IPv6: Myths vs. Reality

An EDU Perspective

Mark Gardner, Virginia Tech

Adam Klemann, Malone

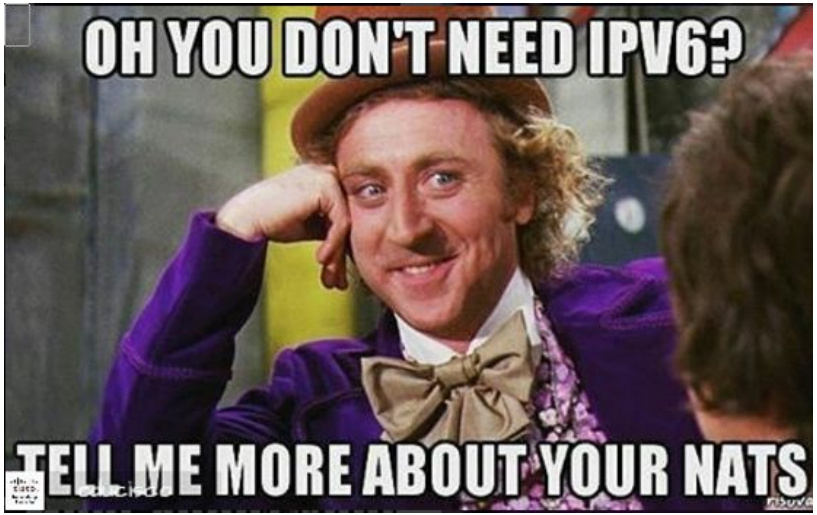
Sticker courtesy of Phil Benchoff

Virginia Tech — Invent the Future®

1892 Malone University — Christ's Kingdom First

Outline

- ***Motivation***
- Context
- Myths & Realities
- Advice
- Summary



https://www.instagram.com/p/BMkHIEnjD4-/

VirginiaTech 1872 Invent the Future®

1892 Malone University Christ's Kingdom First

Not Enough IPv4 Addresses

"A critical point in the history of the Internet was reached today with the allocation of the last remaining IPv4 (Internet Protocol version 4) Internet addresses from a central pool. It means the future expansion of the Internet is now dependant on the successful global deployment of the next generation of Internet protocol, called IPv6." ICANN, 2011-02-03

http://www.icann.org/en/news/releases/release-03feb11-en.pdf

VirginiaTech Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

IPv6 is required (more and more)

"Starting June 1, 2016 all apps submitted to the App Store must support IPv6-only networking."

https://developer.apple.com/news/?id=05042016a

https://upload.wikimedia.org/wikipedia/commons/thumb/f/fa/Apple_logo_black.svg/1024px-Apple_logo_black.svg.png

Virginia Tech 1872 Invent the Future®

1892 Malone University Christ's Kingdom First

IPv6 is already here

With so many devices supporting IPv6, there ***already is*** IPv6 traffic on your network. The question is, shouldn't you be the one to manage it?

http://www.testmart.com/webdata/mfr_promo/IPv6WhitepaperI.pdf

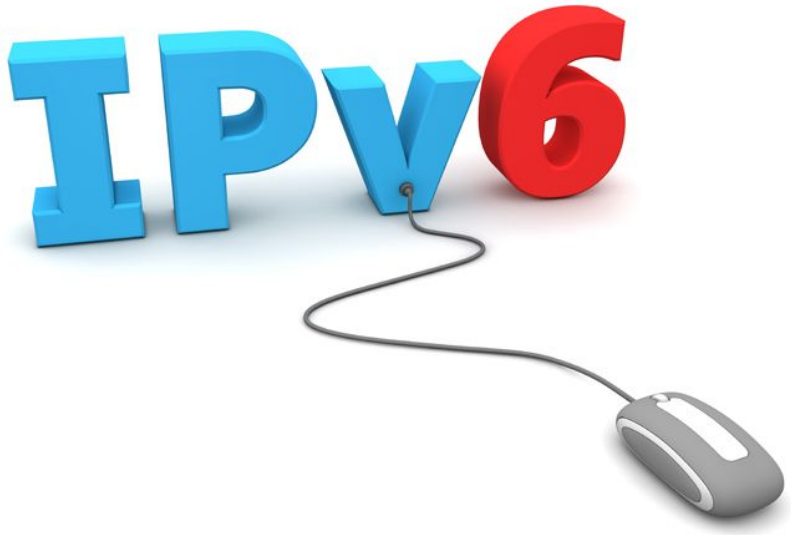
Virginia Tech — Invent the Future®

1892 Malone University — Christ's Kingdom First

(See comments for URLs)

