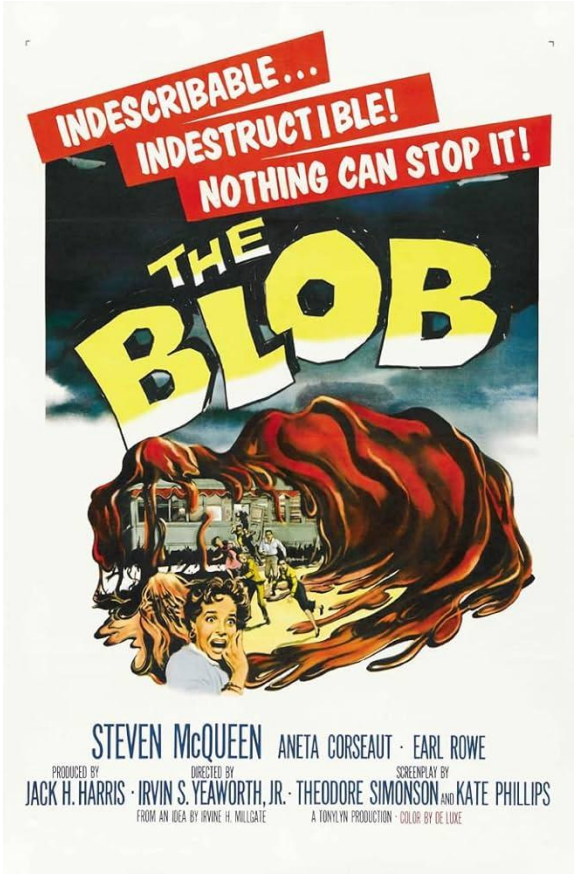
IPv6 Workshop - Campus IPv6

Campus IPv6 - Overview

- Planning
- Deployment Strategy
- IPv6 BLOB… “Nothing can stop it..”



Campus IPv6 - Planning

- Get an allocation
  - Is there a need to request an allocation from ARIN?
  - Does your organization or system already have an allocation you can use?
  - Have you met your Regional Provider (Engage with your community they are awesome!)?
  - Science and Academic community needs (external and internal).

Campus IPv6 - Deployment Strategy

- Internet Edge - with monitoring!
  - Peerings
  - DMZ
  - Core
- Security - with well understood surfaces!
  - Firewalls
  - IDS/IPS
  - Automated Blocking
  - Etc…

Campus IPv6 - Deployment Strategy

- Internet Facing Services
  - DNS
  - Load Balancers / Web Servers
  - Email
  - Business Applications
- Friendly Users
  - Test SSID’s
  - Test wired ports in IT offices
  - Etc.

Campus IPv6 - Planning

- Subnet planning
  - How are you going to break all of this space up and leave plenty of room for the future.
  - IPAM
  - Automation considerations
  - Suggestions: Keep everything on nibble boundaries (4 bits)
    - Standard Allocation: /32
    - Site/Campus: /48
    - Customer/Department/Building: /56
    - Subnet: /64

Campus IPv6 - How Is TACC Doing This?

- Allocation: 2605:2800:2000::/40
  - 16 /44's
  - Initially we had a /48. Currently moving things around to better fit the new paradigm.
  - Mostly HPC with a smaller mix of private cloud and enterprise data center
- Sites/Buildings Receive a /44
  - 16 /48's
  - ROC: 2605:2800:2000::/44
  - Sabey: 2605:2800:2010::/44

Campus IPv6 - How Is TACC Doing This?

- Departments/groups receive a /48
  - 256 /56's, 65,536 /64's
  - Backbone: /48
  - NSO: /48
  - LSS: /48
  - ACI: /48
  - External Projects: /48
  - Etc: /48

Campus IPv6 - How Is TACC Doing This?

