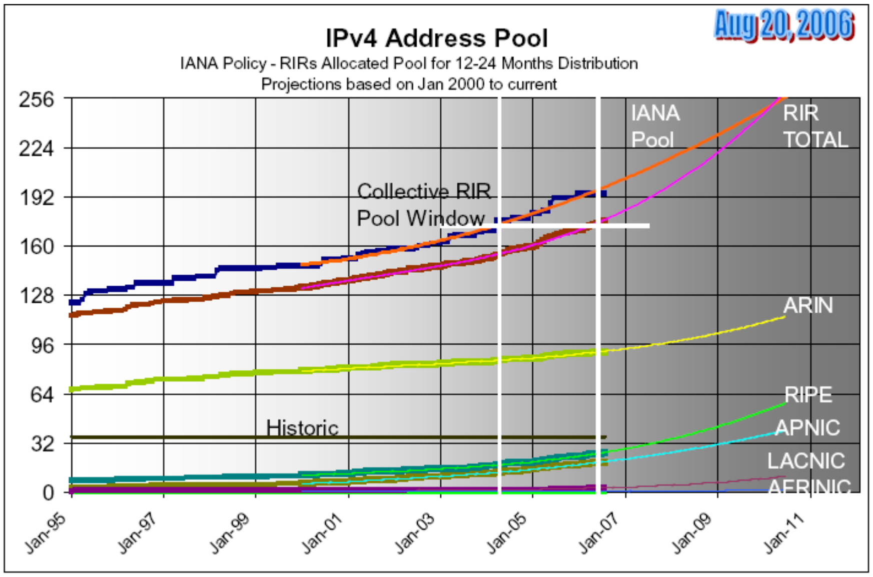
Moonv6 Network Project

July 2006 Technology Status, Test Observations and Results

The Moonv6 project brings together users and suppliers to answer the tough questions about what pieces of IPv6 are ready for prime time. The testing documented in this paper took place in July 2006 and included DNS, DHCP, Transition, Firewalls, IPSec and NTP.

New electronic equipment more often includes a network interface and IP address. A trend can be seen with everything from simple home appliances to cellular phones. As this continues, more IP addresses are being consumed. Currently IPv4 has a fixed number of addresses and the below figure would indicate that no extra addresses will be left in approximately four years.



Update to: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_8-3/ipj_8-3.pdf
Exhaustion of the central IANA pool - orange
Exhaustion of the collective RIR pools - magenta
Relative distribution rates between the RIRs
Time depth of collective RIR pools on pub date - white
Time depth between exhaustion events - diff between orange & magenta

Tony Hain

Figure 1: IPv4 Address Usage

Many commercial enterprises see a two-year horizon for planning, so why take interest in this issue? IPv4 addresses have been distributed unevenly. In Asia and Europe, there is significantly more pressure to find alternatives to the current model due to a lack of addresses. That leaves North America with a technology leadership issue. Would North America be left behind if other regions innovate and gain valuable deployment experience? IPv6 has additional benefits, however number of addresses and technology leadership seem to be at the front.

Introduction

Moonv6 is a collaborative project led by the North American IPv6 Task Force (NAv6TF) and includes the University of New Hampshire InterOperability Laboratory (UNH-IOL), U.S. Government agencies and Internet2 (I2). The Moonv6 network, based at the UNH-IOL and the Joint Interoperability Test Command (JITC) Located at Ft. Huachuca, AZ, has rapidly deployed the most aggressive multi-vendor IPv6 network to date. Together with the "IPv6 Ready" logo program, administered by the IPv6 Forum, the Moonv6 project has taken a key role in the IPv6 technology adoption process. Below is a timeline of how different aspects of IPv6 are tested and verified.

