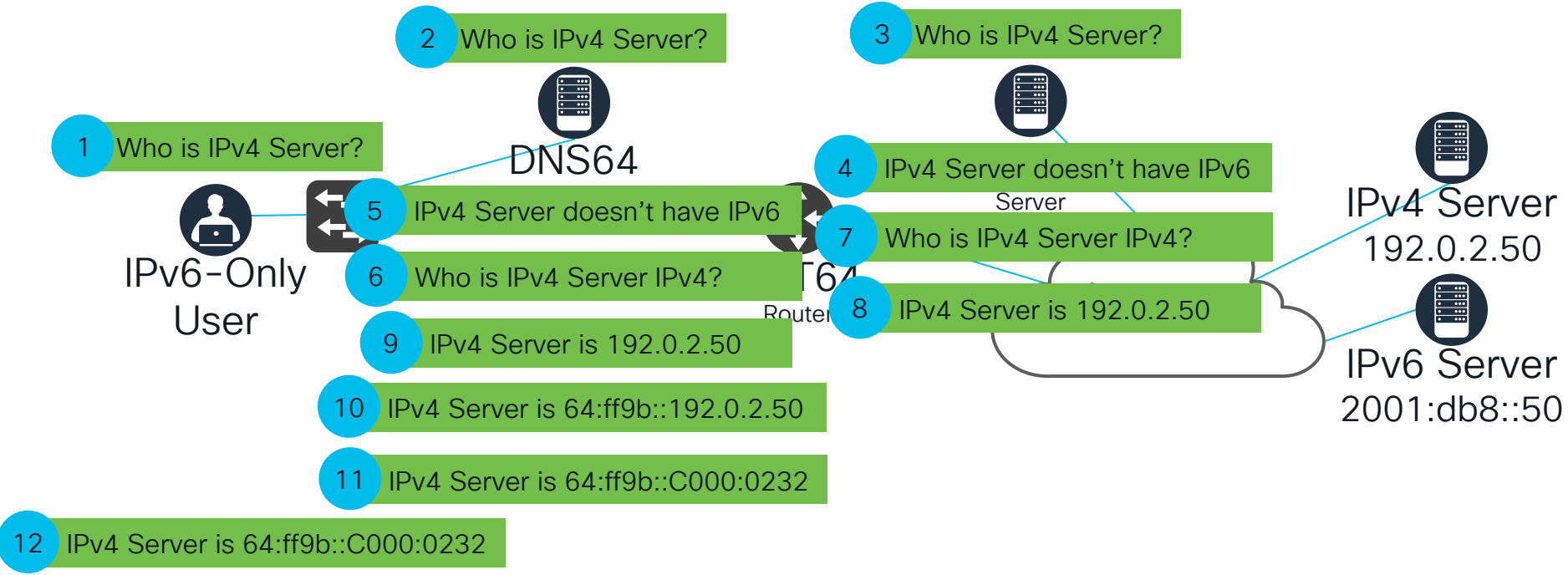
NAT64/DNS64

- RFC6052 IPv6 Addressing of IPv4/IPv6 Translators
  - Well Known Prefix for NAT64 – 64:ff9b::/96
- RFC6145 Stateless IP/ICMP Translation Algorithm
- RFC6146 Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers
- RFC6147 DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers

