IPv6 – From Assessment to Pilot

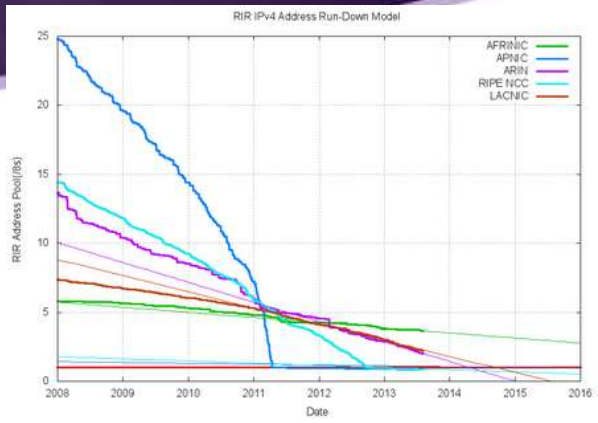
James Small
CDW Advanced Technology Services

Session Objectives

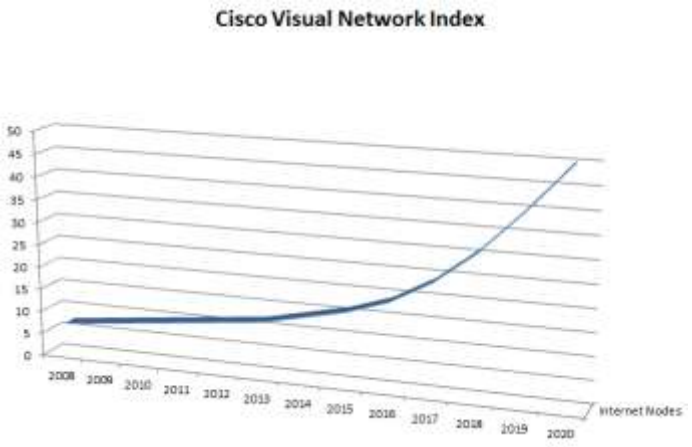
- State of Things
- Business Case
- Plan
- Design
- Implement
- Security & Operations

Current Trends

- Depletion replaced by Growth
- Population penetration
- Multiple mobile device penetration
- The Internet of Things – M2M
- The Internet of Everything

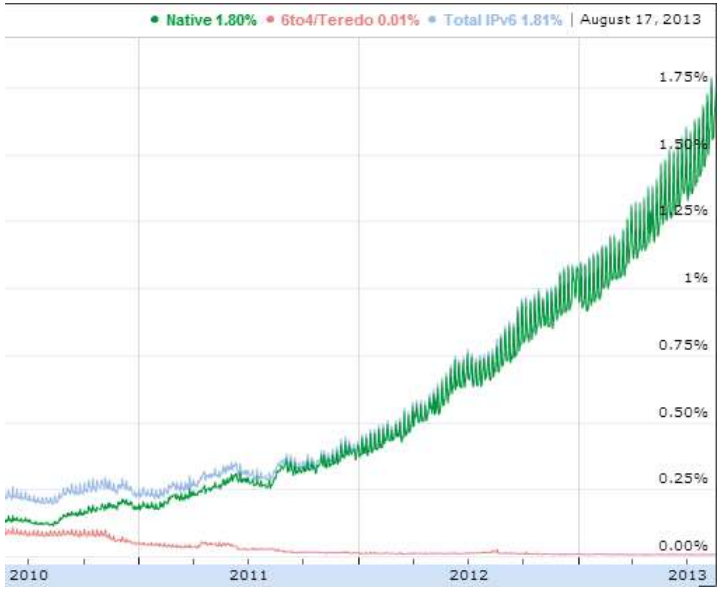


Geoff Huston's IPv4 Address Report



Current Trends

- Global growth:
  - Penetration doubling every 9 months
- US penetration:
  - IPv6 Deployment: 24.76%
    - Prefixes: 40.78%
    - Transit AS: 59.48%
    - Content: 47.72%
    - ***Users: 3.92%***
  - Relative Index: 6.2 out of 10