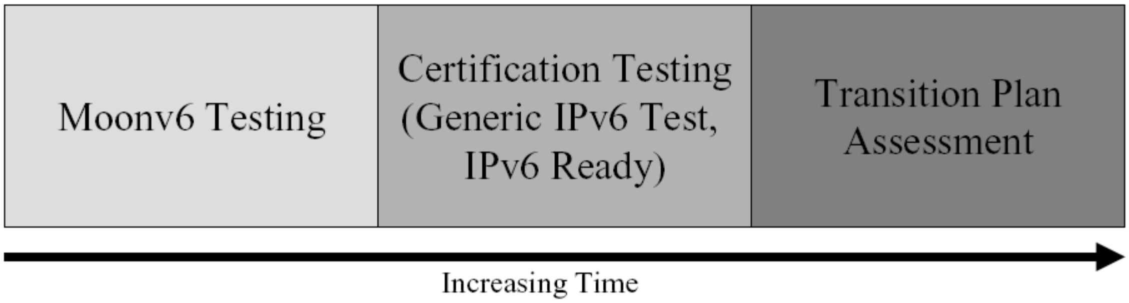

Moonv6 Testing
Certification Testing (Generic IPv6 Test, IPv6 Ready)
Transition Plan Assessment
Increasing Time

Figure 2: IPv6 Testing Progress

Moonv6 offloads the "bleeding edge" of new areas by providing the users and developers fast feedback in their new implementations. The test plans, results and technical expertise from Moonv6 are used to accelerate the development of new certification processes. Both Moonv6 and the certification processes can reduce the load on enterprises and government agencies when assessing transition plans and deployment strategies.

Phase I of the Moonv6 project established the largest next-generation Internet (native IPv6 network) in North America. Initialized in October 2003, Moonv6 has tested or demonstrated every aspect of IPv6. The first two phases focused on functional stability of routing infrastructure, host connectivity and basic applications.

Further testing in 2004 and 2005 moved IPv6 technology forward through a new round of advanced deployment and functionality scenarios. Test items included Mobile IPv6 (via IEEE 802.11 wireless LANs); Ethernet networks; Applications/Data traffic; Firewalls; Access Policy; Stateful Firewall Functionality; Network-level testing and deployment; IPSec and Applications between Firewalls; DHCP; DNS; VoIP; Transition Mechanisms; Dual Stack Routing; Static Tunnel and additional mechanisms (tunnel broker, DSTM); IPv4/IPv6 QoS network level testing and applications testing.

The NAv6TF's future vision for Moonv6 is to create a virtual Internet backbone with the ability to do pre-production testing for security, multimedia, roaming devices, and other services. Going forward, Moonv6 will serve as a deployment test bed and continue to empower service providers and suppliers from every sector, including industry, universities, research laboratories, Internet service providers and U.S. government agencies.

Participants

The latest round of testing involved service providers, networking companies and several government agencies, including:

INTERNET2	iol	SPAWAR	JOINT INTEROPERABILITY TEST COMMAND Increasing Combat Effectiveness Through Interoperability	AIR FORCE COMMUNICATIONS AGENCY
Panasonic	Nominum	QLOGIC		
SPECTRACOM	Agilent Technologies	FORTINET		
IBM	Check Point SOFTWARE TECHNOLOGIES LTD. We Secure the Internet.	extreme networks		
Lucent Technologies Bell Labs Innovations	Microsoft			

Test Scenarios and Results

The July 2006 testing of Moonv6 used similar concepts that were established in the earlier phases of testing. The core network connected all sites in a static manner. As the final network topology was being constructed, protocol-specific test plans were executed at both the UNH-IOL and the JITC Ft. Huachuca sites. Engineers at each of the other sites executed test activities for network applications and some also tested more advanced functionality.

Network Time Protocol Testing

NTP is used to synchronize clocks over a network using a set of distributed clients and servers. This was the first demonstration of NTP in an IPv6 wide area environment. It was found that NTP Server 1 was able to synchronize to GPS satellites or NIST-ACTS via dial-up (both serve as Stratum 0 references). NTP Server 1 (operating as a Stratum 1 reference) was then used to synchronize local and remote servers and clients, plus backup timeserver NTP Server 2 (all operating at Stratum 2), over IPv6. Advanced testing of NTP Server 1 revealed support of DHCPv6 and DNS operation over IPv6.