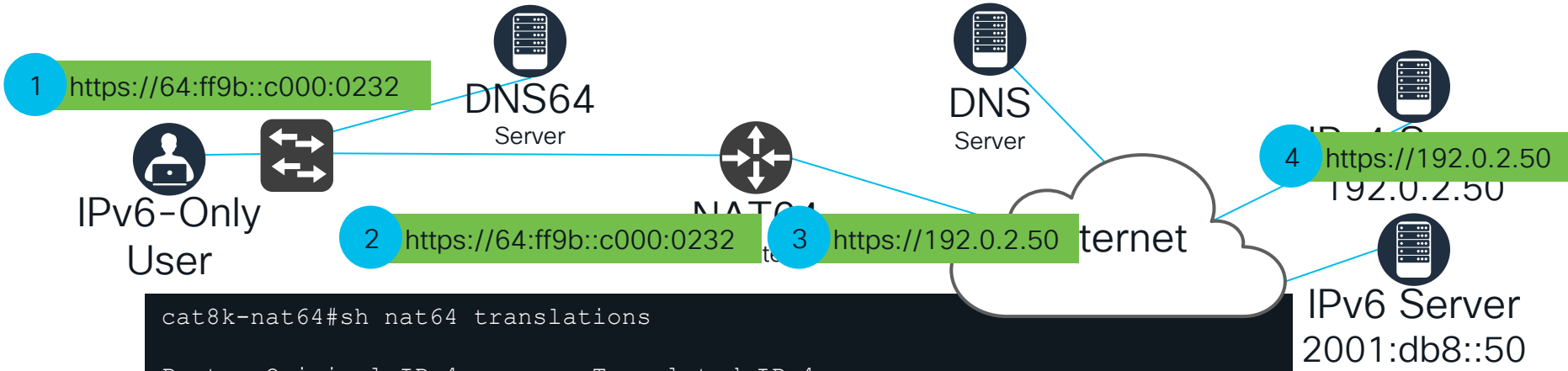
IPv6 AAAA DNS Request



IPv6 AAAA DNS64 Request



NAT64 Traffic Flow




```
cat8k-nat64#sh nat64 translations

Proto  Original IPv4          Translated IPv4
       Translated IPv6        Original IPv6
------------------------------------------------------------------------
-

tcp    192.0.2.50:443         [64:ff9b::c000:0232]:443
       192.0.2.252:52362      [2001:db8:8000:150::2]:52362
```

IOS-XE Router Configuration

IP NAT and NAT64 cannot be together

- When using Well-Known Prefix 64:ff9b::/96

```
interface GigabitEthernet1
 ip address 192.168.67.2 255.255.255.0
 nat64 enable
interface GigabitEthernet2
 no ip address
 nat64 enable
 ipv6 address 2001:DB8:8000:666::5/64
ipv6 access-list nat64-acl
 sequence 10 permit ipv6 2001:DB8::/32 any
nat64 v4 pool nat64-pool 192.0.2.252 192.0.2.252
nat64 v6v4 list nat64-acl pool nat64-pool overload
```

Must be Public per RFC6052

IOS-XE Router Configuration

- Let's use an Internal Prefix
  - Must utilize own DNS64 server

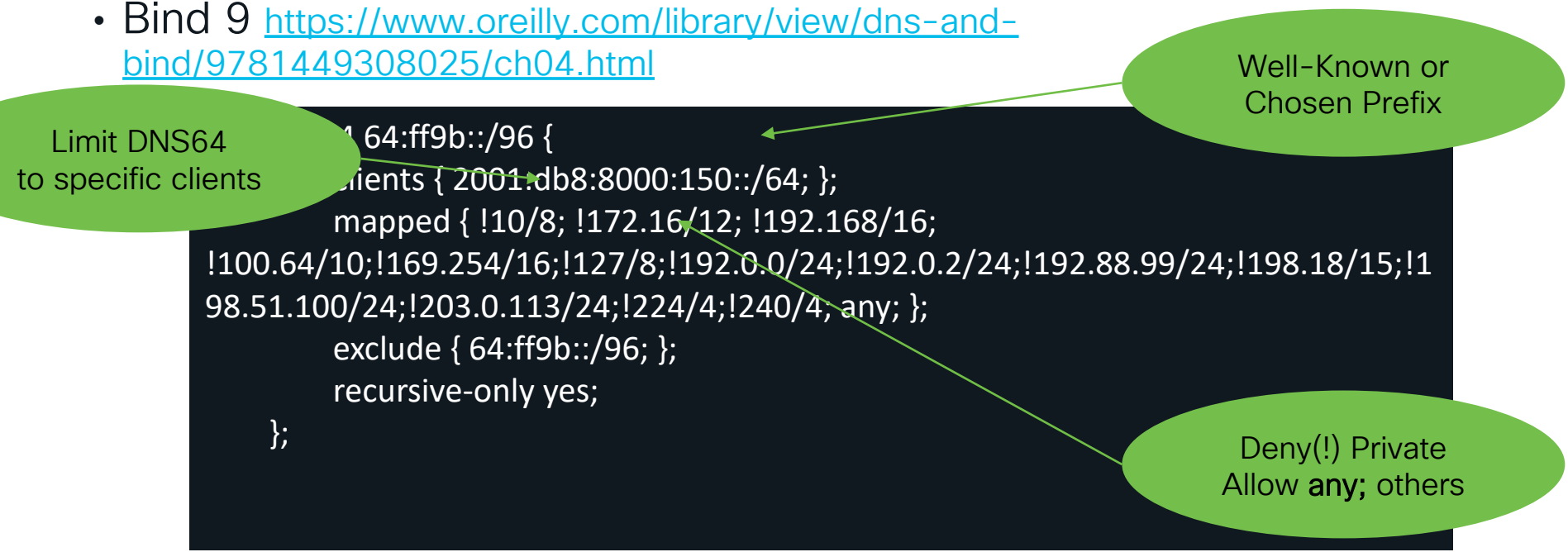
```
interface GigabitEthernet1
 ip address 192.168.67.2 255.255.255.0
 nat64 enable
interface GigabitEthernet2
 no ip address
 nat64 enable
 ipv6 address 2001:DB8:8000:666::5/64
ipv6 access-list nat64-acl
 sequence 10 permit ipv6 2001:DB8::/32 any
nat64 prefix stateful 2001:DB8:FFFF::/96
nat64 v4 pool nat64-pool 192.168.255.254 192.168.255.254
nat64 v6v4 list nat64-acl pool nat64-pool overload
```