Outline

- Motivation
- ***Context***
- Myths & Realities
- Advice
- Summary



https://www.satheesh.net/wp-content/uploads/Ipv6.jpg

Virginia Tech
Invent the Future®

1892
Malone University
CHRIST'S KINGDOM FIRST

Virginia Tech

Blacksburg, VA

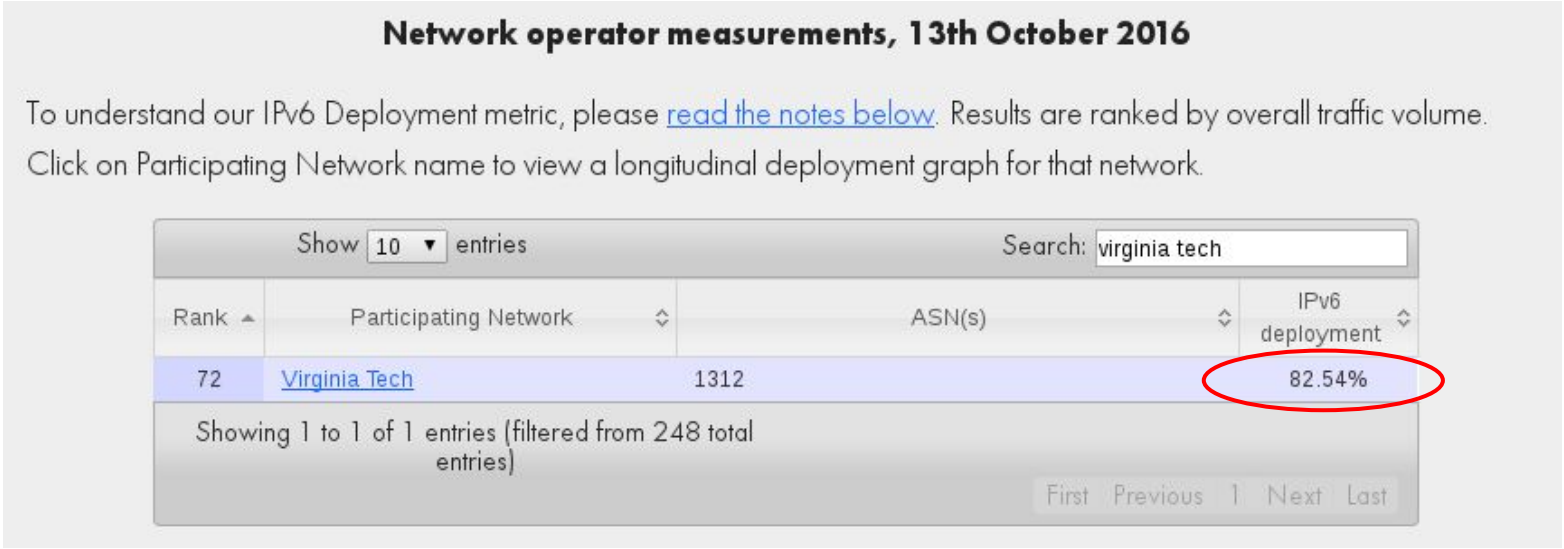
Student population: 25,741 (undergrad), 4,860 (grad)... 31,080 (total)

Facilities: 213 buildings, 2,600 acres (and an airport :-)

Picture credit: http://www.ivanmorozov.com/

VT is highly motivated...

Not enough IPv4 addresses (2 x /16, 2 x /18, 2x /24: around 164,352; currently 30K active WiFi devices at a time, 100K distinct WiFi devices seen in a day)



Network operator measurements, 13th October 2016

To understand our IPv6 Deployment metric, please read the notes below. Results are ranked by overall traffic volume.
Click on Participating Network name to view a longitudinal deployment graph for that network.

