



DEVELOPING AN IPV6 ENTERPRISE PILOT PROGRAM

James Small
CDW Advanced Technology Services

SESSION OBJECTIVES



- Creating Your IPv6 Pilot Plan
- Initial Pilot Roadmap
- IPv6 Changes
- IPv6 Security
- Pilot Phase 2
- Parting Thoughts

Q&A throughout, I may postpone questions until the end depending on time

ROADMAP



- ***Creating Your IPv6 Pilot Plan***
- Initial Pilot Roadmap
- IPv6 Changes
- IPv6 Security
- Pilot Phase 2
- Parting Thoughts

INITIAL PILOT PLAN



- Scope
 - » Production Impact
 - » Goals
 - » Hardware
- Team
 - » Implementers
 - » Testers
 - » Project management
- Location
 - » Deployment
 - » Testing

INITIAL PILOT PLAN



- Schedule
 - » Duration
 - » Deployment
 - » Testing
- Training
 - » Material
 - » Tailored
 - » Support
- Communication
 - » Infrastructure status
 - » Solution/Application issues
 - » Testing issues/progress

INITIAL PILOT PLAN



- Evaluation
 - » Infrastructure goals
 - » Success criteria
- Risks and Contingencies
 - » Incident response
 - » Project failures

PILOT PLAN – INITIAL HARDWARE



Key Infrastructure Items:

- Internet Router – 2900 series
- Internet/DMZ/LAN Switches – 3560 E, X, or C-Series
- Internet Firewall – ASA
- WLC – 2504/5508/vWLC and one or more supported APs
- Beefy server or blade chassis to run Hypervisor host(s)
- Lots of laptops

PILOT PLAN – INITIAL HARDWARE



Bonus Items:

- Load Balancer
- Forward and Reverse Proxy
- ASR 1k
- ACS 5.4
- SIEM Server with IPv6 support
- NetFlow Collector with NetFlow v9 support

PILOT PLAN – INITIAL SOFTWARE



Key Services

- Dual Stack DNS Server with DNS64 support
- Dual Stack DHCP/DHCPv6 Server
- Dual Stack File Server
- Dual Stack Web Server
- Key Applications

Bonus Items:

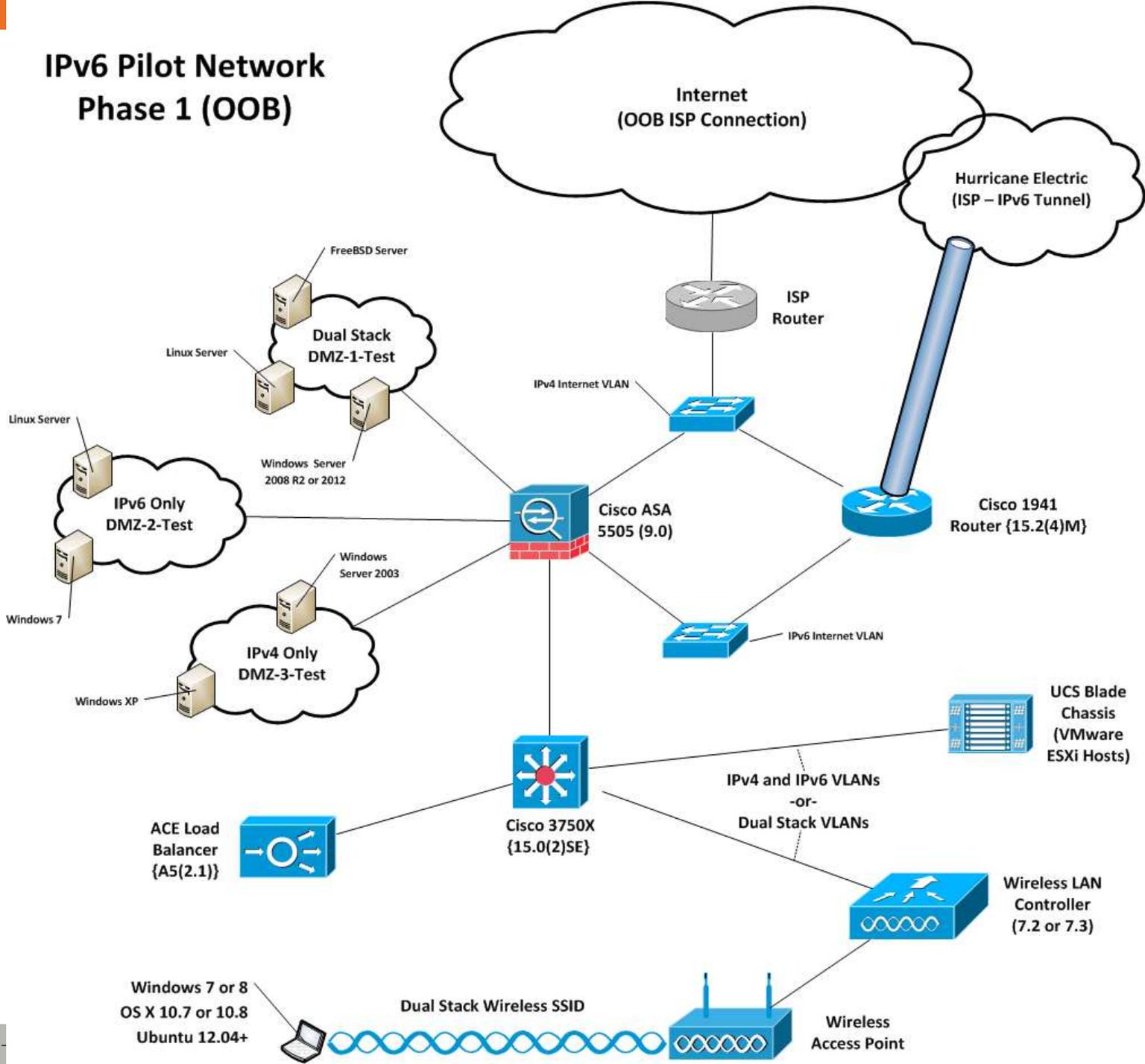
- IPAM Solution

ROADMAP



- Creating Your IPv6 Pilot Plan
- ***Initial Pilot Roadmap***
- IPv6 Changes
- IPv6 Security
- Pilot Phase 2
- Parting Thoughts