Public Recursive DNS64 Servers

- https://gist.github.com/mutin-sa/5dcbd35ee436eb629db7872581093bc5
- Google Public DNS64
  https://developers.google.com/speed/public-dns/docs/dns64
  - 2001:4860:4860::6464
  - 2001:4860:4860::64
- Cloudflare DNS64
  - 2606:4700:4700::64
  - 2606:4700:4700::6400

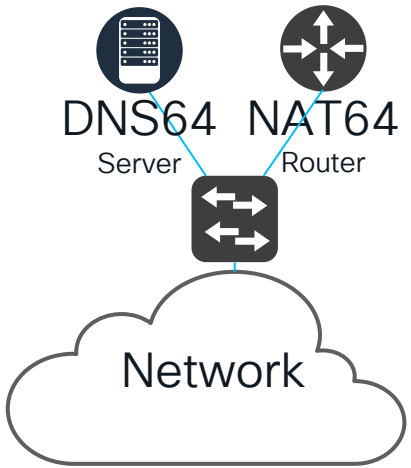
DNS64 Configuration

- Bind 9 https://www.oreilly.com/library/view/dns-and-bind/9781449308025/ch04.html



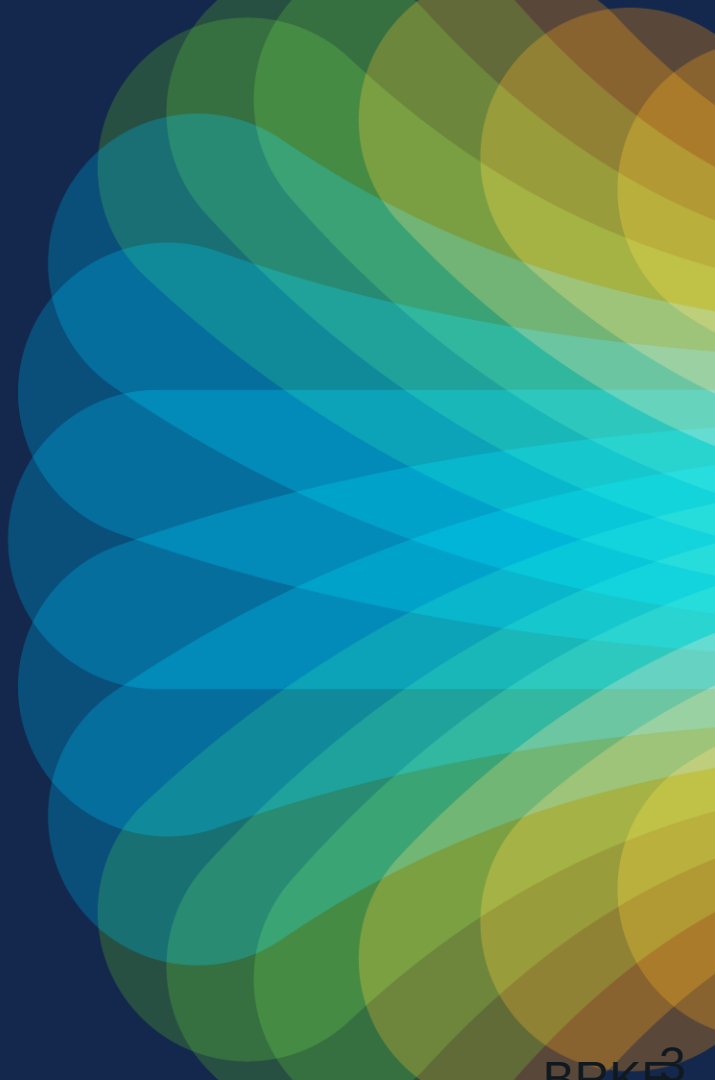
- Infoblox https://docs.infoblox.com/space/nios86/36704017/About+DNS64