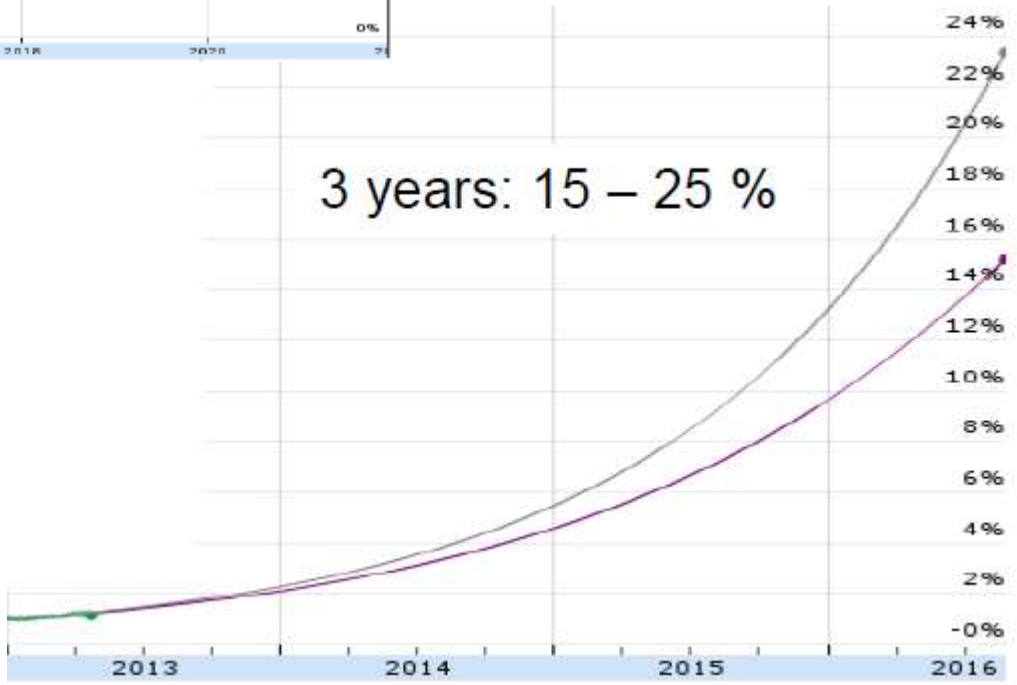


Google's global IPv6 statistics graph

Global IPv6 growth

Graphs from Cisco Live Orlando 2013 – PSOSPG 1330

- *US Growth/Penetration is Double the Global Rate*
- *Critical mass in US next year (10% penetration)*



Opinions on Action

- Gartner – Enterprises must start upgrading their Internet presence to IPv6 now
- Deloitte – In short, we recommend starting (v6 deployment) now
  - "Starting sooner can give organizations enough lead-time for a deliberate, phased roll-out, while waiting could lead to a costly, risky fire drill."

Roadmap

- State of things
- ***Business Case***
- Plan
- Design
- Implement
- Security & Operations

New Trends

- IPv6-Only Data Centers and Networks (especially mobile ones) on the rise
- Internet-of-Things – many key protocols are IPv6 only (IPv4 doesn't have necessary scale)
- Many new trends are IPv6-Only (e.g. IoT)
  - Smart Factories/Buildings/Cities/Grid
  - Intelligent Transportation System

General Business Case

- 65% of Cisco Enterprise Technology Advisory Board members will have IPv6 web sites by the end of this year (2013)
- Top drivers for IPv6
  - BYOD
  - Globalization
  - Internet Evolution/Internet Business Continuity (B2B/B2C)

Legal Business Cases

- Mobile (Tablets/Smartphones)
  - LTE/4G an IPv6 technology
- Multinational Firms – Europe far down the IPv6 path, where are you compared to your counterparts?
- Federal – Goal for full IPv6 deployment by 2014 with some trying to eliminate IPv4 by years end (VA)

Legal Business Cases

- IPv6 Critical mass is coming next year (2014) – B2B, B2C, M2M, and other innovation will follow. Are you ready?
- The Internet of Everything (Traditional Internet, Mobile Internet, and the Internet of Things) is bringing a raft of policy issues to the forefront.
  - Many will be seeking expert counsel from leading technology firms.

What's IPv6 Worth?

- Next-generation workers (BYOD, mobile collaboration, telecommuting, VDI): $2.16 trillion
- Smart factories: $1.95 trillion of total Value at Stake
- Connected marketing and advertising: $1.95 trillion of total Value at Stake
- Smart grid: $757 billion of total Value at Stake
- Smart buildings: $349 billion of total Value at Stake

Is IPv6 Real?