- Individual projects are allocated a /56
  - 256 /64's
  - LSS: /48 -> LSS-Vista: /56 from this /48
- Individual subnets are allocated as a /64
  - 18,446,744,073,709,551,616 addresses
  - **Nothing smaller than a /64 will be allocated.** Don't ask. It doesn't matter.
  - LSS: /48 -> LSS-Vista: /56 - LSS-Vista-Compute: /64
  - LSS: /48 -> LSS-Vista: /56 - LSS-Vista-MGMT: /64

Campus IPv6 - ScienceDMZ

- ScienceDMZ as a considerations before campus assets
  - ScienceDMZ is a fantastic place to test IPv6
  - Green vs Brown - fields?
  - Start small stay in the ScienceDMZ core
  - Try in-house first with “your” subnets / vlans**
    - **“Your” - super well defined and understood
  - Expand one small step at a time
    - Management interfaces
    - Peering (R&E)
    - ScienceDMZ core (how is that MTU?)

Campus IPv6 - ScienceDMZ

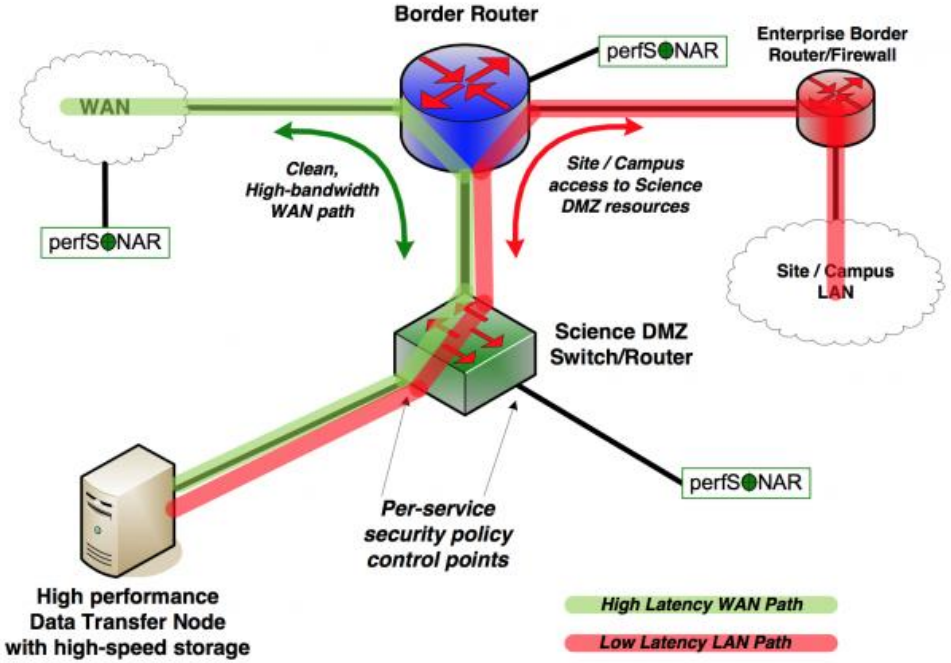
- Evaluate your needs once comfortable (ScienceDMZ scope)
  - Do you have researchers or research teams who need IPv6 for their systems in their communities?
  - Are there other group who might benefit from IPv6 connectivity or eyes on?
    - (Security, Network Operations, etc…)
  - Will you be interacting with any federal systems after 2025?

Campus IPv6 - ScienceDMZ

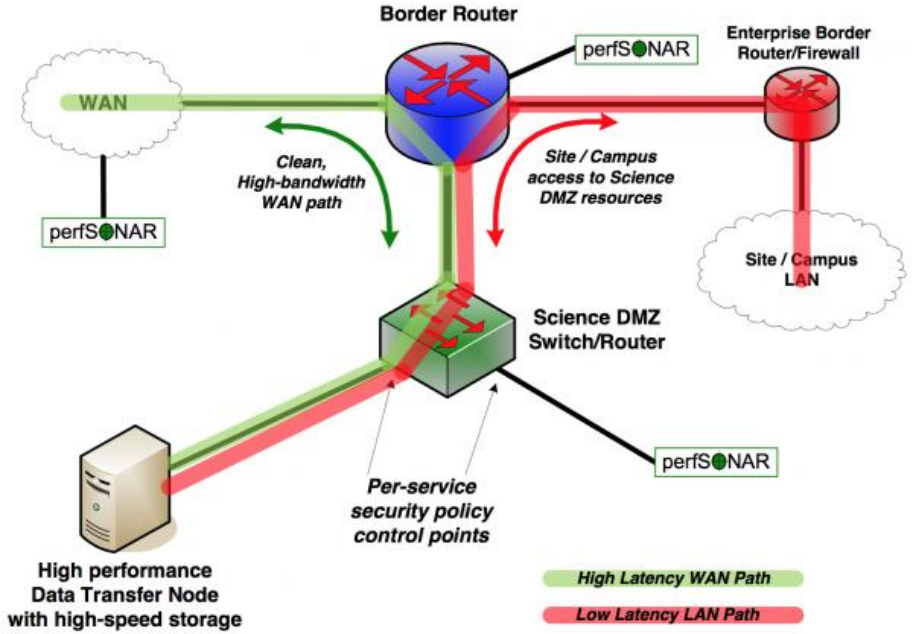
- ScienceDMZ is happy and IPv6 enabled (or best possible) now what?
- Campus look
  - Use what we've learned
  - Leverage the "IPv6 blob" systematically and slowly deploy
  - Language can matter
    - "Legacy IPv4 protocol"