Show 10 entries Search: virginia tech

Rank	Participating Network	ASN(s)	IPv6 deployment
72	Virginia Tech	1312	82.54%

Showing 1 to 1 of 1 entries (filtered from 248 total entries)

First Previous 1 Next Last

http://www.worldipv6launch.org/measurements/

IPv6 at VT

- 1997: 6Bone experimentation between ECE and IT
- 1998: early field trial Cisco firmware (a few subnets)
- 2001-2007: Windows, Mac OS, Linux, BSD support IPv6
- 2004: commanded “turn it on and fix whatever breaks”
  - Parallel IPv4 and IPv6 networks in 20 buildings
- 2006: native IPv6 routing on all subnets in data center
- 2009: Google via IPv6; 51% of hosts using IPv6 to access
- 2010: Parallel core routers removed
- *2012: RFC 6540/BCP-177 IPv6 is no longer optional*
- 2016: 81.5% of VT hosts reach Google via IPv6

VirginiaTech
Invent the Future®

1892
MALONE UNIVERSITY
CHRIST'S KINGDOM FIRST

VT's infrastructure

- Border
  - Juniper MX960, distributed
  - Full IPv6 Internet routes
- Core
  - Juniper MX960
  - MPLS, virtual networks, VPN policy
  - NAT bypass for IPv6 and local traffic
- Distribution
  - Juniper EX9208, QFX 5100
  - First hop routing, VRF aggregation
  - Upstream Inter-AS MPLS-routing

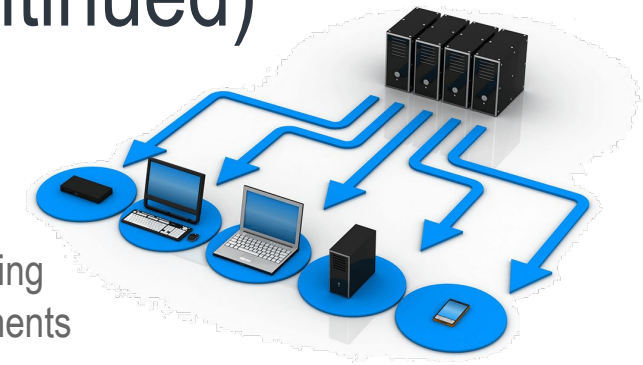
http://accesscomputers.co.in/images/network_infrastructure.jpg

VirginiaTech Invent the Future®

MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

VT's infrastructure (continued)

- Wired
  - Cisco Catalyst desktop switching
  - Layer 2 distribution and access
    - Multicast Listener Discovery (MLD) snooping
    - Need filtering for rogue Router Advertisements
- Wireless
  - Aruba controllers
    - IPv6-aware to cut down on NDP multicast
    - SDP intelligence (Aruba Airgroup)
      - Eliminate another source of multicast
  - Aruba LWAPs: intelligent conversion of multicast to unicast



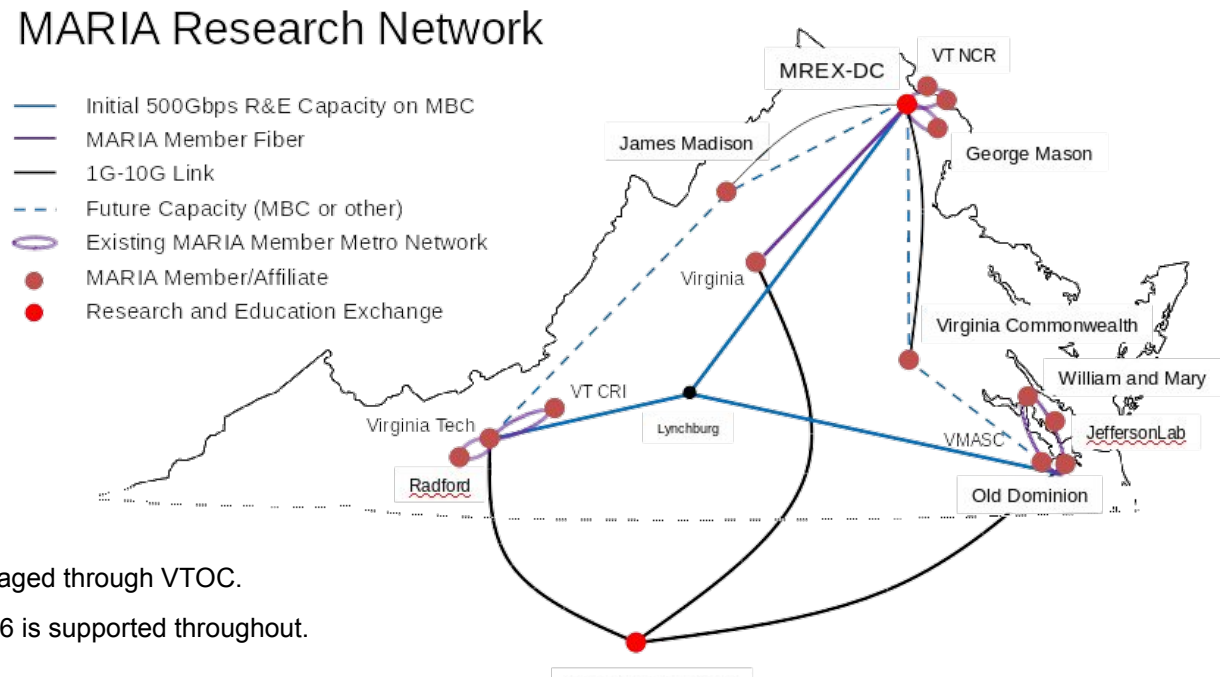
https://jm-restart.co.uk/wp-content/uploads/2015/08/IT-Infrastructure-Computer-Network.png