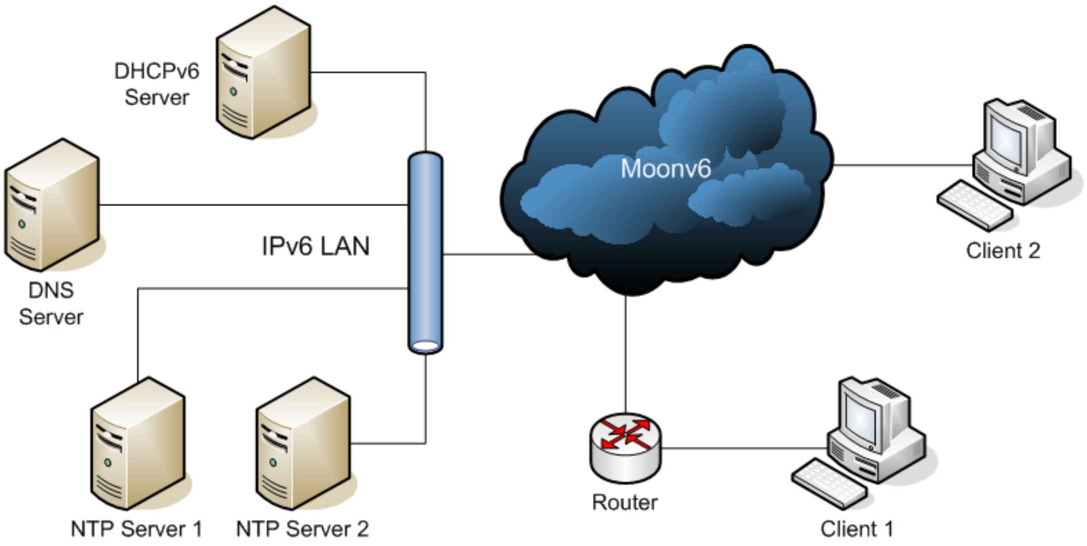


Figure 3: NTP Network Topology

DoD IPv6 Information Assurance Testing

The Joint Interoperability Test Command (JITC) performed an IPv6 Information Assurance (IA) vulnerabilities assessment during the DoD's Joint Users Interoperability Communications Exercise 2006 (JUICE 06). This assessment is critical to a successful transition to Internet Protocol (IP) Version 6 (IPv6), and crucial to continued support of the warfighter in FY 2008 and beyond.

The JUICE 06 IA Assessment identified IPv6 IA vulnerabilities in individual devices and within networks that are representative of operational DoD systems. The JUICE 06 network architecture consisted of equipment and networks that were assessed within a simulated Defense Information Systems Network Core. The assessment included Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) and Teleport environments with client and server resources provided by Microsoft Vista Beta Builds 5520 and 5472. The JITC provided a separate assessment for MO2 enclave. The JITC also hosted a Public Key Infrastructure (PKI) and Internet Protocol Security (IPSec) integration experiment using Microsoft Vista Client and Server Beta Builds 5520 and 5472. Providing automated key exchange in a ubiquitous IPv6 environment was the main objective to this experiment. The Blue Team assessed the simulated networks using the DoD IPv6 Generic Test Plan (GTP) Version 2 (Draft) and the Blue Team IA Annex to the IPv6 GTP, and the PKI and IPSec Integration experiment used the PKI, IPSec, and IPv6 Integration Experiment Test Plan Whitepaper.

The Blue Team provided data analysis of vulnerabilities discovered during the technical assessment. The vulnerabilities were recorded starting with the routers having the highest total average of vulnerabilities with switches and servers having a medium total average of vulnerabilities, and Microsoft XP workstations having the lowest total average of vulnerabilities. The Milestone Objective 2 (MO2) architecture contained the IPv6 packets to the IPv6 only enclave as anticipated. The PKI, IPSec and IPv6 Integration Experiment was able to establish IPSec over IPv6 tunneling and remain secure on one version of Beta software. The Microsoft Vista Beta software encountered issues typical of Beta software.