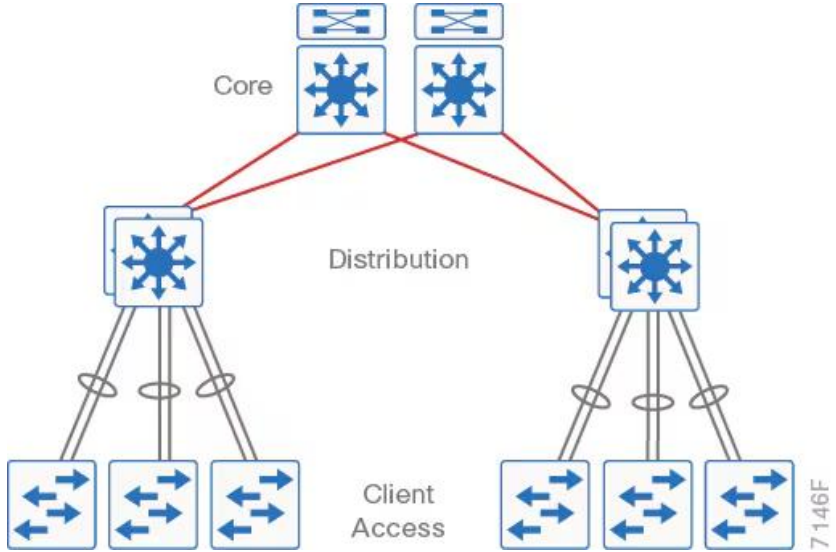
Quick word about the ScienceDMZ pattern

https://fasterdata.es.net



Campus IPv6 - Discussion (~10 - 15 min max)





IPv6 Workshop - Consumer Devices

Consumer Devices - Overview

IPv6 out of the box and then some!

- Operating Systems
  - Linux
  - Windows
  - Mac OS
- Mobile Devices
- IoT - ‘stuff’
- Datacenter / fleet management:
  - OOB / BMC / IPMI / iLo and many more..
  - Management and Stewardship software
- Other?!

Woes and WIN of bring your own device!

- Average person has 16 connected devices!
  - Streaming “smart” TV (chromecast, fire tv, apple tv)
  - Gaming devices
  - Phone(s)
  - Computers
  - Smart watches
  - Tablets
  - Stuff the cat or grad students dragged in…
  - And… and… and…
- Now multiply that number by your entire campus population.

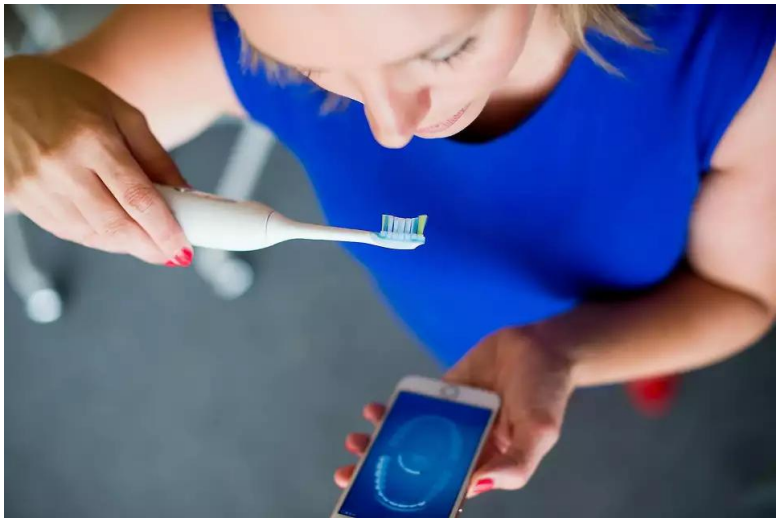
Woes and WIN of bring your own device!