- Penetration on AT&T's Network: 10.72%
- Penetration on Verizon's Mobile Network: 33.37%
- Carriers deploying CGN because of IPv4 depletion:
  - AT&T (in many cases with U-verse you can no longer get a public IPv4 address – even for business) ☹
  - Verizon (allows opt-out in some cases)

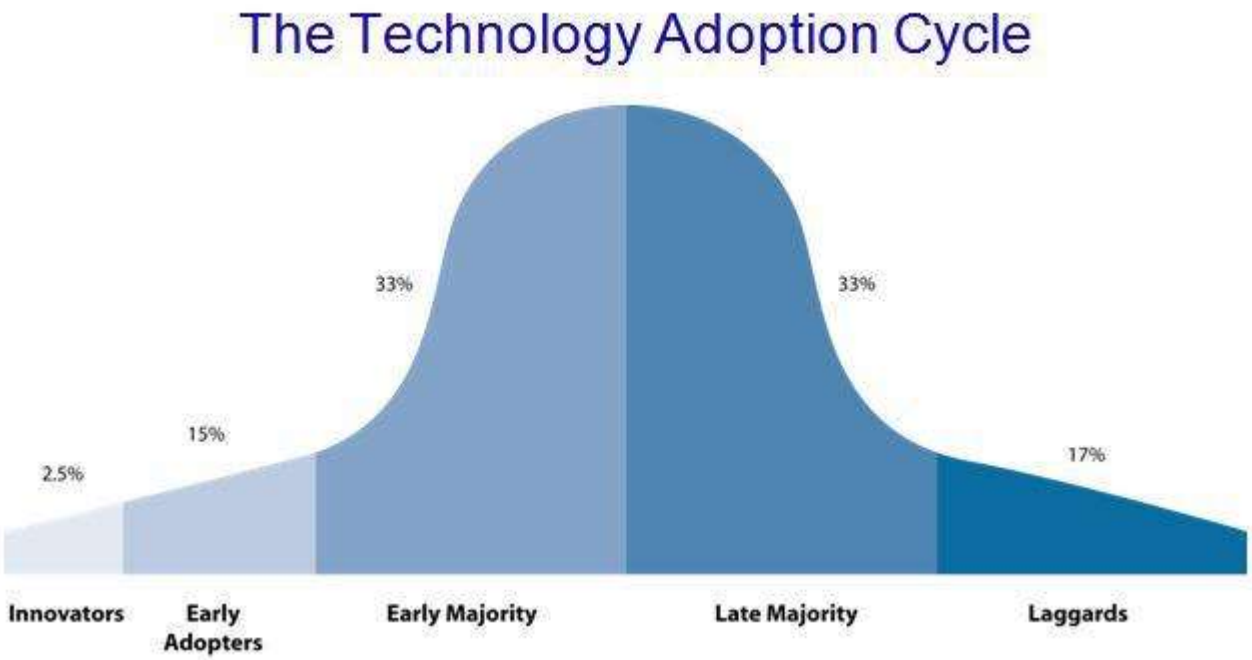
Procrastinator's Guide

How Long to Deploy?

Organization Size	Rough Timeline
Small	1-2 years
Medium	2-3 years
Large	3-4 years
Multi-national	4-5 years

Procrastinator's Guide

When do you adopt technology?



2013 the catalyst

Procrastinator's Guide

Based on Your Technology Adoption Point:

Organization Size	Innovator	Early Adopter	Early Majority	Late Majority	Laggard
Small	-	Challenge	2014 Q3	2015 Q4	2017 Q4
Medium	-	-	2013 Q3	2014 Q4	2016 Q4
Large	-	-	Challenge	2013 Q4	2015 Q4
Multi-National	-	-	-	Challenge	2014 Q4