Placement NAT64/DNS64



- Service Block
  - Placed near IPv6-Only Users
  - Can reach internal IPv4 resources
- Integrated
  - DNS64 can be limited to specific IPv6 addresses
  - Translation prefix can be advertised to network
- Edge
  - IPv6 is fully functional internally for **everything(?)**
  - IPv6-Only Users can reach internal IPv6-Only and Dual Stack Resources
  - Only required for external sites that haven't Dual Stacked

IPv6-Only



IPv6-Only

- Where do we start?
- Do I need to disable IPv4 in OS?
- Stop IPv4 on the Network
- How did my Web Browser Connect
- NetFlow shows us what is being utilized
- Network Equipment

Where do we start?

- Outside In
  - Network Engineers
  - Help Desk
  - Select user VLAN's
    - VLAN by VLAN
    - Site by Site
  - Data Center
  - Network Infrastructure

Do I need to disable IPv4 in OS?

- On an IPv6-Only VLAN

```
C:\>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:8000:150::2
   Link-local IPv6 Address . . . . . : fe80::9c73:7c11:8a59:3f3d%13
   Autoconfiguration IPv4 Address. . : 169.254.42.133
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 2001:db8:8000:150::1
                                       fe80::272:78ff:fe55:17d%13
```

- What happens while travelling?

Stop IPv4 at Layer 2

- VLAN Map, example for limited address space

```
vlan access-map vlan-map-ipv4-link-local 10
 match ip address ipv4-link-local-deny
 action forward
vlan access-map vlan-map-ipv4-link-local 20
 match ip address ipv4-link-local-permit
 action drop
vlan filter vlan-map-ipv4-link-local vlan-list 150
ip access-list extended ipv4-link-local-deny
 10 deny   ip 169.254.0.0 0.0.255.255 any
 20 permit ip any any
ip access-list extended ipv4-link-local-permit
 10 permit ip 169.254.0.0 0.0.255.255 any
```

Stop IPv4 at Layer 3

- Unicast Reverse Path Forwarding

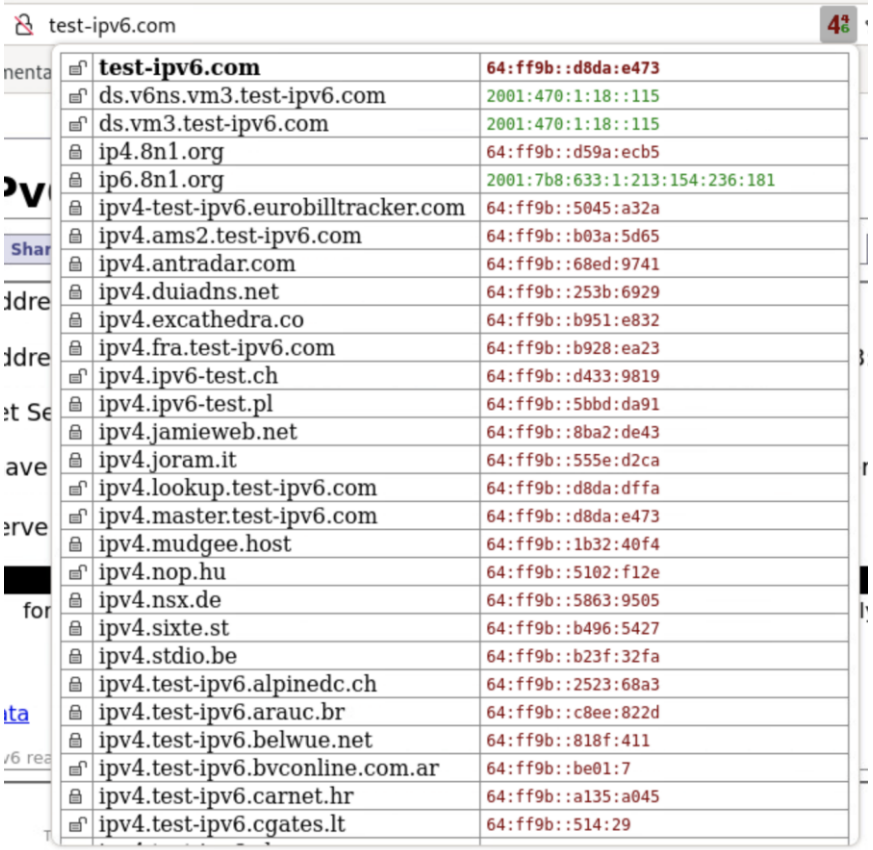
```
interface Vlan150
 no ip address
 ip verify unicast source reachable-via rx
```