- Is it possible to leverage the vast size that IPv6 offers (think about the quantity of space in a single /64)?
- Often subnets or vlans are not a technical problem to be solved instead a quality of service or even policy solution.
- Can policy be solved with patterns like the ScienceDMZ provides?
- Work with your security teams to integrate solutions and solve surface area issues.
- Routable addresses are great! (ACLs and firewalls let the packets hit the floor!)

IoT - Internet of Things

How does the joke go: “The S in IoT is for security…”

- Toothbrushes act as a DDoS source!
  - Talk about taking a bite out of the internet with IoT



IoT - Internet of Things

- Surface areas and un-trusted /64 areas?
  - How can we leverage IPv6?
- Can zero trust products behave with IPv6?
  - Yes!
  - Keycloak, token exchange products, hashicorp vault, and many many more…
- A very large cloud provider is now “charging” a fee for IPv4 use.
  - IoT tends to have ‘cloudy’ endpoints.
  - Homework left to “us” on where this will go…
- Can cloudy devices not touch production areas with proper planning?

Where are the edges? Instruments or clients stuck in IPv4 only..

- Can a VPN concentrator that offers a IPv6 address and route be provided?
  - Can that VPN have a “split profile” for commodity IPv6 and Legacy IPv4?
    - Let the client route and even have the bonus of non-IPv6 traffic stay out of the path.
- Planning helps to eliminate friction from the ‘client- experience’ of using the networks!
- Example case: Researcher laptops in the DMZ?
  - What is the DMZ in a R&E world?
  - How about remote sensors or data acquisition kit?

Datacenter and “fleet” management

OOB - Out of Band

IPMI - Intelligent Platform Management Interface

BMC - Baseboard Management Controller

LOM - Lights Out Management

Problem statement:

Get thing(s) managed and stewarded by a connection that are not at or near “humans” using IPv6 only.

(Think - Virtual crash cart and much much more as explained by the zero touch provisioning in the AAAA DNS section)

Where we are vs. where the device is?

Out of band devices can be quite advanced and have their own eco systems!

(including many areas that IPv6 can work extremely well)

- Management suites for hardware.
- The BMC device itself
- Management suite ability to call home! (recall github fun…)
  - OEM knocks it out of the park with IPv6 support for all aspects BUT, not the location to pull latest firmware, drivers, mgmt packs, etc…!!!
- OEM / VAR - Work in concert with them they do listen!

Other considerations?

- Device and management planes
  - Number of devices won’t decrease
  - Keep a security hat on
  - Leverage the OEMs

Discussion:

- What are trends that you are seeing?

But I need to talk to IPv4 and I'm IPv6 only!

Not everything is a silver bullet but, there are band-aids.

- There is special dedicated space just for this!
  - Well-Known Prefix 64:ff9b::/96
- RFC 6146 - Stateful NAT64 (Love their ASCII art… Section 1.2.2)
- Open source solutions to help (CLAT)
  - https://github.com/vitlabuda/tundra-nat64
  - https://www.jool.mx/en/index.html
- OEM solutions for production
  - Major Vendors of Firewalls, and Network equipment
  - Load Balance "default" feature.