VirginiaTech Invent the Future®

MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

IPv6 in Virginia

MARIA: Mid-Atlantic Research Infrastructure Alliance



Managed through VTOC.

Native IPv6 is supported throughout.

Virginia Tech — Invent the Future®

Malone University — Christ's Kingdom First

Malone University

Canton, OH

Student population: 1,565 (undergrad), 397 (grad)... 1,962 (total)

Facilities: 17 buildings, 72 acres (no airport :-)

Malone uses a private IPv6 address space

- Replicated successful design using private address space
  - IPv4: 172.16.153.229
  - IPv6: fd00:172:16:153::4bc2 prefixlen 64 dynamic
- Enabled dual-stack on switches that support the configuration
- Migrating others to dual-stack as the equipment is upgraded
  - 10 of 17 buildings completed

VirginiaTech Invent the Future®

MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Malone's infrastructure setup

- Mix of legacy Cisco and newer Enterasys/Extreme switching (currently testing Juniper).
- Registered for IPv6 public address space in 2013
- Upgraded DNS to dual stack in 2014
- Dual-stack DHCP added last year, previous tests used self-assigned or statically set in 2015
- Converted all DMZ servers to dual-stack
- 6000 devices, 3000 active

VirginiaTech 1872 Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Malone's Internet & Internet2 connections

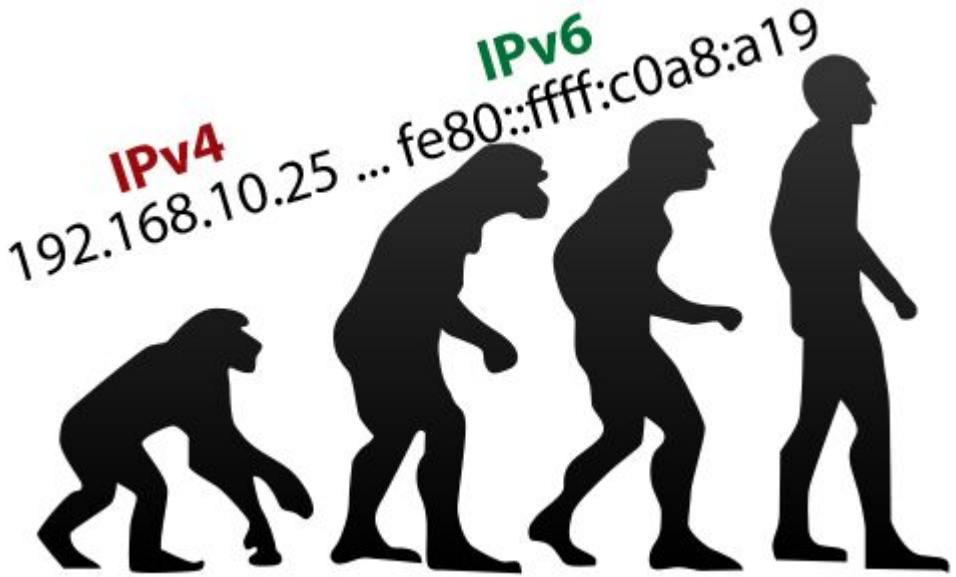
- Three physically diverse fibers to two separate ISPs
- Commodity Internet from three ISPs including statewide academic network partner OARnet
- All connections BGP routed for dual stack