- Access List

```
interface Vlan150
 no ip address
 ip access-group no-ipv4 in
 ip access-group no-ipv4 out
ip access-list extended no-ipv4
 10 deny ip any any
```

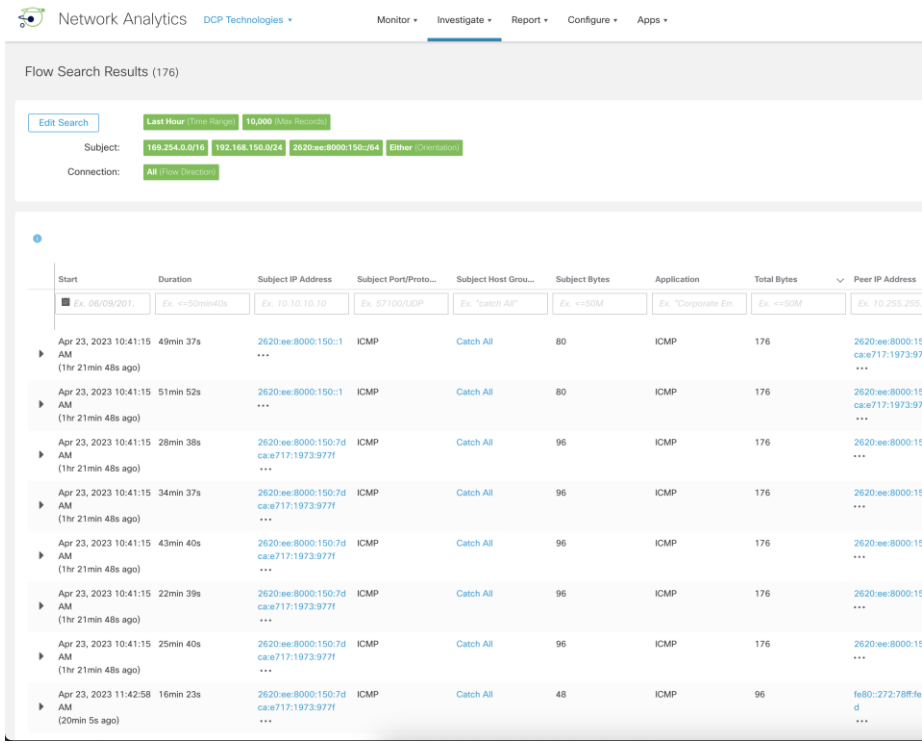
How did my Web Browser Connect

- IPvFoo
  - Extension for Firefox and Chrome
  - Can be added to Edge enabling “Allow extensions from other stores.”
  - By using the Well-Known Prefix, we still know what is only IPv4



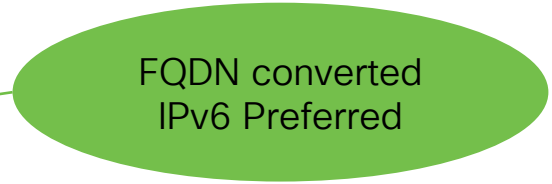
NetFlow shows us what is being utilized

- Why do we still see IPv4?
  - NetFlow on L2 interfaces happens before L3 processing.
  - 169.254.0.0/16 link-local IPv4
    - UPnP/SSDP 239.255.255.250:UDP/1900
    - Multicast DNS 224.0.0.251:UDP/5353
  - Static Configuration?
- IPv6 is all that is active!



Network Equipment

- Services converted to IPv6? All services support IPv6?
  - NTP - `ntp peer ipv6 time.example.com`
  - NetFlow
    - `flow exporter FLOWEXPORTER`
      `destination 2001:DB8::2055`
  - Logging - `logging host fqdn ipv6 syslog.example.com`
  - DNS - `ip name-server 2001:DB8:53::111 2001:DB8:53::112`



But do the services support IPv6?