IPv6 Pilot Network Phase 1 (OOB)



INITIAL PILOT ROADMAP



- Obtain IPv6 /48 Prefix
- Pilot Addressing Plan
- Design and Build Out
- Address Provisioning
- DMZ Setup
- Internal Network Setup



Image source: northeritrust.com

OBTAIN AN IPV6 NETWORK ADDRESS



- Sign up for free IPv6 Internet access from Hurricane Electric (<http://tunnelbroker.net>)
- With your account, request a /48 prefix
- Q: Why start with Hurricane Electric?
- A: It works great, service is available from anywhere on the Internet, and you get a /48 all for free.
- Most important aspect of starting with HE:
 - » You need practice creating an addressing plan and deploying IPv6. It will take you at least 3 times to get your addressing plan right so let's get started...



Image source: beachdecorshop.com

PILOT ADDRESS PLAN GUIDELINES



Developing a great address plan takes practice

- Site - /48
- Loopback Network - /64
- Loopback - /128
- Translation Services - /56
- Point-to-Point - /126
- Everything else - /64

	NAME	STREET	CITY	STATE
1				
2	LOMAR TAXIDERMRY	1401 AUSTIN ST	ABILENE	TX
3	HAMMER'S TAXIDERMRY	1711 ELM DALE RD S	ABILENE	TX
4	VERRIPS TAXIDERMRY STUDIO	10655 US HIGHWAY 87 S	ADKINS	TX
5	NOURI'S TAXIDERMRY	11465 FORD RD	ADKINS	TX
6	LAKE FORK TAXIDERMRY	HIGHWAY 17 & COUNTY 1558	ALBA	TX
7	ROCKER B TAXIDERMRY	401 S MAIN ST	ALBANY	TX
8	STACY HARGROVE	N US HIGHWAY 283	ALBANY	TX
9	L ADAMS WOODWORK PLUS	1198 N JOHNSON ST	ALICE	TX
10	S G BRISENO TAXIDERMIST	3717 W HIGHWAY 44	ALICE	TX
11	HIP-O TAXIDERMRY	2801 E HIGHWAY 90	ALPINE	TX
12	C D TAXIDERMRY	103 WOFFORD LN	ALVIN	TX

Image source: spatial.scholarslab.org

EXAMPLE HIGH LEVEL PILOT ADDRESS PLAN



Create your addressing plan on nibble boundaries:

- Split up your address allocation by Place In Network (e.g. 2001:db8:babe:**X000**::/52)
 - » 2001:db8:babe:0000::/52 – Management
 - 2001:db8:babe:0000::/64 – Loopbacks
 - » 2001:db8:babe:1000::/52 – Labs
 - » 2001:db8:babe:2000::/52 – DMZs
 - » 2001:db8:babe:3000::/52 – Servers
 - » 2001:db8:babe:4000::/52 – User/Desktop
 - » (...)
 - » 2001:db8:babe:F000::/52 – Special Purpose
 - 2001:db8:babe:FF00::/56 – Reserved for translation services

PILOT ADDRESS PLAN THOUGHTS



Prefixes

- Basic subnet plan - spreadsheet
- 65k prefixes per /48 - not scalable!

Nodes

- > 18 quintillion possible per subnet
- Sizeable deployments - IPAM desirable

Reference:

[IPv6 Subnetting Best Current Operational Practices](#)

THOUGHTS ON INITIAL TOPOLOGY



- Network Types
 - » Dual Stack
 - » IPv4 Only
 - » IPv6 Only
- Areas to Look at:
 - » Static/Dynamic Routing
 - » Load Balancing
 - » Proxying
 - » Tunneling
 - » NAT
 - » Dual data/control/management planes

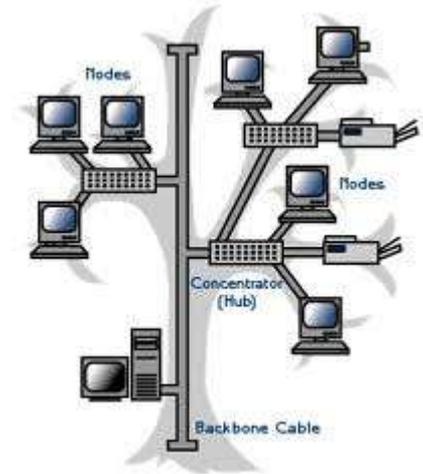


Image source: fcit.usf.edu



A WORD OF CAUTION ON NAT



- NAT was invented for address conservation
- Address conservation not needed for IPv6
- Think carefully before using NAT
 - » What applications will this degrade or break?
 - » How much is operational complexity increasing?
 - » How difficult does support become?
- More thoughts in Appendix

BUILD OUT INITIAL PILOT



- Infrastructure setup
- Hypervisor setup
- Physical and Virtual Nodes with representative Operating Systems
- Key Applications