VirginiaTech Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Outline

- Motivation
- Context
- ***Myths & Realities***
- Advice
- Summary

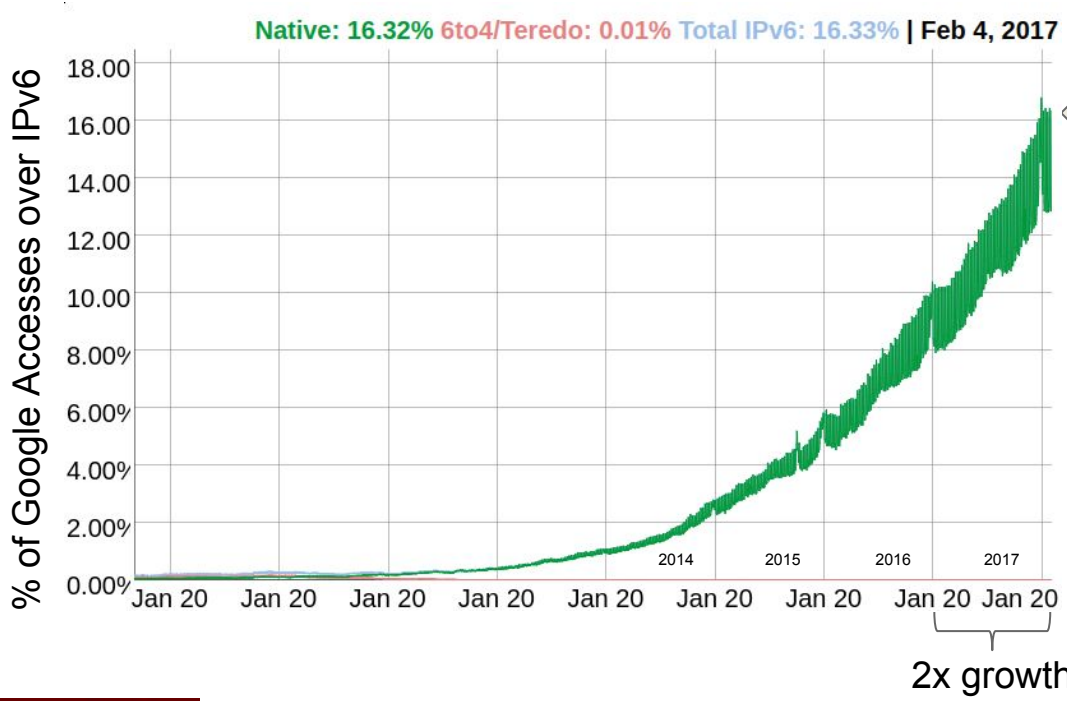


http://www.thetelecomblog.com/wp-content/uploads/2015/07/ipv6-evolution.png

Virginia Tech 1872 Invent the Future®

1892 Malone University Christ's Kingdom First

Myth: No one uses IPv6...



https://www.google.com/intl/en/ipv6/statistics.html

Myth: Content is not available via IPv6

- IPv6 accessible:
  - Google, Gmail, Youtube, Facebook, LinkedIn, Flickr, Snapchat, Wikipedia, Microsoft, Apple…
- IPv6 traffic:
  - 94% of the bytes on VT's network are already IPv6 traffic
  - VT: 29 TB per day (week ending 2017-02-04)
  - Google, search, Gmail, Youtube, etc.: 100%*, 15 TB/day
  - Netflix: 100%*, 12 TB/day

* Of the devices that are IPv6-capable (desktops, laptops, servers, smartphones, etc.)