Network Equipment

- Services converted to IPv6? All services support IPv6?
  - SNMP
    - `snmp-server group <v3-group-name> v3 [auth|noauth|priv] access ipv6 <ipv6-acl> <ipv4-std-acl>`
      `snmp-server community private RW ipv6 <ipv6-acl> <ipv4-std-acl>`
      `snmp-server community public RO ipv6 <ipv6-acl> <ipv4-std-acl>`

      `snmp-server host 192.0.2.162 <snip>`
  - VTY Access-Lists
    - `line vty 0 4`
      `ipv6 access-class <ipv6-acl> in`
      `access-class <ipv4-std-acl> in`
  - Authentication
    - `tacacs server TACACS`
      `address fqdn tacacs.example.com`
    - `radius server RADIUS`
      `address fqdn radius.example.com`

Adding IPv6 requires restating IPv4

FQDN converted IPv4 Preferred

But do the services support IPv6?

Routing Protocols

- Router ID's are 32-bit values
- Commonly represented as 4 dotted octets
- Cisco Routers are nice enough to utilize an interface IPv4 address
- IPv6-Only must manually configure router-id
  - Majority will not work
- Don't be surprised with the first router reload

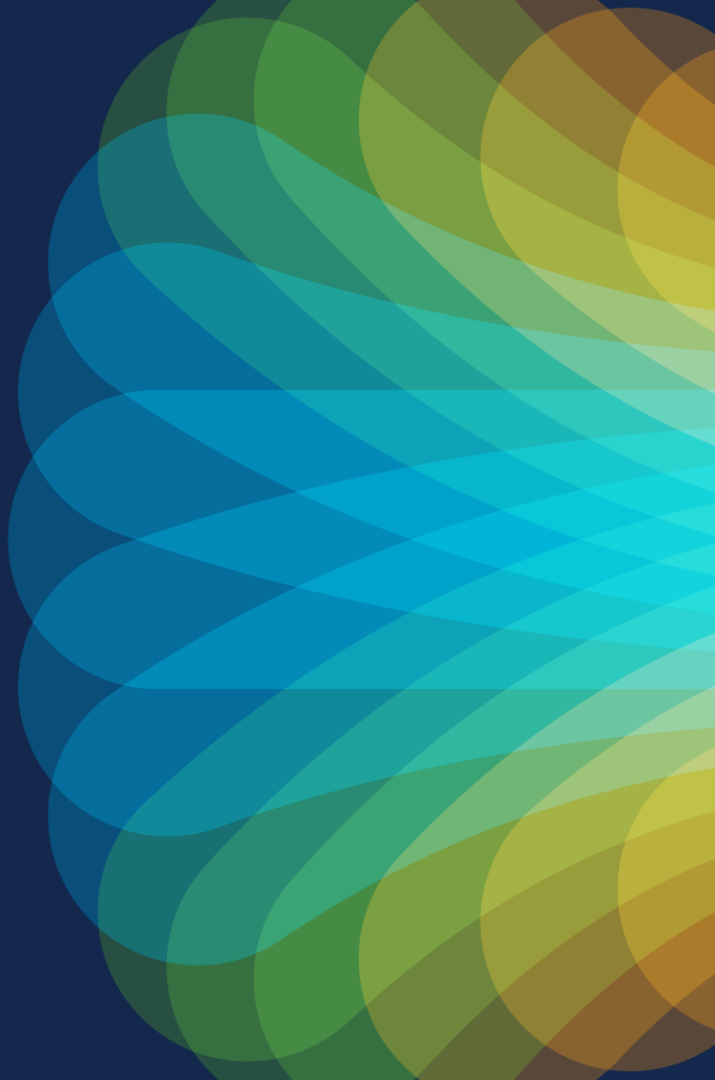
Routing Protocols

- BGP
  - `%BGP-4-NORTRID: BGP could not pick a router-id. Please configure manually.`
  - `bgp router-id x.x.x.x`
- OSPFv3
  - `%OSPFv3-4-NORTRID: Process OSPFv3-<area>-IPv6 could not pick a router-id, please configure manually`
  - `router-id x.x.x.x`
- EIGRP
  - NOTHING
  - `eigrp router-id x.x.x.x`
- RIPng and ISIS could care less