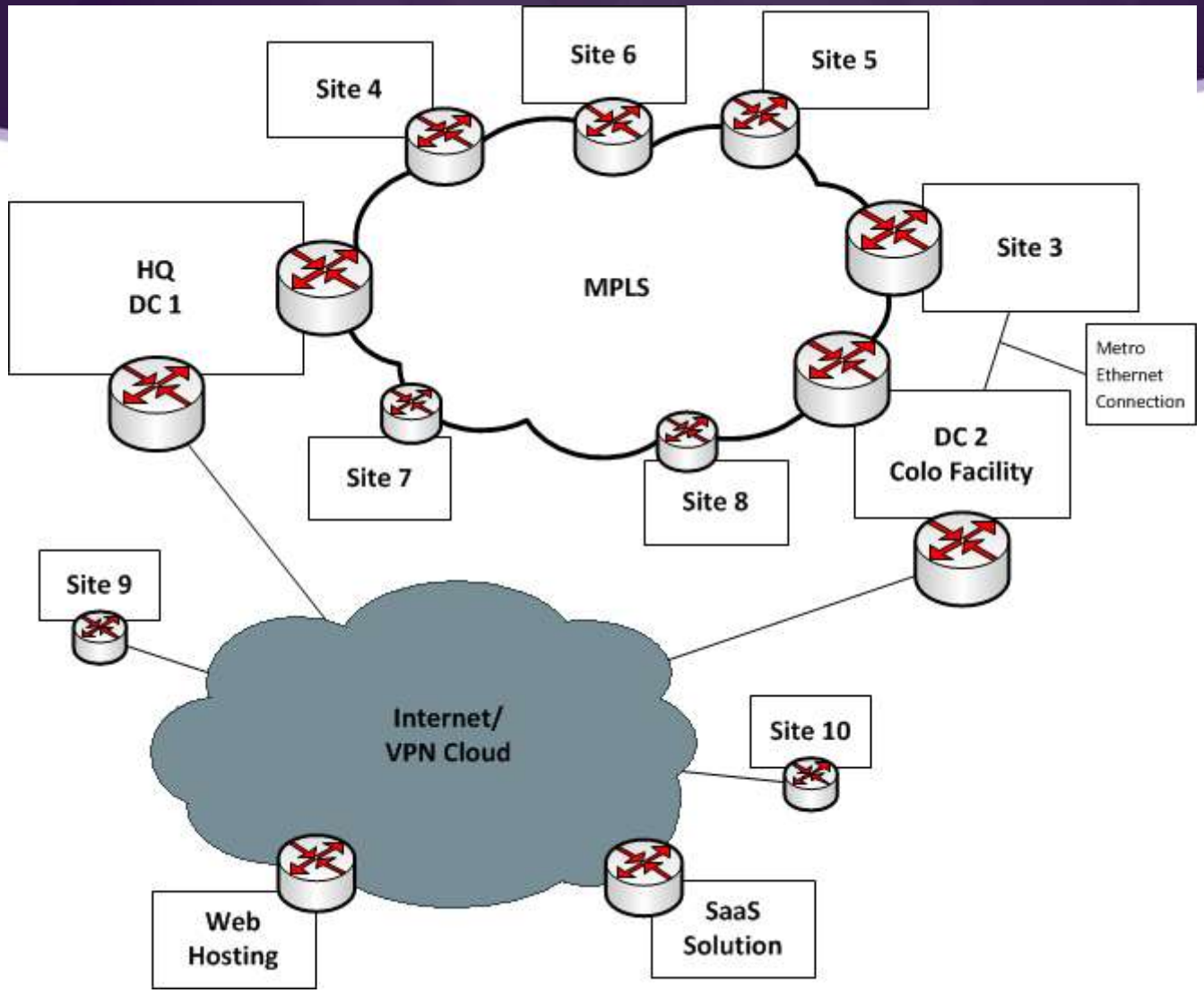
Roadmap

- State of things
- Business Case
- ***Plan***
- Design
- Implement
- Security & Operations

Getting Started - Planning

- LNP – A fictitious mid-size company
  - 500 employees
  - 10 sites
  - IT department and some outsourcing
  - Many business partners (B2B)
  - Services for both business and consumer (B2B/B2C)
  - Technologies include BYOD/VDI/Telecommuting/Ubiquitous Collaboration

LNP Topology



Planning – Assessment

- Need an accurate topology diagram
- Need a comprehensive inventory
  - All network infrastructure items
  - All client/server/mobile operating systems
  - All client/server/mobile applications
  - All telecommunications circuits/services
  - All business partners/services

Assessment - Network

- Network Infrastructure Devices
  - IPv6 supported by device?
  - IPv6 supported in accelerated path or slow path?
  - IPv6 performance equivalent to IPv4?
  - Hardware/software upgrade(s) required for IPv6 support?
  - IPv6 support includes necessary/desired features?
  - Where device doesn't cut it what's the work around and/or replacement?

Assessment – O/S

- Client/Server/Mobile Operating Systems
  - IPv6 supported? Fully?
  - DHCPv6 fully supported?
  - RDNSS supported?
  - Where O/S doesn't cut it what's the work around and/or replacement?