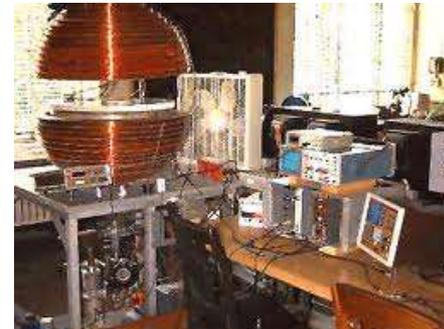


Image source: dspace.mit.edu

IPV6 SUPPORT INFRASTRUCTURE



- DNS
 - » Transport
 - » Accessibility
 - » Dynamic DNS
- DHCPv6
 - » Stateless
 - » Stateful
- WINS/NetBIOS
 - » Viability
 - » Recommendations



Image source: jranderson.photoshelter.com

IPV6 ADDRESS PROVISIONING OPTIONS



- Static
 - » Gotchas
- SLAAC
 - » Options
 - » RDNSS
 - » Stateless DHCPv6
- DHCPv6
 - » Stateful DHCPv6
 - » SLAAC

IPV6 ADDRESS PROVISIONING THOUGHTS



Address Options and Applicable Systems:

- Pure Static
- Static with Options
- SLAAC, no DHCPv6
 - » Basic
 - » RDNSS
 - » Dynamic VLAN Assignment
- SLAAC with (Stateless) DHCPv6
- DHCPv6 (Stateful DHCPv6)

BUILD YOUR IPV6 DMZ



In order of preference:

- Option 1 – Dual Stack
- Option 2 – Load balanced (SLB64)
- Option 3 – Dual Stack Reverse Proxy
- Option 4 (Discouraged) – Use NAT64



Image source: flickr.com

BUILD YOUR IPV6 INTERNAL NETWORK



- Connect Internal IPv6 Network to IPv6 Internet
 - » Option 1 (Preferred) – Dual Stack
 - » Option 2 – Forward Proxy
 - » Option 3 – (Legacy) Tunneling
 - » Option 4 – Stateful NAT64 (IPv6 Only)



Image source: wikipedia.org

ROADMAP



- Creating Your IPv6 Pilot Plan
- Initial Pilot Roadmap
- ***IPv6 Changes***
- IPv6 Security
- Pilot Phase 2
- Parting Thoughts

CHANGES WITH IPV6



- QoS Syntax

IPv4-Only	Dual Stack
match ip dscp	match dscp
match ip precedence	match precedence
set ip dscp	set dscp
set ip precedence	set precedence

Protocol Updates:

- From HSRPv1 to HSRPv2
- From NTPv[1-3] to NTPv4
- Anything with "IP" in the command suspect

- VRF Syntax

IPv4-Only	Dual Stack
<pre>ip vrf Red rd 65001:1 ! interface G0/0 ip vrf forwarding Red ip address 192.168.1.1 255.255.255.0</pre>	<pre>vrf definition Red rd 65001:1 ! ! Must explicitly declare each ! address family to use address-family ipv4 exit-address-family ! address-family ipv6 exit-address-family ! interface G0/0 vrf forwarding Red ip address 192.168.1.1 255.255.255.0 ! ipv6 enable ipv6 address 2001:db8:babe::1/64</pre>

MULTI-PROTOCOL REALITIES



IPv4 and IPv6 are ships in the night!

- IPv4 L2 Cache

```
ip access-list ext example1
```

```
  permit ip 192.168.0.0  
  0.0.255.255 any
```

```
!
```

```
interface G0/0
```

```
  ip access-group example1 in
```

- IPv6 L2 Cache

```
ipv6 access-list example2
```

```
  permit ipv6  
  2001:db8:babe:1::/64 any
```

```
!
```

```
interface G0/0
```

```
  ipv6 traffic-filter example2 in
```

MULTI-PROTOCOL REALITIES



IPv4 L2 Cache:

```
show ip arp
```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	192.168.232.1	-	0000.0c9f.f05a	ARPA	Vlan90
Internet	192.168.232.3	54	0011.bba6.1e80	ARPA	Vlan90
Internet	192.168.232.12	0	0023.ebe1.5d16	ARPA	Vlan90
Internet	192.168.234.149	0	Incomplete	ARPA	

IPv6 L2 Cache:

```
show ipv6 neighbors
```

IPv6 Address	Age	Link-layer Addr	State	Interface
FE80::90:2	0	02d0.2bff.74db	REACH	Vl90
2001:470:C4E8:1:108E:7EC3:BCDA:AF5C	47	000c.29f9.ed0b	STALE	Vl101
2001:470:C4E8:2::2	0	02d0.2bff.74db	DELAY	Vl90
FE80::3974:DC3C:AF4D:7239	47	000c.29f9.ed0b	STALE	Vl101
2001:470:C4E8:2::3	0	-	INCMP	Vl90

EIGRP - BASICS



From IPv4 to IPv6

```
interface Loopback0
 ip address 172.31.255.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
!
router eigrp 1
 network 10.1.1.0 0.0.0.255
 network 172.31.255.1 0.0.0.0
 passive-interface Loopback0
```

```
ipv6 unicast-routing
!
interface Loopback0
 ipv6 enable
 ipv6 address 2001:DB8::1/128
 ipv6 eigrp 1
!
interface FastEthernet0/0
 ipv6 enable
 ipv6 address 2001:DB8:1001::1/64
 ipv6 eigrp 1
!
ipv6 router eigrp 1
 passive-interface Loopback0
```