But I need to talk to IPv4 and I'm IPv6 only! - Drawbacks - Client

NAT64 with DNS64 in concert is an excellent one off solution BUT…

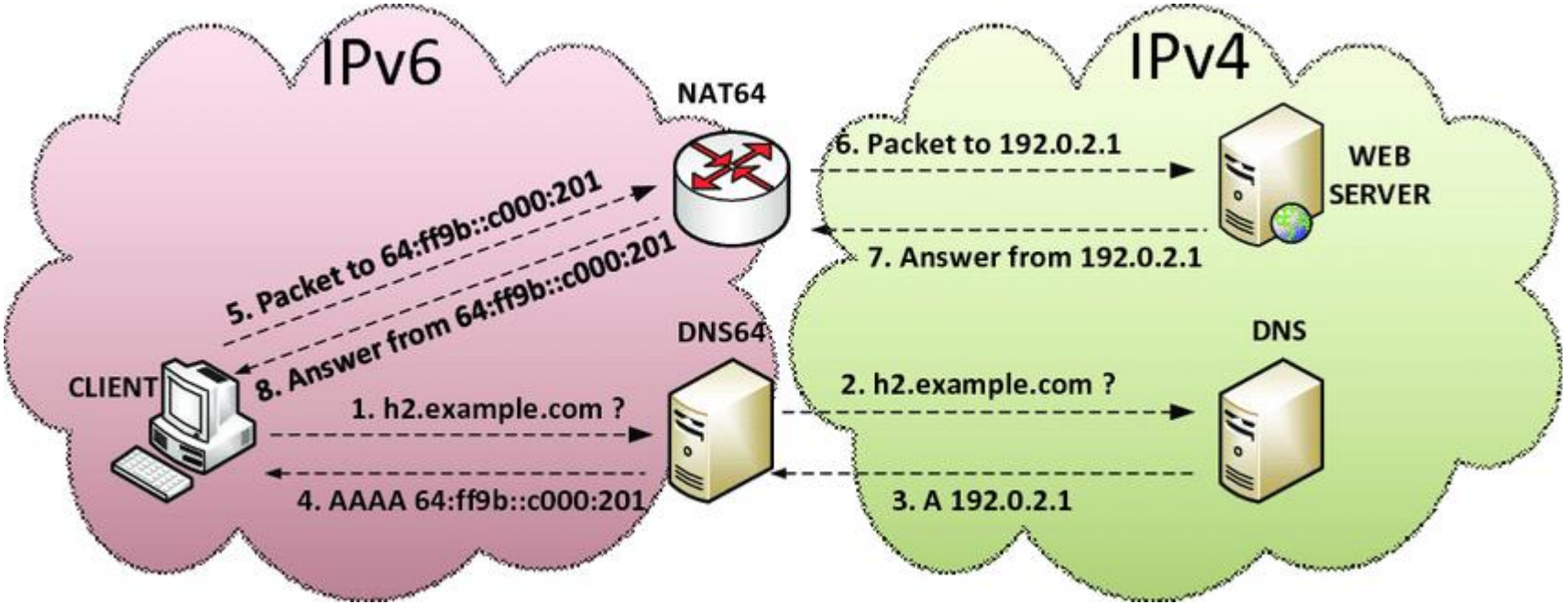
- No less than 8 additional steps that must happen for a simple transaction to occur.
- NAT64 can be a slippery slope…
  - Backup product selection that is IPv4 only yet, needs to be able to switch from push to pull
  - NAT64 will do half the equation… (This won't work and won't scale!!)
- OEMs and VARs will happily sell a subscription or feature set license!
- Open-Source offerings can have unexpected sharp edges.
- Plan accordingly

Nat64 / DNS64 - Success story.

Use case software developers and access to version control

- Oh Github… (But, IPv6 is in progress)
  - Nat64 applied at the OEM firewall
  - DNS64 offers translation (IPv6 enabled devices can talk to Legacy IPv4)
  - Additional overhead but, worth it in this situation.
- Developers extremely happy they can get to github again!
  - And other things… OpSEC team kudos for the catch!
- “Just works” ™ - until it doesn’t

NAT64 - Diagram



Happy Eyeballs (Fast Fallback)

RFC 6555 - Happy Eyeballs: Success with Dual-Stack Hosts

“” When a server's IPv4 path and protocol are working, but the server's IPv6 path and protocol are **not working**, a dual-stack client application **experiences significant connection delay** compared to an IPv4-only client. This is undesirable because it causes the dual-stack client to have a **worse user experience**. This document specifies requirements for **algorithms that reduce this user-visible delay** and provides an algorithm.

“”

Happy Eyeballs (Fast Fallback)

- Client sends out connection attempts on IPv4 and IPv6
- Client uses protocol that responds first
- IPv6 is preferred
- Support is baked into most modern browsers
- Support for proxies and other network devices can vary, check release notes and ask your vendors.