Assessment - Apps

- Client/Server/Mobile Applications
  - IPv6 supported? Fully? Documented? Examples?
  - IPv6 support validated by independent test lab?
  - Need to develop vendor ranking:
    - 5 - Official support (documentation & testing)
    - 4 - Claimed support (limited/no documentation or testing)
    - 3 - No official statement, but employees claim support via forums/blogs)
    - 2 - No official statement, but non-employees claim support
    - 1 - No official statement, forums/blogs state some support
    - 0 – No information available

Assessment - Telecomm

- Telecommunications Circuits/Services
  - Native/Dual Stack IPv6 Internet service available?
  - If not native, tunneled service?
  - Dual Stack MPLS service available (6VPE)?
  - Dual Stack Managed Internet and Security (e.g. Firewall) service available?
  - Dual Stack SIP service available?
  - Options/time lines where native/dual stack not available?

Assessment – B2B

- All Business Partners/Services
  - Partner/service supports dual stack?
  - Options/time lines where native/dual stack not available?

- Examples
  - Web/Application/”Cloud” Hosting
  - E-mail
  - B2B

Assessment - Accreditation

- IPv6 Ready Logo Program:
  - https://www.ipv6ready.org/

- USGv6 – NIST IPv6 Technical Standards Profile:
  - http://www-x.antd.nist.gov/usgv6/index.html
  - Certifying Labs (UNH IOL, ICSA Labs)

Procurement

- Update procurement policies to require IPv6 support – leverage existing templates:
  - NIST SP500-267 - A Profile for IPv6 in the U.S. Government – Version 1.0:

    http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf
  - RIPE 554 - Requirements for IPv6 in ICT Equipment (Obsoletes RIPE-501):

    http://www.ripe.net/ripe/docs/ripe-554

Policies & Procedures

- Policies and procedures will need to be updated
  - How will new and existing standards be updated to support/include IPv6?
- Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government

  https://cio.gov/wp-content/uploads/downloads/2012/09/2012_IPv6_Roadmap_FINAL_20120712.pdf

Training

- How will you and your team train on IPv6?
  - Instructor Led?
  - Online/Videos?
  - College Courses?
  - Books/Publications?
  - Labs?
  - Hands on?
  - Timeline?

Roadmap

- State of things
- Business Case
- Plan
- ***Design***
- Implement
- Security & Operations