VirginiaTech 1872 Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Myth: Poor performance

NEW YORK

IPv4 x IPv6 Connection/Total Time Comparison

DOMAIN	CONNECT TIME		TOTAL TIME	
	IPv4	IPv6	IPv4	IPv6
GOOGLE	.031 sec	.030 sec	.061 sec	.055 sec
FACEBOOK	.062 sec	.055 sec	.100 sec	.085 sec
YOUTUBE	.030 sec	.003 sec	.063 sec	.056 sec
WIKIPEDIA	.036 sec	.035 sec	.043 sec	.042 sec
NETFLIX	.036 sec	.068 sec	.050 sec	.085 sec
LINKEDIN	.035 sec	.037 sec	.042 sec	.044 sec
PANDORA	.102 sec	.092 sec	.176 sec	.158 sec
CLOUDFLARE	.029 sec	.030 sec	.035 sec	.033 sec
SUCURI	.035 sec	.035 sec	.041 sec	.042 sec

https://blog.sucuri.net/2016/08/ipv4-vs-ipv6-performance-comparison.html

Performance is comparable (in many cases better)

Myth: IPv6 security is worse (or better)...

- Same / Similar
  - IPSEC (started with IPv6, “backported” to IPv4)
  - Firewall: iptables → iptables6
  - ARP cache poisoning → Neighbor Cache Corruption (control L2 access)
  - P2P ping pong attacks (RFC 6164)
  - Rogue DHCP → rogue DHCP and rogue router advertisements (RFC 6105)
- Different
  - Brute force scanning is impractical, unless…
    - Addresses are assigned according to a pattern (unfortunately, commonly done)
    - IPv4 scan, then lookup IPv6 through DNS (avoids brute force)
      - IPv6-only will mitigate this attack
  - Fragmentation attacks (RFC 6946)
  - IPv6 Extension Header Chain tricks (draft-ietf-6man-oversized-header-chain-09)
  - Dual stack (IPv4 and IPv6)
    - Cross-IP attacks (part IPv4, part IPv6)
    - “Pivot attack”: gain access through IPv4, exploit other machines through IPv6

http://networklessons.com/wp-content/uploads/2013/02/ipv6-logo.jpg

Aside: Firewalls yes, NATs not necessarily

- NAT/NPAT *is not* a security tool
  - Work around for too few IPv4 addresses
  - Not needed with IPv6 (but still an available tool)
    - Malone replicated existing NAT for consistency
- Firewalls *are* a security tool
  - Windows: ICF (IPv4), IPv6 ICF (IPv6)
  - OSX/BSD: ipfw/pf (IPv4), ip6fw/pf (IPv6)
  - Linux: iptables (IPv4), iptables6 (IPv6)

Myth: Apps will break

- Many already work
  - Especially common apps
- Sadly, a few are broken (even for IPv4)
  - Getting better
  - Mostly special purpose / custom apps that need some love

http://jackfreeman.io/wp-content/uploads/2014/09/appstorebroken1.png

VirginiaTech Invent the Future®
1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Reality: IPv6 is not so bad

http://www.thetechlabs.com/wp-content/uploads/2011/02/ipv6-v2.jpg

- Not something to fear or avoid
  - Yes there are some differences
  - But not as much as you may think
- Most equipment supports IPv6 now
  - Most vendors have got the kinks worked out
  - Still, it pays to eval in your environment
- Most apps work out of the box
  - Still some vendors are surprised when asked about IPv6

VirginiaTech
Invent the Future®

1892
MALONE UNIVERSITY
CHRIST'S KINGDOM FIRST

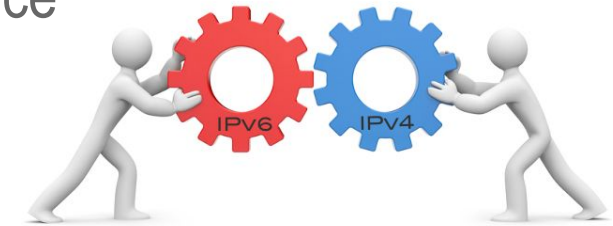
Aside: Why not large scale / CGN (NAT444)?

- Introduces complexity/fragility for users *and* NEs
- Breaks the end-to-end principle
- Significant security, scalability, and reliability problems...
  - ...due to being stateful
- Makes it impossible to host services
  - Perhaps tolerable for home but not good for EDUs
- IPv4 address limit may still be exceeded for certain services
- Logging of translations needed for law enforcement
  - (Although you should be doing this anyway)

VirginiaTech 1872 Invent the Future®
1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Reality: You don't have to go IPv6-only