The conclusion for this assessment was that the IPv6 IA vulnerabilities are similar to known IPv4 vulnerabilities. This assessment only used the IPv6 vulnerabilities known at the time of this test.

IPSec Testing

With increasing amounts of data being stored on remote servers, and the widespread use of the Internet as a communication medium, securing Internet traffic at the IP level is becoming more and more of a necessity. This most recent Moonv6 event saw vendors with IPSec capabilities spanning the spectrum.

Both manual keyed implementations, and implementations using IKE with Pre-shared Keys, were shown to inter-operate correctly. Significantly more configuration errors were encountered with manual keys, offering more evidence to the need for reliable implementations supporting automatic-keying protocols.

From an applications perspective, a Panasonic Network IP Camera was connected to hosts with a tunnel mode IPSec/IKE connection. For hosts that did not support IPSec, the Network IP Camera connected to a Home Gateway with IPSec and the home gateway handled the security association. The performance of the Network IP Camera was not hindered by the IPSec overhead.

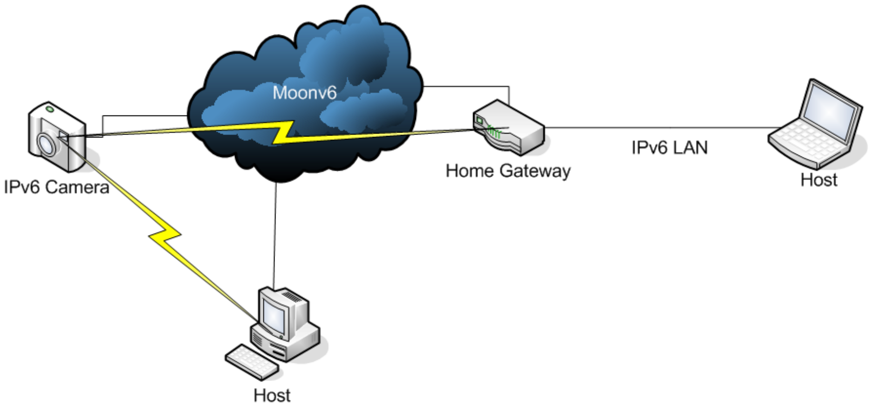


Figure 4: IPSec Network Topology

DNS Testing

To make IPv6 "user-friendly", stable DNS services are a requirement. Various aspects of DNS operation were tested. This included incremental and entire zone transfers, host queries and DNS operation with firewalls.

The primary issue with DNS and IPv6 is that older standards are being used by some modern implementations. Queries were observed for A6 records, the ip6.int domain, and bitstream labels, all of which have been removed from the standards track.