EIGRP - ADVANCED



Integrated Multi-Address Family

```
router eigrp DualStack
!  
address-family ipv4 unicast autonomous-  
system 2  
!  
af-interface Loopback0  
  passive-interface  
exit-af-interface  
!  
network 10.1.1.0 0.0.0.255  
network 172.31.255.2 0.0.0.0  
exit-address-family
```

```
address-family ipv6 unicast autonomous-  
system 2  
!  
af-interface default  
  shutdown  
exit-af-interface  
!  
af-interface Loopback0  
  passive-interface  
exit-af-interface  
!  
af-interface FastEthernet1/0  
  no shutdown  
exit-af-interface  
!  
exit-address-family
```

OSPF - BASICS



From IPv4 (OSPFv2) to IPv6 (OSPFv3)

```
interface Loopback0
 ip address 172.31.255.1 255.255.255.255
!
interface FastEthernet0/0
 ip address 10.1.1.1 255.255.255.0
!
router ospf 1
 passive-interface Loopback0
 network 10.1.1.0 0.0.0.255 area 0
 network 172.31.255.1 0.0.0.0 area 0
```

```
ipv6 unicast-routing
!
interface Loopback0
 ipv6 enable
 ipv6 address 2001:DB8::1/128
 ipv6 ospf 1 area 0
!
interface FastEthernet0/0
 ipv6 enable
 ipv6 address 2001:DB8:1001::1/64
 ipv6 ospf 1 area 0
!
ipv6 router ospf 1
 passive-interface Loopback0
```

OSPF - ADVANCED



Integrated Multi-Address Family

```
interface Loopback0
ip address 172.31.255.1 255.255.255.255
ipv6 enable
ipv6 address 2001:DB8::1/128
ospfv3 2 ipv4 area 0
ospfv3 2 ipv6 area 0
!
interface FastEthernet1/0
! (...)
ospfv3 2 ipv6 area 0
ospfv3 2 ipv4 area 0
!
```

```
router ospfv3 2
!
address-family ipv4 unicast
passive-interface Loopback0
exit-address-family
!
address-family ipv6 unicast
passive-interface Loopback0
exit-address-family
!
```

BGP - BASICS



From IPv4 to IPv6

```
router bgp 65203
network 203.0.113.0 mask 255.255.255.0
neighbor 198.51.100.1 remote-as 65301
neighbor 198.51.100.1 description IPv4_ISP
```

```
ipv6 unicast-routing
!
router bgp 65001
  bgp log-neighbor-changes
  neighbor 2001:DB8:1001::2 remote-as
  65002
!
address-family ipv6
  network 2001:DB8:1001::/64
  neighbor 2001:DB8:1001::2 activate
exit-address-family
```

BGP - ADVANCED



Integrated Multi-Address Family

```
ipv6 unicast-routing
!
router bgp 65203
no bgp default ipv4-unicast
!
neighbor 198.51.100.1 remote-as 65301
neighbor 198.51.100.1 description IPv4_ISP
!
neighbor 2001:db8:0:1::1 remote-as 65301
neighbor 2001:db8:0:1::1 description
IPv6_ISP
```

```
address-family ipv4
neighbor 198.51.100.1 activate
network 203.0.113.0 mask 255.255.255.0
exit-address-family
!
address-family ipv6
neighbor 2001:db8:0:1::1 activate
network 2001:db8:ace::/48
exit-address-family
```

[IPv6 Peering Best Current Operational Practices Draft](#)

ROADMAP



- Creating Your IPv6 Pilot Plan
- Initial Pilot Roadmap
- IPv6 Changes
- ***IPv6 Security***
- Pilot Phase 2
- Parting Thoughts

MONITORING AND CONTROLLING IPV6



Service	Number	Description
IPv6 Encapsulation Teredo/Miredo	IPv4/41 UDP/3544	Tunnel IPv6 over IPv4 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 Destined to 192.88.99.0/24 for IPv4
IPv6 Encapsulation IPv6 Ethertype	TCP/443 0x86DD	IPv6 over IPv4 SSL Tunnel, many variants Distinct from IPv4 Ethertype (0x0800)
DNS IPv6 Records	Several	AAAA, updated PTR records - can be transported over IPv4 or IPv6



IPV6 SECURITY



Common IPv6 Security Issues and Options:

Issue	Solution
Spoofed/Illegitimate RAs	RA Guard (or PACL)
Spoofed NDP NA	MLD Snooping, DHCPv6 Snooping, NDP Inspection, SeND
(Spoofed) Local NDP NS Flood	NDP Inspection, NDP Cache Limits, CoPP
(Spoofed) Remote NDP NS Flood	Ingress ACL, CoPP, NDP Cache Limits
(Spoofed) DAD Attack	MLD Snooping, NDP Inspection
(Spoofed) DHCPv6 Attack	DHCPv6 Guard
Spoofed/Illegitimate DHCPv6 Replies	DHCPv6 Guard

SWITCH IPV6 SECURITY OPTIONS



3560/3750 E+X, 2960/3560 C, 2960S - 15.0(2)SE:

- IPv6 First Hop Security Features Include:
 - » IPv6 Snooping
 - » IPv6 FHS Binding
 - » NDP Address Gleaning
 - » IPv6 Data Address Gleaning
 - » IPv6 DHCPv6 Address Gleaning
 - » IPv6 Device Tracking
 - » NDP Inspection
 - » IPv6 PACL
 - » IPv6 DHCPv6 Guard
 - » IPv6 RA Guard
 - » IPv6 Source Guard