Remove IP Routing

- `no ip routing`
  - BGP goes down immediately
    - Can't be configured, current configuration removed
    - `%BGP-5-ADJCHANGE: neighbor 2001:DB8::2 Down Unknown path error`
      `%BGP_SESSION-5-ADJCHANGE: neighbor 2001:DB8::2 IPv6 Unicast topology base removed from session  Unknown path error`
  - EIGRP goes down after hold time
    - Both Numbered and Named
    - `%DUAL-5-NBRCHANGE: EIGRP-IPv6 1: Neighbor FE80::5054:FF:FE1B:C299 (GigabitEthernet1) is down: holding time expired`
  - OSPFv3 goes down after dead time
    - `%OSPFv3-5-ADJCHG: Process 1, Nbr 192.168.0.1 on GigabitEthernet1 from FULL to DOWN, Neighbor Down: Dead timer expired`
  - RIPng goes down after holddown time
  - ISIS could care less

Additional Learning



Further Reading

- Validated Solution: IPv6 Integration with Cisco SD-Access, SD-WAN, and Firepower
  - https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/Cisco-Validated-Solution-Profiles/b_cisco_validated_solution_ipv6.html

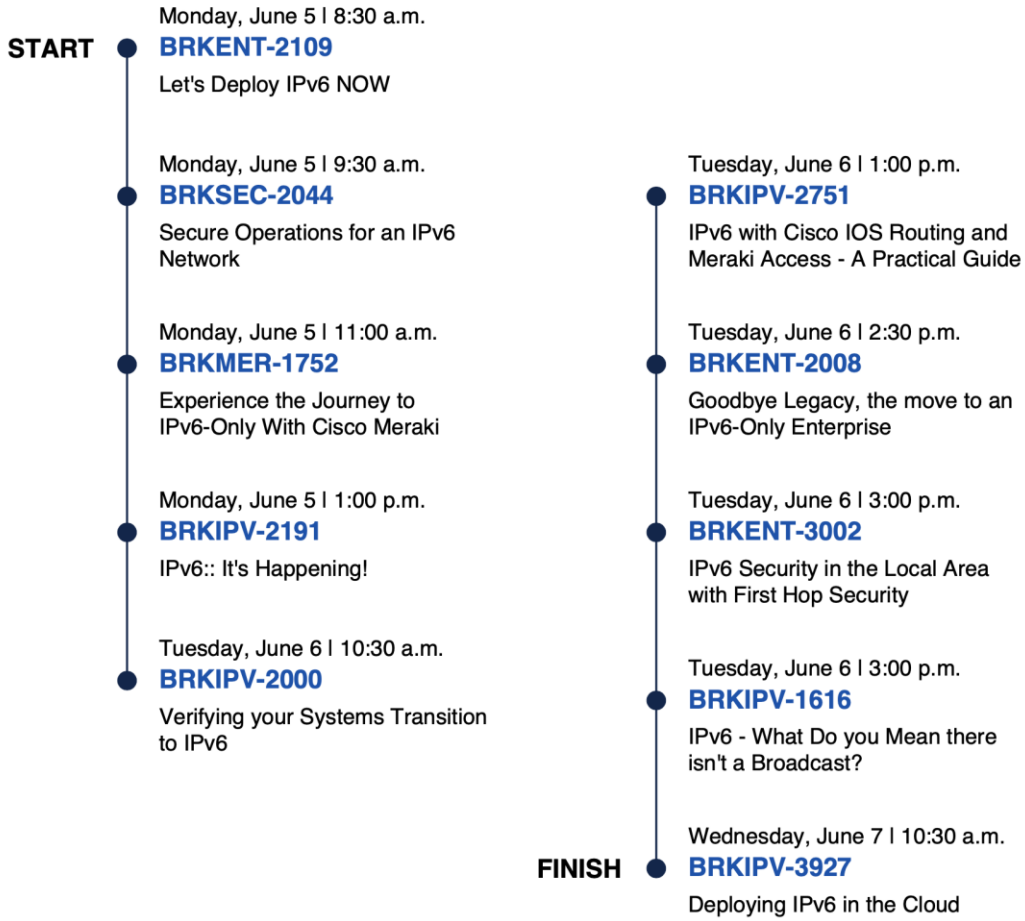
- An IPv6 Campus of the Future
  - https://blogs.cisco.com/networking/an-ipv6-campus-of-the-future