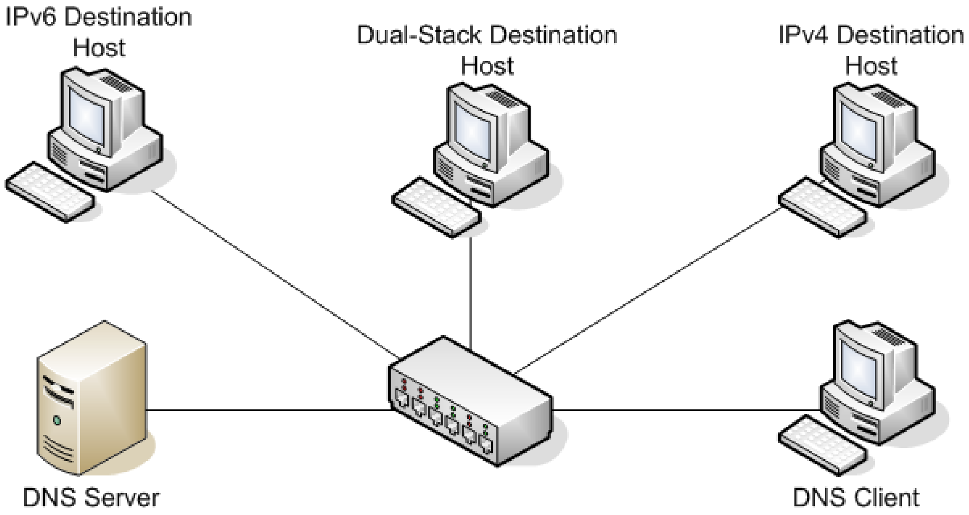


Figure 5: DNS Network Topology

DHCP Testing

For IPv6 to be successful in the enterprise and consumer market, IPv4 equivalency is a must. One key area is the automatic configuration of hosts, primarily through DHCP. This Moonv6 event saw the largest group yet of DHCPv6 capable devices in one location.

Host vendors were able to acquire both DNS information, as well as prefix information from DHCP Servers. In another first, a DHCP network utilizing prefix delegation was set up between 5 different vendor devices. The router in the network received a DHCP address prefix of 48 bits. The router then delegated 64 bit prefixes to the hosts on its network, namely Host2. Host1 was also able to configure a DHCP server, and receive configuration information from either server.

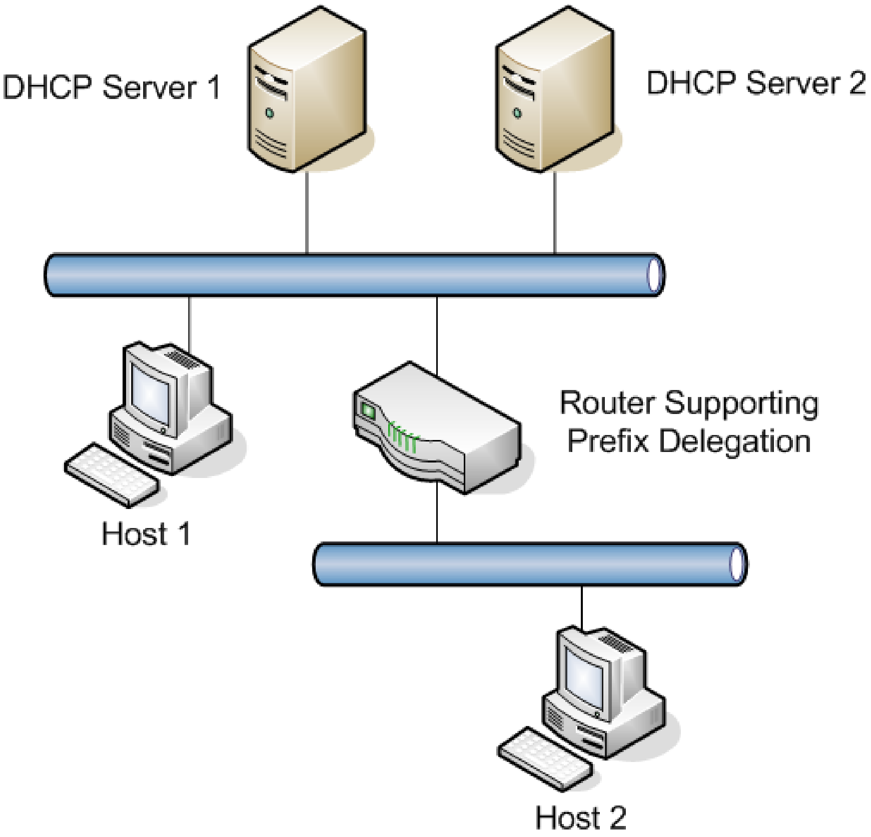


Figure 6: DHCP Network Topology

Firewall and Application Testing

In today’s Internet, not all packets can be trusted to have complete access to a network. Firewalls must be utilized to block potential attacks, and to restrict the type of traffic flowing in and out of a network. One challenge in this space is to test in a realistic environment. How do you send a mix of applications across a device and see if it functions properly? Application-aware firewalls were tested with a variety of application layer data such as, HTTP, FTP, POP3, SMTP, TELNET and VOIP in an emulated network environment.