IPV6 ACCESS CONTROL



- Firewall Policy
 - » Don't block all ICMPv6!!!
 - » Simple Examples for transit traffic, can get more granular:

Source Criteria:		Destination Criteria:		Service	Action
Source	Destination		
... (naming rules)					
any6		any6		<input type="checkbox"/> IPv6-Ops <ul style="list-style-type: none"> packet-too-big parameter-problem time-exceeded unreachable	Permit

Source Criteria:		Destination Criteria:		Service	Action
Source	Destination		
... (naming rules)					
any4		any4		<input type="checkbox"/> IPv4-Ops <ul style="list-style-type: none"> parameter-problem time-exceeded unreachable	Permit

- » Reference [NIST SP 800-119](#) (Section 3.5, Table 3-7)
- » Reference [RFC 4890](#) (Recommendations for Filtering ICMPv6 Messages in Firewalls)

IPV6 ACCESS CONTROL



- Router/Switch Policy
 - » Don't block the NDP's NS/NA functionality or you will break IPv6!

ipv6 access-list Example1

```
permit any host 2001:db8::1
```

```
permit icmp any any nd-ns
```

```
permit icmp any any nd-na
```

```
deny ipv6 any any
```

THINGS TO REVISIT WITH IPV6



- IPsec
 - » Consider migrating to IKEv2/IPsecv3
- Secure Hashes:
 - » Migrate from MD5 (broken) to SHA2
- Diffie Hellman Groups:
 - » Migrate from 1/2/5 to 14+ (14 is only 2048 bits!)
- Implement Anti-Spoofing functionality (RPF)
- Look at implementing IPv6 Bogon filtering from Team Cymru
- Build it right from the start!

ROADMAP

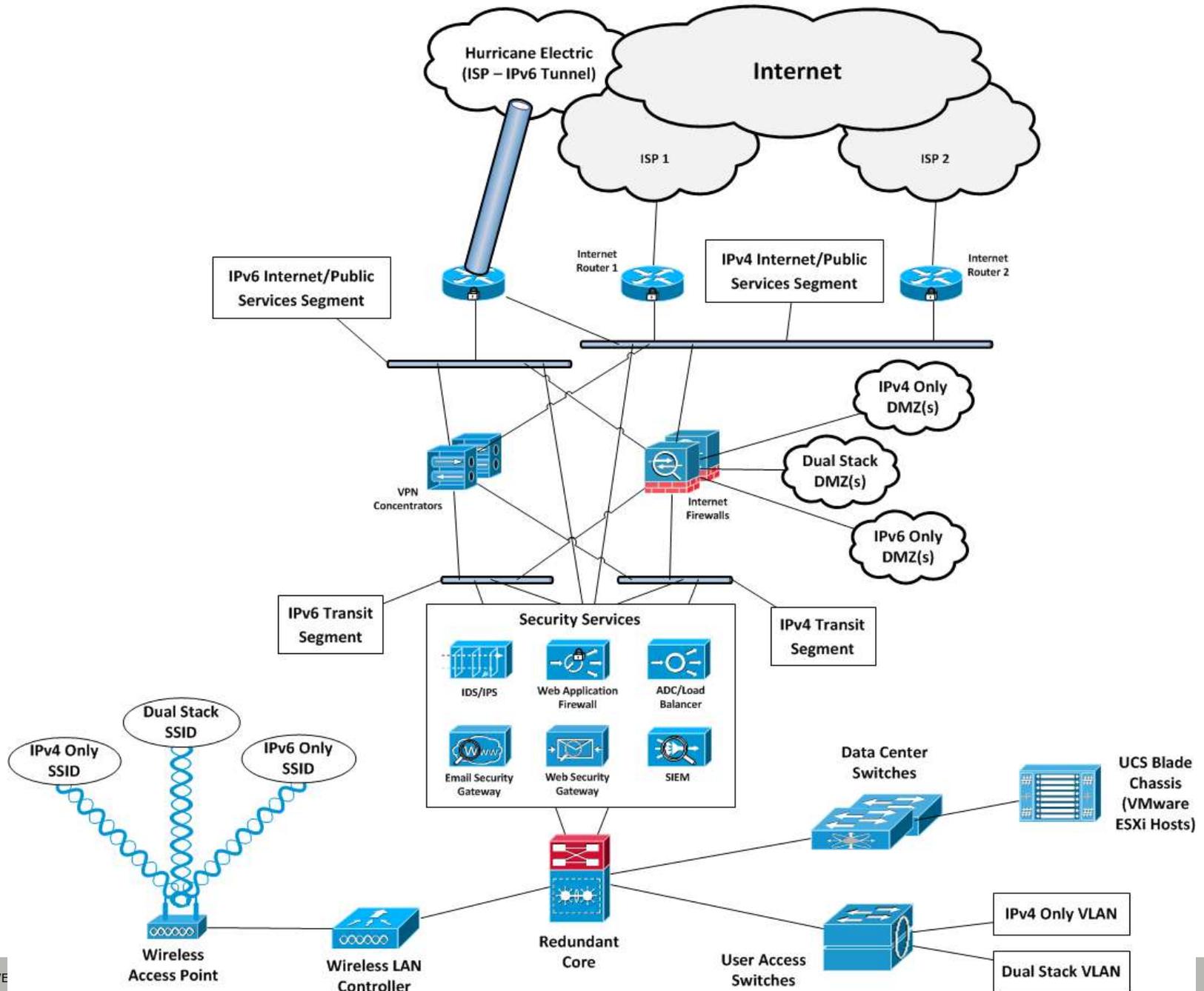


- Creating Your IPv6 Pilot Plan
- Initial Pilot Roadmap
- IPv6 Changes
- IPv6 Security
- ***Pilot Phase 2***
- Parting Thoughts