- RFC6586 - Experiences from an IPv6-Only Network – April 2012

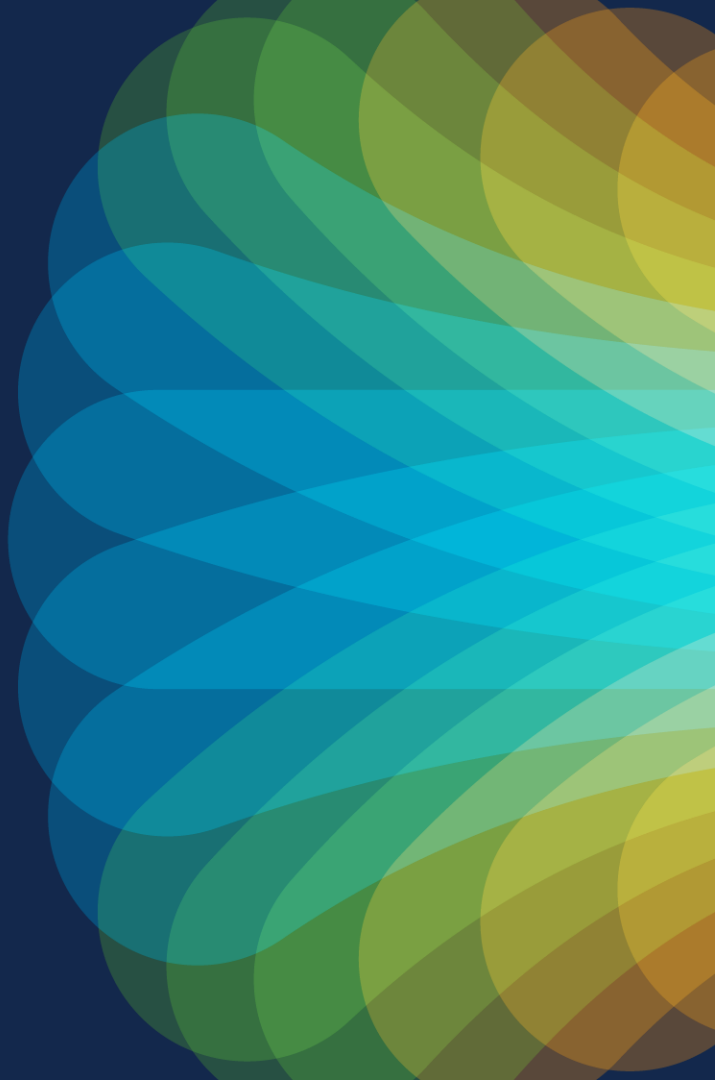
IPv6

Deploying and Securing IPv6

Learn from specialists about IPv6 in their respective area. From the fundamentals of the Neighbor Discovery Protocol, deployment guidelines, security in the network, and troubleshooting.



Conclusion



Get to it, IPv6 is approaching 30

- NetFlow is required to see what is happening on the network.
- IPv6-Only User VLAN's are ready to be deployed
  - If your applications are ready
  - Cogent and Hurricane Electric are both reachable directly
- IPng Working Group proposed October 1994
  - https://datatracker.ietf.org/wg/ipngwg/history/
- RFC1883 - December 1995
  - Updated RFC8200 (STD 86) - July 2017
- RFC6586 - Experiences from an IPv6-Only Network – April 2012

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

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

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!

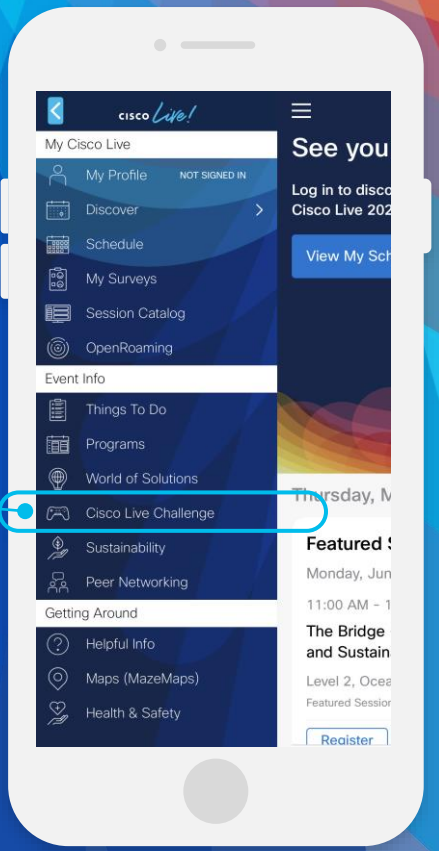
Cisco Live
Challenge

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!


cisco Live!
Let's go
#CiscoLive