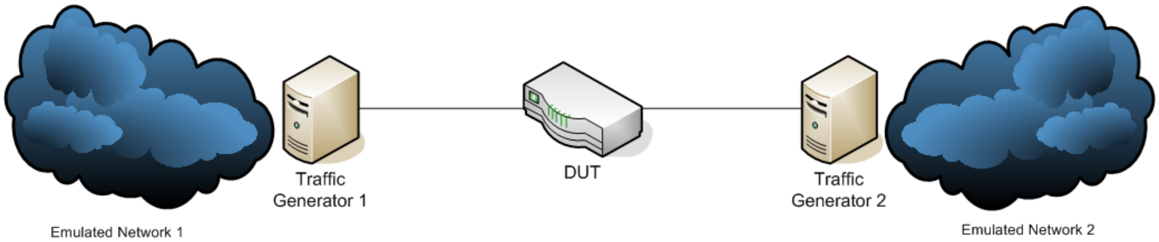


Figure 7: Security Testing Configuration

Firewall deep-inspection functionality of application traffic in a mixed IPv4/IPv6 environment was validated and compared with the same test scenarios in an IPv4 only environment. A realistic protocol mix was configured to simulate the forwarding and blocking capabilities in an actual network.

A critical concern that must be addressed in an IPv4/IPv6 transition environment is equivalent quality of the user experience. If a security device performs adequately with IPv4, it should also sustain comparable performance levels when processing mixed IPv4/IPv6 and pure IPv6 traffic. Responding to that concern, the 2006 Moonv6 Transition Test Suite included performance tests that compared security devices for IPv4, IPv6 and mixed IPv4/IPv6 performance. These tests used real-world application mix traffic to measure the metrics. The tests successfully validated that security devices can sustain adequate performance and QoE levels in transition IPv4/IPv6 environments.

Transition Testing

To demonstrate that transition mechanisms are working, three scenarios were tested. The testing started with dual stacked routing on a single interface. This approach seems to be the most popular among network operators because it does not rely on any kind of tunneling or encapsulation schemes; each frame is routed as-is and all routers in the network can route both IPv4 and IPv6 frames natively.

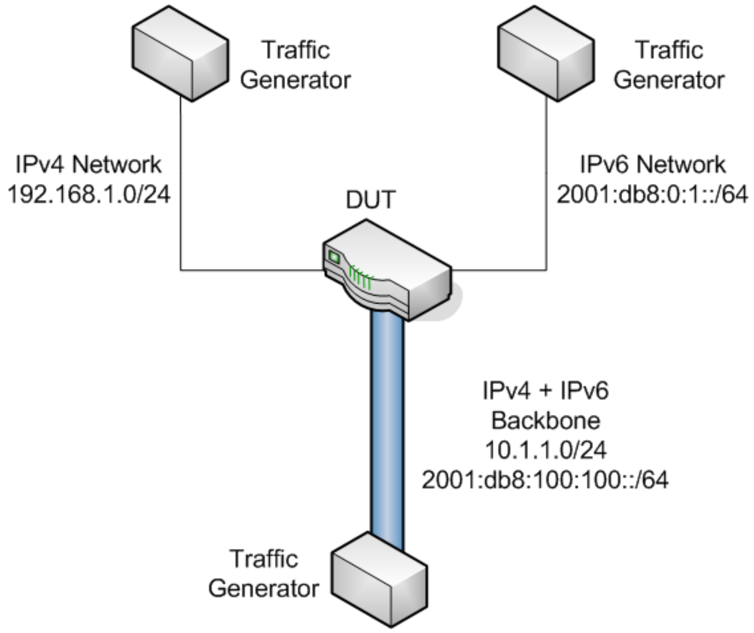


Figure 8: Dual-stack Routing

6in4 is a transition mechanism that statically connects IPv6 edge domains over an IPv4 core network. In the 6in4 model, the IPv4 backbone network acts as a point-to-point link layer for disperse IPv6 domains. In this scheme, IPv6 packets are encapsulated in IPv4 packets based on a pre-configured set of point-to-point tunnels. Tunnel endpoints are IPv4 addresses known to the 6in4 gateway. The Traffic Generator connected to the IPv6 Tunnel sends both encapsulated and unencapsulated traffic.