IPv6 Pilot Network – Phase 2 (Production Overlay)



DESIGN YOUR OVERLAY PILOT TOPOLOGY



ENTERPRISE PILOT – PHASE 2



- Move from Out-Of-Band to an Overlay
 - Request and setup full IPv6 BGP Peering
 - Expanding your pilot coverage
 - Begin leveraging your standard security solutions
 - » IDS/IPS
 - » Load Balancer
 - » Web Security Gateway
 - Build up your operational and planning abilities for IPv6 deployment
- Web Application Firewall
 - Production SIEM
 - E-mail Security Gateway

ROADMAP



- Creating Your IPv6 Pilot Plan
- Initial Pilot Roadmap
- IPv6 Changes
- IPv6 Security
- Pilot Phase 2
- ***Parting Thoughts***

SOME THOUGHTS ON IPV6 PROJECTS



- IPv6 is a large topic
- Don't try to do everything at once – break deployment into manageable pieces
- Start simple – phase in more advanced features, don't try to enable all options from day 1
- IPv6 touches everything – as you get closer to production make sure you involve personnel from all impacted areas



Image source: blog.lib.umn.edu

COSTS



- All applications, systems, network/infrastructure need to be inventoried for IPv6
 - » Some may have no support
 - » Some may have limited/software only (slow) support
 - » Some will have full support or full support with upgrades
- No hard deadline, but judicious planning will minimize expenditures



Image source: fisherpreciousmetals.com

MORE DETAILS ON GETTING STARTED



Additional Appendix Topics:

- Building Business Support (More Ideas)
- Building Your Project Plan (More Ideas)
- Build Your Team
- Develop Your Architecture
- Assess Your Infrastructure
- Training
- Deployment Approaches
- IPv6 Address Planning



Image source: drawingdownthevision.com

MORE THOUGHTS ON IPV6



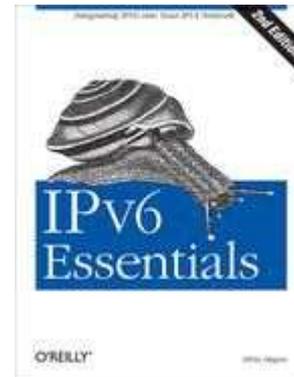
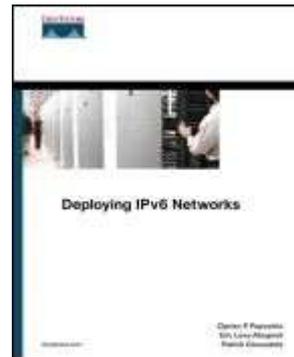
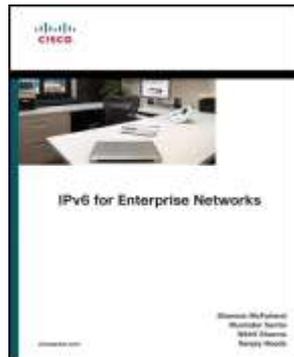
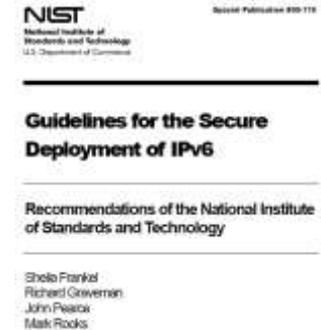
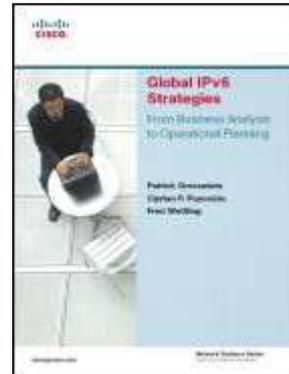
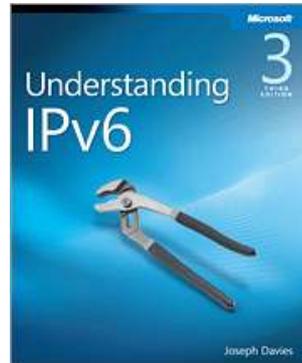
Additional Appendix Topics:

- IPv6 Mindset Changes
- Operational Issues/Risks
- Thoughts on NAT
- Issues with Disabling IPv6
- Application Compatibility
- Windows IPv6 CLI Basics
- IPv6 Solutions MIA



Image source: brides.com

RECOMMENDED READING





QUESTIONS



[@netsec14](#)



My IPv6 Blogs:
[Packet Pushers](#)

APPENDIX



- Building Business Support
- Building Your Project Plan
- Build Your Team
- Develop Your Architecture
- Assess Your Infrastructure
- Training
- Deployment Approaches
- IPv6 Address Planning
- IPv6 Mindset Changes
- Operational Issues/Risks
- Thoughts on NAT
- Issues with Disabling IPv6
- Application Compatibility
- Windows IPv6 CLI Basics
- IPv6 Solutions MIA



Additional IPv6 Business Case

- Specific Use Cases
 - » Internet of Things (Gartner – A top 10 strategic technology in 2012)
 - » Industry specific (SmartGrid, Embedded Networks, Building controls/sensors, etc.)
- Proxy Mobile IPv6 (PMIPv6) allows seamless roaming from 4G connections to Wireless connections and is getting rolled out soon