- IPv4 isn't going away
  - Dual stack (IPv4 and IPv6) will exist for a while
    - But dual stack increases complexity
  - Users will likely not notice which IP they are using
  - Many client apps will not notice
- Need both for now
  - Some content is still IPv4
  - Tipping point is coming soon but not yet here



http://www.nttcom.tv/wordpress/wp-content/uploads/2012/06/Dual-Stack1.jpg

VirginiaTech Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

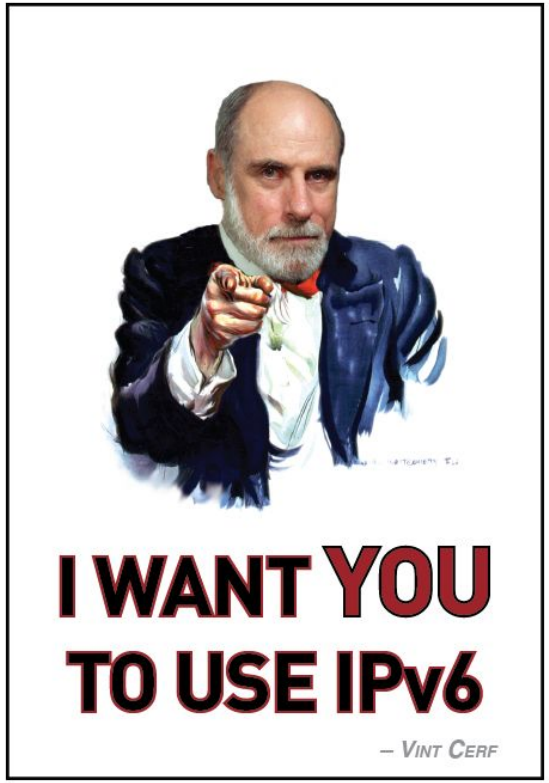
Reality: IPv6-only is (mostly) possible

- Main content providers are IPv6 accessible
  - Google, Gmail, Youtube, Facebook, LinkedIn, Flickr, Snapchat, Wikipedia, Microsoft, Apple...
- Accessing IPv4 content
  - NAT64: translates IPv6 to IPv4 and vice versa
    - Here is a good use of NAT :-)
  - DNS64: synthesizes IPv6 from IPv4
  - VT is testing NAT64/DNS64

VirginiaTech 1872 Invent the Future®
1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Outline

- Motivation
- Context
- Myths & Realities
- ***Advice***
- Summary



VirginiaTech
Invent the Future®

1892
MALONE UNIVERSITY
CHRIST'S KINGDOM FIRST

Advice: Getting Started

- Start with what you know
  - Run parallel IPv6 network until have your bearings
- Plan to unlearn IPv4-isms
  - Could/should things be different?
    - Plenty of addresses, how does that change things?
    - Is NAT really needed?
  - Some things are different
    - Route fragmentation isn't a problem
    - DHCP isn't necessary for assigning host addresses, consider SLAAC

VirginiaTech 1872 Invent the Future®
1892 Malone University Christ's Kingdom First

Advice: Starting Strong

- Put your network engineers on the IPv6 network
  - Problems will get solved fast!
- Access Google, etc., over IPv6… Identifies breakage!
- Purchasing standard: require confirmed IPv6 support
  - Confirm support via eval units in your environment
    - Eval in IPv6-only network to make sure...
  - Ron's rule: if the vendor's web site isn't IPv6 they aren't committed to IPv6 ("Dog fooding" or "eating their own dog food")
  - Does the vendor supply software updates over IPv6?
- Pay it forward: dual stack your own services

VirginiaTech 1872 Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Advice: Getting Used to Differences

- Accept privacy addresses, they are here to stay
  - All major platforms support; Windows enabled by default
  - Can avoid PA on servers but impractical on mobile/laptop
  - “Bite the bullet and record ND & ARP mappings”
- Accept that static address assignment is going away
  - DHCPv6 (“stateful”) vs. SLAAC+DHCPv6 (“stateless”)
  - Benefit: easier to renumber and reconfigure
  - Record mappings over time (useful for security)

VirginiaTech 1872 Invent the Future®
1892 Malone University Christ's Kingdom First

Best Practices

- IPv4-only service should send a reset on IPv6 access
  - Avoids waiting for timeout (“Happy Eyeballs”)
  - If you have to reset, why not make available on IPv6… :-)
- Routing: no change required
  - But configure router advertisements for SLAAC
  - Routing easier due to less fragmented address space
- Randomize address assignments (prevents scanning)
- Consider testing IPv6-only network (future proofing)
  - IPv6-only is useful for testing vendor support