Designing

- Address Plan
- Phases
- Timeline
- Project Plan

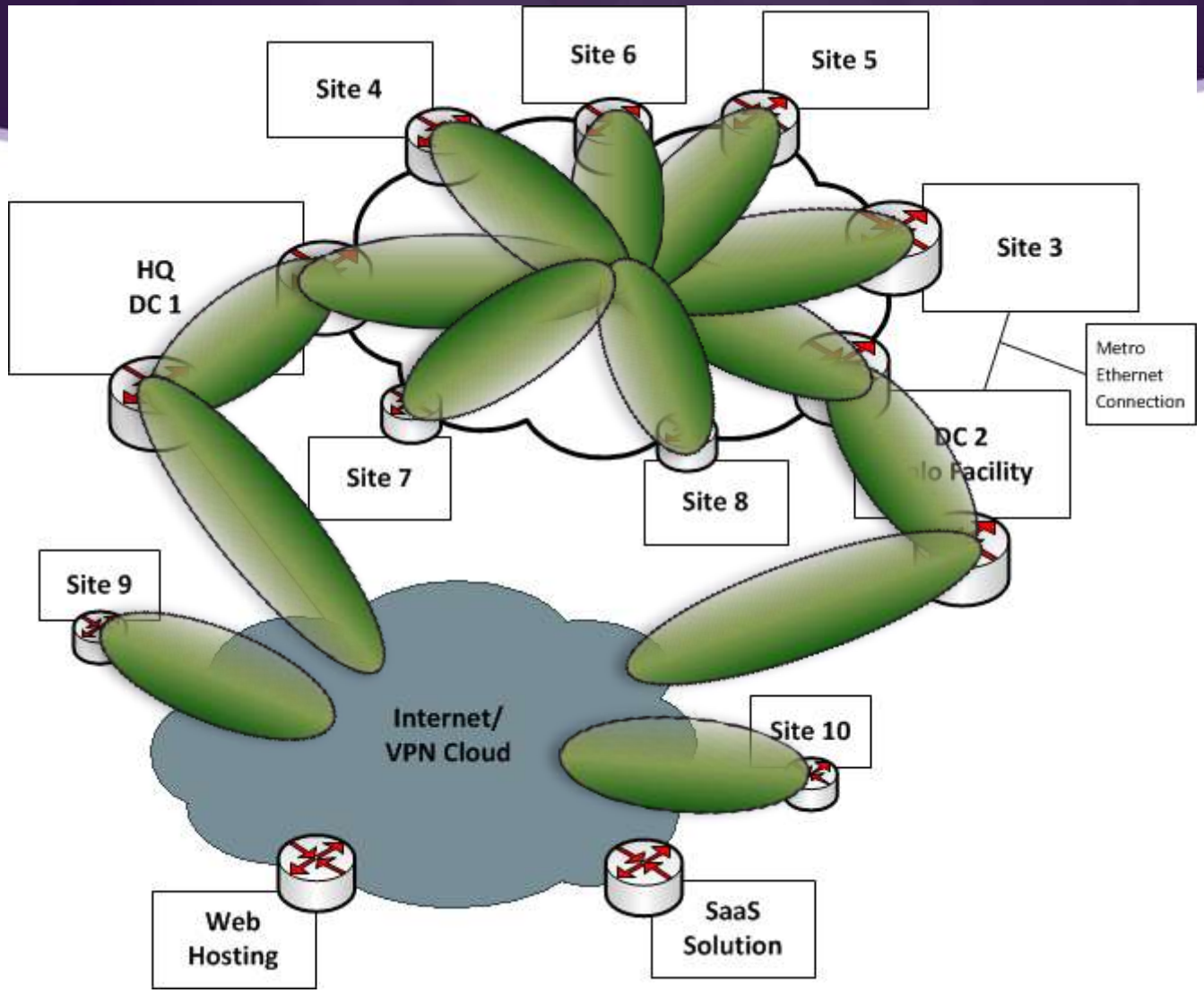
Designing – Address Plan

- Set aside some serious time to do this well or you'll be kicking yourself later
  - /44 from ARIN
    - 2001:db8:abc0::/44
      - 2001:db8:abc[region]:[sitep1][sitep2][PIN][Instance]::/64
        - Region - 4 regions in US roughly along time zone boundaries and then North and South
        - Site - 256 site codes
        - Place In Network - Management, Lab, DMZ, Server, User/Desktop, etc...
        - Instance - User VLAN 1, User VLAN 2, User VLAN 3, etc...

Designing - Approach

- Recommended approach – Core to Edge
  - Enable IPv6 in your network core
    - Routing Protocols
    - WAN
  - Allows time to learn and deploy IPv6 without impacting users, servers, and applications
  - Eventually connect Internet Edge
  - Start with test VLAN(s) and SSID(s) – limited access, tightly controlled

Core to Edge Approach



Designing - Phases

- IPv6 will need to be phased in
- Labs are great but may not be a realistic option for many companies
  - A typical enterprise has a limited lab or staging areas which can be used for basic proof of concept
  - If you have a lab which simulates production and resources available which can mock up a complete IPv6 deployment then bonus!

Designing - Phases

- Using your topology diagram carve up your network into phases
- Start with sites with a large IT presence
- Talk to your WAN carrier – do they support dual stack for MPLS or your WAN technology?
  - If not you must look at other carriers or do an overlay… ☹
- Talk to your ISP – do they support dual stack?
  - If not you can tunnel or consider other ISPs

Designing - Phases

- Phasing in service will typically require coordination with your WAN provider and ISP
- Does your WAN optimization, VPN/encryption, and Network Management and Monitoring Systems all support IPv6?
- Plan out all network infrastructure upgrades/refreshes necessary to support IPv6 as part of the phased approach
- Plan out change management and testing for each phase/site

Designing - Timeline

- Phasing in IPv6 to 10 sites
  - Need to space out upgrades/refreshes
  - Need to follow change management procedures/windows
  - Upgrading network infrastructure results in an outage so typically off-hours and restricted days/times
  - Not all windows available – monthly/quarterly/yearly freezes/restrictions to contend with
  - Most people don't typically enjoy working every weekend
- This could take 6-12 months – planning out is key

Designing - Timeline

- Network Deployment is just the start of IPv6
- You need to think through rolling it out to all servers and applications – this is the most involved part of the project
- Coming up with a high level time line and building a project plan around that is key to provide realistic goals and deadlines

Roadmap

- State of things
- Business Case
- Plan
- Design
- ***Implement***
- Security & Operations

Thoughts on Pilots

- How many of you piloted:
  - Your new E-mail system (e.g. Exchange)?
  - Your new UC/collaboration system (e.g. Cisco UC or Microsoft Lync)?
  - Your new CRM solution?
- Treat IPv6 similarly – if you typically conduct a pilot for new large scale solutions then have at it. If not, then don't.