BUSINESS VALUE PROPOSITION



- Universal access (no NAT!)
 - » Eliminating NAT dramatically simplifies connectivity while only marginally complicating security
- Low power wireless sensors and embedded networking open a new realm of possibilities
 - » Smart Grid, Smart Home, Intelligent Sensors
- Peer to Peer Communication and Innovation Flourish
 - » Voice Calls/Conferencing, Collaboration

NEW MARKET OPPORTUNITIES



- SOHO/Consumer Space (now possible without NAT complexity)
 - » Managed services (Health and Security Monitoring, Appliance maintenance, Telemedicine)
- New Network Realms
 - » Personal Sports & Entertainment (Networked Treadmills)
 - » Asset Management, Environmental Monitoring
 - » Advanced Metering Infrastructures, Industrial Automation
- Easy Peer to Peer Communication Opens Markets
 - » More Efficient Video Consultation for Professionals
 - » Widespread Telepresence and Video Conferencing

INNOVATION AND EFFICIENCY



- Embedded networking allows facility automation
 - » Possible savings of 30% or more on energy costs (apricot.net)
- Easy market entry with anything to anything connectivity available to all
 - » Easy communication from anywhere to anything
 - » People to people
 - » Device to device

BUILDING YOUR PROJECT PLAN



- Secure management commitment
- Incremental, measurable, and achievable steps
- Be realistic, start simple – IPv6 Multicast Routing may not be required on day 1
- Effective risk analysis and containment
- Managing/motivating non-compliant vendors and teams

BUILD YOUR TEAM



IPv6 is a systemic change, in addition to the network team you'll need:

- Systems/System Administration
- Development/Applications/DBAs
- Security
- Desktop
- Operations – Monitoring/Tools, Help Desk

DEVELOP YOUR PERIMETER ARCHITECTURE



- Accessible Web Servers
- Accessible VPN Concentrators
- Accessible E-mail Servers/Gateways
- Accessible Portals/Applications
- Supporting Back Ends/Tiers

ASSESS YOUR INFRASTRUCTURE



- Network/Security Equipment
 - » IPv6 done in hardware/line rate?
 - » IPv6 done in software (degraded performance)?
 - » Upgrade(s) required?
 - » Roadmapped support but not current?
 - » Incompatible?

ASSESS YOUR INFRASTRUCTURE



- Operating Systems
 - » Which versions fully support IPv6?
 - Windows Vista, 7, 8, Server 2008, Server 2012
 - OS X 10.7+
 - Fedora 17, Ubuntu 12.04+
 - UNIX, FreeBSD 9.0
 - » Which versions have issues/limitations?
 - Windows XP, Server 2000, Server 2003
 - OS X before 10.7
 - Some quirks with older versions of Linux/BSD

ASSESS YOUR APPLICATIONS



- Web Servers and supporting software
- E-mail
- Databases
- Network Management Systems
- COTS and custom applications

TRAINING



What is your development plan for:

- Network staff
- Systems staff
- Developers
- DBAs
- Security staff
- Desktop staff
- Operations – Monitoring/Tools, Help Desk

IPV6 ADDRESS PLANNING



- Probably the most important part of your deployment!
- PI or PA?
- Smallest advertised prefixes which won't be filtered (BGP, PI, PA)
- ULAs?
- IPAM?

IPV6 MINDSET CHANGES



- Learning to think in networks instead of hosts
- Letting go of the address scarcity mentality
- Effective use of IPAM tools become crucial
- Running a multiprotocol network – back to the IPX/AppleTalk/DECNet days

OPERATIONAL ISSUES/RISKS



- Rogue RAs (Windows Internet Connection Sharing)
- Rogue Tunnels
- Overlay containment when tunneling (ISATAP reach/control)
- DNS Issues
- Broken IPv6 and Happy Eyeballs

PROBLEMS WITH NAT



- Some protocols do not work correctly through NAT and require “fix-ups” (ALG’s) or extra configuration
 - » E.g. ICMP, FTP, SIP, H.323, RTSP, some VPNs
- NAT breaks end-to-end connectivity
 - » Connection establishment and/or packet data requires a 3rd party
 - » Affects Voice Calls, Video Conferencing, file sharing, Collaboration, etc. For example, Skype, Facetime, Webex, and Microsoft Sharepoint Workspace work better without NAT.
 - » Note: Multiple NAT tiers can totally break these applications
- NAT for address overlap is technically challenging
- Limits innovation, increases costs/barriers for new ideas/solutions

BENEFITS OF NAT



- NAT simplifies changing ISPs (If PI Addresses not used)
- NAT hides the network topology and foils many simple network scans
 - » NAT alone is **not** secure, but it has been a helpful safety net against sloppy firewall policies
 - » Without NAT, firewall policies must be more robust and actively managed
- NAT can easily solve some complex network issues
 - » Multi-homing ISP's, return path selection, asymmetric routing
- NAT is ubiquitous
 - » Today, software is developed with an expectation of NAT
 - » Tomorrow...?

