

# Mind the Gap

IPv6(only) and Enterprise Networks

Jen Linkova, RIPE NCC::EDUCA, June 6th 2018

# Different Technology, Same Story

Year 2008

**Me:** ...what about WiFi?

**Enterprise engineer:** We do not need it. It's insecure. Everything works w/o it.

**Me:** but you have it already, you just do not control it...

Year 2018

**Me:** ...what about IPv6?

**Enterprise engineer:** We do not need it. It's insecure. Everything works w/o it.

**Me:** but you have it already, you just do not control it...

# IPv6 Excuse Bingo

We don't need that many addresses	We'll deploy IPv6 next financial year	I don't want to lose the <a href="#">security</a> provided by NAT	Can't we just <a href="#">buy</a> more IPv4 addresses?
IPv6 just isn't a priority	It's not supported by <a href="#">Google Compute</a>	Our business intelligence team can't even parse IPv4 logfiles	We can use <a href="#">RFC6598</a>
What do you mean I have to wrap an IP in square brackets?	Our <a href="#">Dynamic DNS</a> doesn't support it	Too many people have <a href="#">broken IPv6 stacks</a>	Our recursive DNS can't handle the extra load
<a href="#">Android</a> doesn't support DHCPv6	IPv6 is <a href="#">slower</a> than IPv4	We have IPv6, but we just want to keep things simple	Our Lawful Intercept doesn't support IPv6 yet

<https://ipv6bingo.com/>

# Technical Issues

Issue #1: Network Access ~~Control~~ Surveillance

Issue #2: Dual-stack is hard

Issue #3: Multihoming

Issue #4: Legacy systems/applications

# Issue #1: Network Access ~~Control~~ Surveillance

Q: "How do I know who was using this address?"

A: IP stack configuration != network access enforcement.

- Use 802.1x
- Use Neighbor Cache has MAC <-> IP mapping info
- Remember MAC address randomization.

# Good News

Starting with Junos OS Release 18.1R1, ON CHANGE streaming of ARP, ND, and IP sensor information associated with interfaces is supported through gRPC for MX Series routers and PTX Series routers.

Issue #2: Dual-Stack is Hard

Engineer: ...we need to disable IPv6.

Me: Why??

Engineer: it's hard to troubleshoot dual-stack..

Me: [facepalm]

Solution: Moving to IPv6-Only.

# IPv6-Only in Enterprises?!

Q: Is it ever possible?

A: Yes. But it depends.

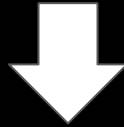
- Phones and web-based apps mostly works.
- Desktop apps might have issues
  - time to talk to vendors!
- And now VPNs...



# IPv6-Only and VPN: Breaking News!

Fact #1: VPNs are for accessing your corporate network from outside.

Fact #2: There are IPv6-only networks out there.



Fact #3: Time to make sure your VPN supports IPv6-only clients.

# VPN and IPv6: What Might Go Wrong?

- VPN Server rejecting clients w/o IPv4 address
- Split tunnels considered harmful:
  - a. Corp DNS is used to resolve all names
  - b. Only internal traffic is sent via VPN
  - c. Broken connectivity in NAT64 networks
- CORP DNS does not return any AAAA at all

## Issue #3: Multihoming Using PA Addresses

Q1: How to send packets to the right uplink?

ISPs implements BCP38

Q2: How to react to uplink failure/recovery?

# Issue #3: Multihoming Using PA Addresses

Q1: How to send packets to the right uplink?

A: Use one of the following:

- Policy Based Routing
- Source-Address Dependent Routing (SADR)
- IPv6 Segment Routing

## Issue #3: Multihoming Using PA Addresses

Q2: How to react to uplink failure/recovery?

A1: Tactical solution: use the "Conditional RA" approach;

A2: (Long-term): multiple Provisioning Domains (mPVD) technology.

# Conditional Router Advertisements

Uplink is NOT operational:

- Router sends RAs with preferred lifetime = 0 for the affected prefix

Uplink is operational:

- Router sends RAs with preferred lifetime > 0 for the affected prefix

More details: [draft-ietf-v6ops-conditional-ras](#)

# Multiple Provisioning Domains

intarea  
Internet-Draft  
Intended status: Standards Track  
Expires: December 6, 2018

P. Pfister  
E. Vyncke, Ed.  
Cisco  
T. Pauly  
D. Schinazi  
Apple  
W. Shao  
Telecom-ParisTech  
June 4, 2018

## **Discovering Provisioning Domain Names and Data draft-ietf-intarea-provisioning-domains-02**

### Abstract

An increasing number of hosts access the Internet via multiple interfaces or, in IPv6 multi-homed networks, via multiple IPv6 prefix configurations context.

This document describes a way for hosts to identify such contexts, called Provisioning Domains (PvDs), where Fully Qualified Domain Names (FQDNs) act as PvD identifiers. Those identifiers are advertised in a new Router Advertisement (RA) option and, when present, are associated with the set of information included within the RA.

Based on this FQDN, hosts can retrieve additional information about their network access characteristics via an HTTP over TLS query. This allows applications to select which Provisioning Domains to use as well as to provide configuration parameters to the transport layer and above.

# Issue #4: Legacy Systems/Applications

Solution: start ASAP.

- Identify the broken applications
- File bugs
- Update your requirements with IPv6 support



# Just When You Think You are Done...

Is IPv6 actually being used?

Me: our network is dual-stacked, time to move to Ipv6-only

Server admin: you mean enabling that IPv6 thingy which I disabled while ago?

Is IPv6 actually working?

What's IPv6 traffic level? Do you monitor e2e connectivity?

QUESTIONS?