Implementing

- With the multi-phase design plan begin the project
- If you have a lab or staging area it can be used to validate software/configurations before deploying
- If not – that's why you have change control, change windows, testing, and back out plans
- A strong project manager and management buy in is crucial

Implementing

- Obtain an IPv6 Network Address from ARIN
- Make sure you can monitor and control/block IPv6
  - NMS support
  - ACLs/Firewalls support IPv6 and have appropriate controls in place
- Make sure your initial deployment includes a test VLAN and SSID connected to the IPv6 core

Implementing

- Once the core is deployed you can look at connecting to the Internet
- Risk is low – your firewall will block inbound access
- Outbound access is limited to the tightly controlled test VLAN(s)/SSID(s)
- Once you are confident with your setup look at expanding the test networks to include all of IT and select test users

Implementing

- Once any issues are addressed, the next phase is expanding the access layer to include more users
- The more challenging piece is to begin adding servers to the IPv6 deployment
  - Each server/application should be tested to insure all functionality works with dual stack
  - Enlist the aid of SMEs and the Vendor
  - Adding servers should leverage change control

Roadmap

- State of things
- Business Case
- Plan
- Design
- Implement
- ***Security & Operations***

Security Concerns

- VPN Bypass
- Router Advertisement Spoofing/Flooding
- DHCPv6 Spoofing
- Remote Scanning/DoS Attack
- Monitoring and Detection
- Preventing Tunneling and Firewalling
- Loss of NAT “Security”

Monitoring/Detecting IPv6

Service	Number	Description
IPv6 Encapsulation	IPv4/41	Tunnel IPv6 over IPv4
Generic Tunnel	IPv4/47	Tunnel anything over GRE
Teredo/Miredo	UDP/3544	Tunnel IPv6 over UDP (NAT Traversal)
Teredo/Miredo	Non-Standard	IPv6 destination starting with 2001:0000::/32 over UDP over IPv4
TSP	TCP|UDP/3653	IPv6 Tunnel Broker using the Tunnel Setup Protocol (RFC 5572)
AYIYA	TCP|UDP/5072	IPv6 Tunnel Broker using Anything in Anything (www.sixxs.net/tools/ayiya/)
Public 6to4 Anycast Relay	IPv4:192.88.99.1	Starting with IPv6 source address of 2002::/16 (6to4 is IPv6 over IPv4/41) Destined to 192.88.99.0/24 for IPv4
IPv6 Encapsulation	TCP/443	IPv6 over IPv4 SSL Tunnel, many variants
IPv6 Ethertype	0x86DD	Distinct from IPv4 Ethertype (0x0800)
DNS IPv6 Records	Several	AAAA, updated PTR records - can be transported over IPv4 or IPv6

Image source: gfi.com

Example Firewall Policy

Block Tunneling IPv6 through IPv4 network:

Source Criteria:			Destination Criteria:		Service	Action	...	...	...	Description
Source	...	...	Destination	...						
ing rules, 9 filtered rules)										
any			any		41	Deny				Protocol 41 (IPv6 over IPv4 - ISATAP, 6to4, 6rd, 6in4, 6over4)
any			192.88.99.0/24		ip	Deny				Public 6to4 Anycast block
any			any		gre	Deny				GRE
any			any		3544	Deny				Teredo/Miredo
any			any		3563	Deny				TSP
any			any		5072	Deny				AYIYA
any			any		ip	Permit				

If you don't want IPv6 traffic going through a firewall then explicitly block it!

IPv6 Access Control

Source Criteria:		Destination Criteria:		Service	Action
Source	... ...	Destination	...		
ming rules)					
any6		any6		IPv6-Ops packet-too-big parameter-problem time-exceeded unreachable	Permit

- Don't block all ICMPv6!!!