VirginiaTech 1872 Invent the Future®
1892 Malone University Christ's Kingdom First

Challenges

- Different so plan for training
- Dual stack diagnosis can be more difficult
  - "It works for me but not for you"
    - Works via IPv4, but not IPv6
  - First deployment should be the network the NEs use
    - (Can't say this too much…! :-)
- Be aware of which network you are using:
  - Implicit: foo.vt.edu; explicit: foo.ipv4.vt.edu, foo.ipv6.vt.edu
  - Many tools have IPv4/IPv6 options to select the stack

Suggested Reading

- https://blog.cloudflare.com/98-percent-ipv6
- http://packetpushers.net/why-your-network-should-go-ipv6-only/
- https://www.arin.net/knowledge/preparing_apps_for_v6.pdf
- http://www.networkworld.com/article/2231256/cisco-subnet/cisco-subnet-testing-nat64-and-dns64.html/
- https://www.nitrd.gov/nitrdgroups/images/7/7e/IPv6-DREN3-Lessons-RonBroersma.pdf

Outline

- Motivation
- Context
- Myths & Realities
- ***Summary***

http://www.worldipv6launch.org/wp-content/themes/ipv6/downloads/World_IPv6_launch_logo.svg

Virginia Tech 1872 Invent the Future®

1892 Malone University Christ's Kingdom First

http://www.silicon.co.uk/wp-content/uploads/2012/09/Grasko.jpg

Summary

- IPv6 is here to stay
- It isn't scary, just a bit different
- Lots of help is available (including us)
- Many practical benefits

Isn't it about time for you to start using IPv6?

VirginiaTech
Invent the Future®

1892
MALONE UNIVERSITY
CHRIST'S KINGDOM FIRST

Contact Us

- Small Campus Contacts
  - Adam Klemann: aklemann AT malone.edu
  - Jim Shaffer: jshaffer AT malone.edu
  - Shawn Campbell: scampbell AT malone.edu
- Large Campus Contacts
  - Mark Gardner: mkg AT vt.edu
  - Eric Brown: brownej AT vt.edu
  - Phil Benchoff: benchoff AT vt.edu

http://www.crowdfundingpr.org/wp-content/uploads/2014/02/contact-info.jpg

VirginiaTech Invent the Future®

1892 MALONE UNIVERSITY CHRIST'S KINGDOM FIRST

Questions?

http://www.acneeinstein.com/wp/wp-content/uploads/man-with-questions.jpg

VirginiaTech
Invent the Future®

1892
MALONE UNIVERSITY
CHRIST'S KINGDOM FIRST

Extra Slides

https://www.joachim-sicker.de/wp-content/uploads/2014/08/Fotolia_30415714_XS.jpg

Virginia Tech
Invent the Future®

1892
Malone University
CHRIST'S KINGDOM FIRST

Akamai: Adoption by Country

RANK	IPV6 %	COUNTRY
1	46.8%	Belgium
2	27.6%	Greece
3	26.1%	Germany
4	25.6%	Switzerland
5	25.4%	India
6	23.6%	United States of America
7	23.4%	Luxembourg
8	18.3%	Portugal
9	16.4%	Estonia
10	13.6%	United Kingdom

https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp

Akamai: Adoption by Network

RANK	IPV6 %	NETWORK
1	46.2%	Comcast Cable
2	44.3%	AT&T Communications Americas
3	72.7%	Reliance Jio INFOCOMM Ltd
4	25.0%	Time Warner Cable Inc.
5	81.5%	Verizon Wireless
6	59.0%	Sky Broadband
7	29.6%	Cox Communications Inc
8	76.0%	T-Mobile
9	34.0%	Deutsche Telekom (formerly T-Systems USA, Inc.)
10	19.8%	UPC

https://www.akamai.com/us/en/our-thinking/state-of-the-internet-report/state-of-the-internet-ipv6-adoption-visualization.jsp

VT's infrastructure (continued)

- Timer modifications
  - Lower prefix preferred lifetime and max Router Advertisement interval
    - Work in progress
  - Mitigate some roaming problems
- Legacy (not IPv6 aware)
  - Multicast encapsulated in multicast LWAP tunnels
    - Avoids serious micro-burst dropped packet problems