NAT – PROS/CONS



Pros

- Easier ISP Mobility
- Avoid Renumbering
- Small Site Multihoming
- Identical Small Sites
- Topology Hiding
- Some Added Security
- Path Selection/Hiding

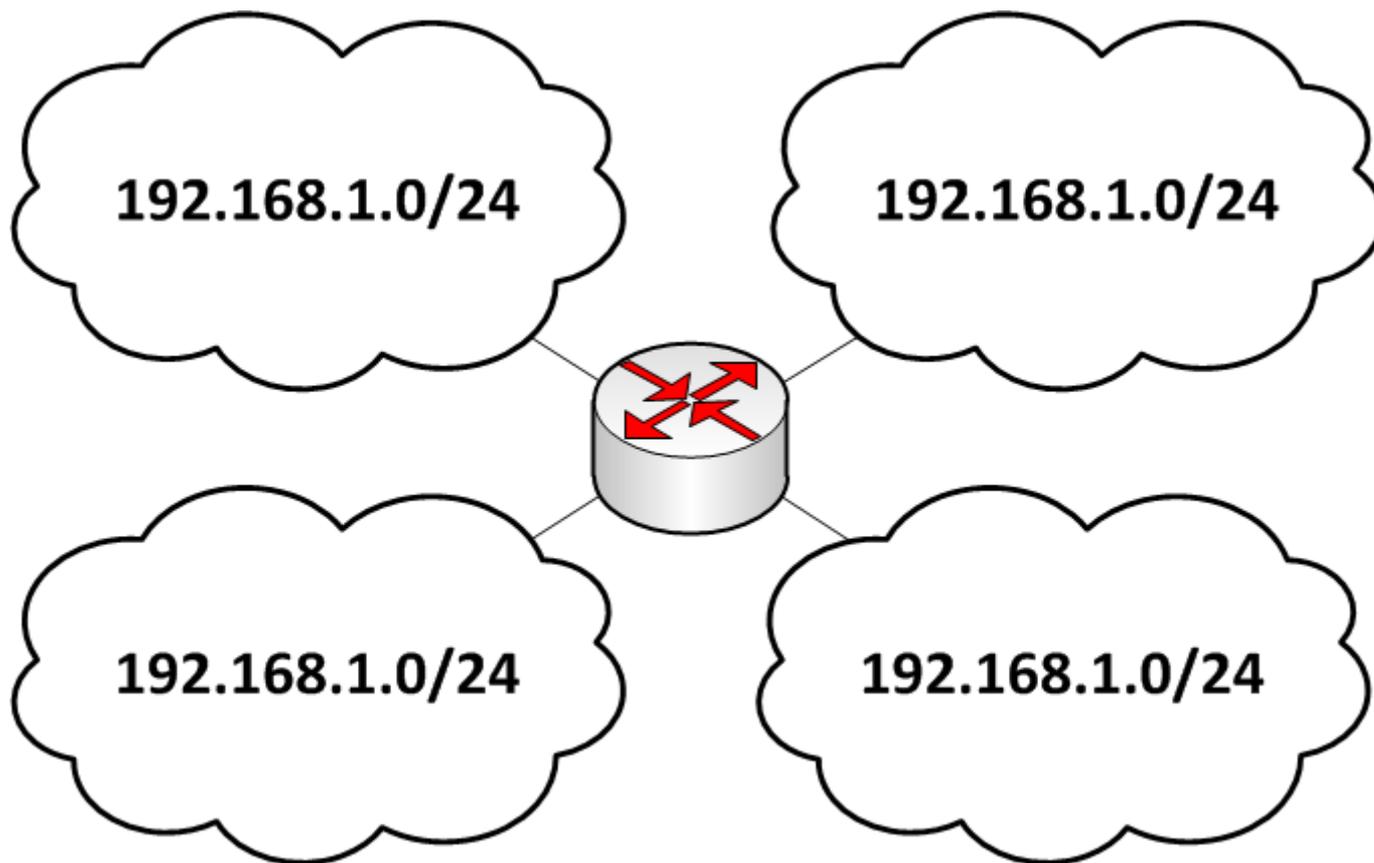
Cons

- Hidden Costs
- Breaks End to End
- Many Apps Need ALGs
- Overlapping Networks
- Increased Complexity
- False Sense of Security
- Inhibits Innovation

THE HIDDEN COSTS OF NAT



Something to consider when evaluating NAT:



NAT – ALTERNATE SOLUTIONS



Problem

- Avoid Renumbering
- Small Site Multihoming
- Identical Small Sites
- Topology Hiding
- Perceived Security

IPv6 Solution

- PI or ULA + GUA
- LISP or ULA + TTLd GUA
- Standardized Link-Locals
- Proxies/MIPv6
- Stateful Firewall

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

APPLICATION COMPATIBILITY



- Things to look for:
 - » Embedded IPv4 addresses/literals (e.g. "198.43.84.7")
 - » Fields allow IPv6 addresses to be entered
 - » Can it handle both DNS A and AAAA (IPv6) records?
 - » Does it use the socket API or anything else that is IPv4 specific?
 - » Where IP addresses are stored, can the database/storage mechanism deal with IPv6?

EDUCATION - IPV6 BASICS



New Windows Commands - netsh interface ipv6:

show addresses	Detailed information on IPv6 interface addresses
show destinationcache	Displays the contents of the destination cache, sorted by interface; the destination cache stores the next-hop addresses for destination addresses
show global	Shows global configuration parameters such as interface address randomization
show interfaces	Detailed interface list including index numbers/zone identifiers, also try level=verbose
show neighbors	Displays contents of the neighbor cache, sorted by interface; the neighbor cache stores the link-layer addresses of recently resolved next-hop addresses
show prefixpolicies	Shows prefix policy table (IPv6 versus IPv4 preference order)
show privacy	Shows interface address privacy configuration parameters

Note: netsh commands can be abbreviated:

- netsh interface ipv6 show interface

Abbreviate as:

- netsh int ipv6 sh int

CISCO SOLUTIONS MISSING IPV6



- WAAS
- Nexus 1000V
- VSG
- ASA 1000V