Source Criteria:		Destination Criteria:		Service	Action
Source	... ...	Destination	...		
ming rules)					
any4		any4		IPv4-Ops parameter-problem time-exceeded unreachable	Permit

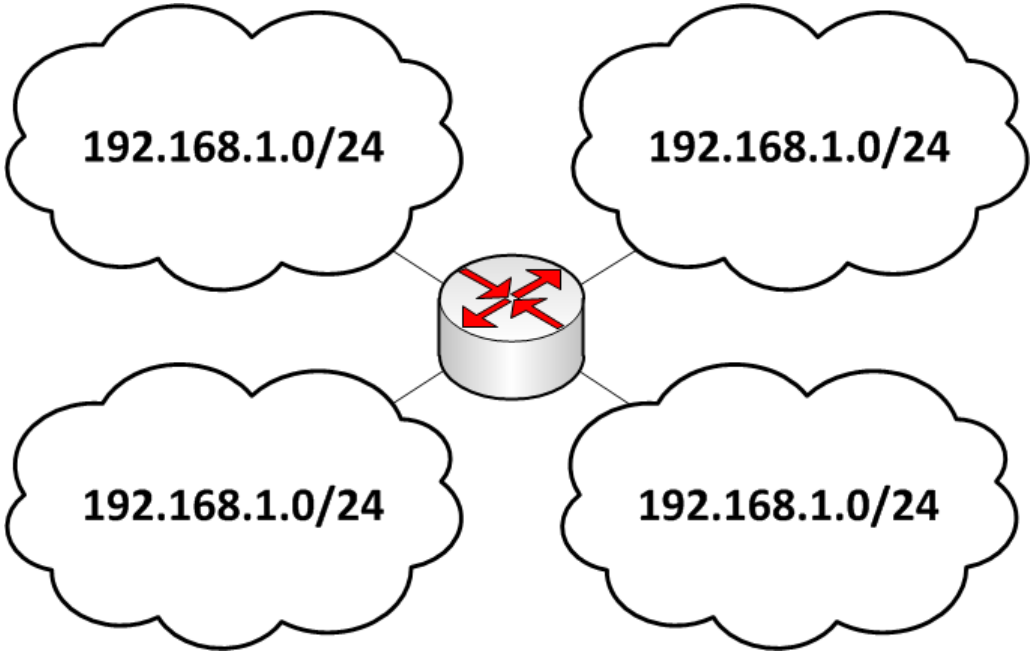
- Good References - NIST SP 800-119 & RFC 4890

Loss of NAT "Security"

- NAT provides topology hiding – giving that up requires some getting use to
- Consider:
  - NAT adds tremendous complexity. You want to deploy the latest UC or multimedia solution? Sorry, our security solution doesn't support that version yet (because of NAT).
  - The majority of the security comes from stateful firewall inspection and well configured policies – not from NAT.
  - The vast majority of attacks are user initiated "drive by downloads" which NAT does not protect against

NAT Challenges

- NAT adds substantial operational complexity. Consider the following common B2B scenario. What's the business value proposition for NAT again?



Operations

- Good training will help ensure smooth operations
- Validate escalation paths for critical systems/applications – standard IT operations but make sure procedures are up to date with IPv6 deployment
- Create an IPv6 task force to quickly address any problems from deploying IPv6
  - Up front testing, change control, and good project management will prevent most issues

What Partners Can Help With

CDW ATS IPv6 Services

- IPv6 Educational and Planning Workshop
- IPv6 Readiness Assessment
- IPv6 Pilot
- IPv6 Design and Deployment
- DirectAccess Deployment – An IPv6 Solution

Questions

Backup Slides

Appendix

Redmond's Stance

Per the Microsoft IPv6 FAQ:

"From Microsoft's perspective, IPv6 is a mandatory part of the Windows operating system and it is enabled and included in standard Windows service and application testing during the operating system development process. Because Windows was designed specifically with IPv6 present, Microsoft does not perform any testing to determine the effects of disabling IPv6. If IPv6 is disabled on Windows 7, Windows Vista, Windows Server 2008 R2, or Windows Server 2008, or later versions, some components will not function. Moreover, applications that you might not think are using IPv6—such as Remote Assistance, HomeGroup, DirectAccess, and Windows Mail—could be."

Disabling IPv6 in Windows

What breaks if IPv6 is disabled on Windows Vista and Later?

- Hyper-V Cluster - It is not possible to add a new node to an existing cluster
- TMG Server - RRAS breaks
- Exchange - Mail flow & Installation problems
- SBS Server - Exchange services fail to start & network shows offline
- DirectAccess - Does not work
- HomeGroup - Does not work
- Applications using Windows Peer-to-Peer Networking will not work