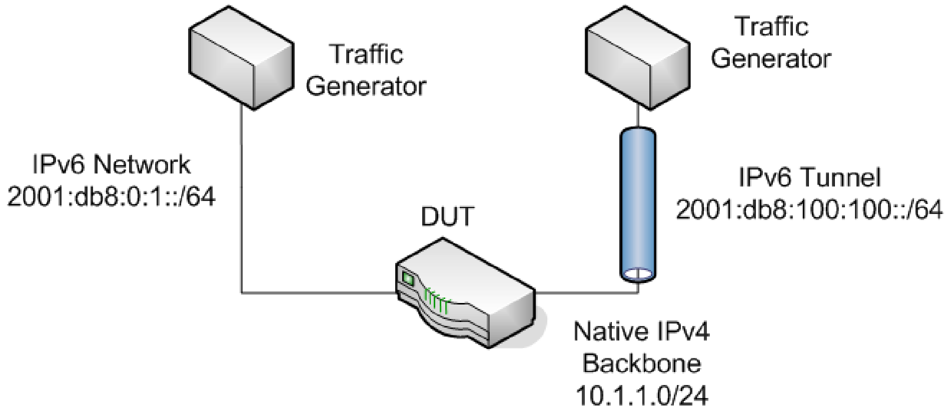


Figure 9: 6in4 Tunneling: Configured Transition Mechanism

6to4 is a transition mechanism that automatically connects IPv6 edge domains over an IPv4 core network. The IPv4 backbone in a 6to4 transition scheme acts as a dynamic, multipoint link-layer bridging the disperse IPv6 domains on top of the IPv4 routing topology. Rather than configuring static tunnels, IPv6 network prefixes are assigned to IPv6 routing domains such that the IPv4 address of the destination 6to4 gateway can be derived from the IPv6 address.

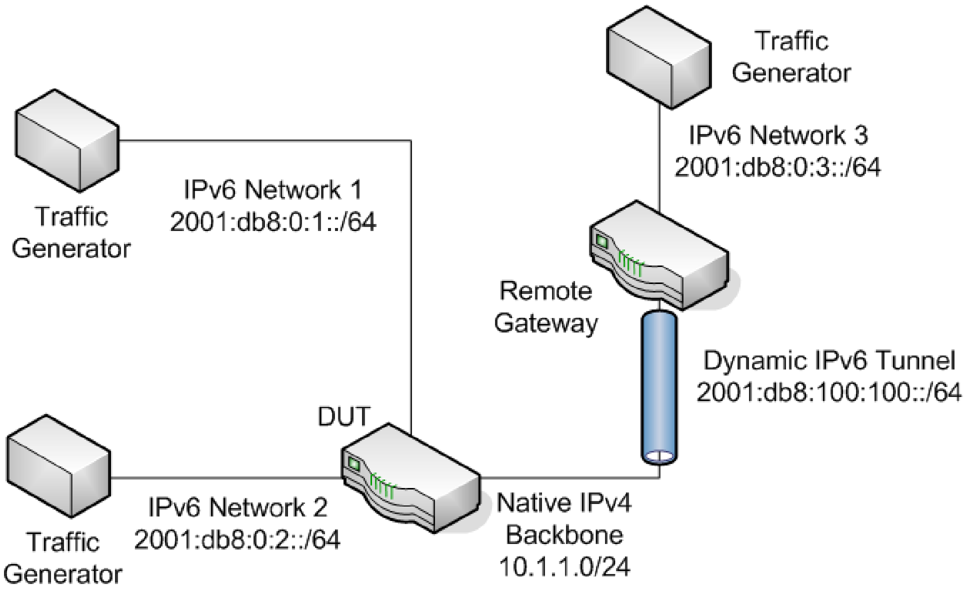


Figure 10: 6to4 Tunneling: Dynamic Transition Mechanism

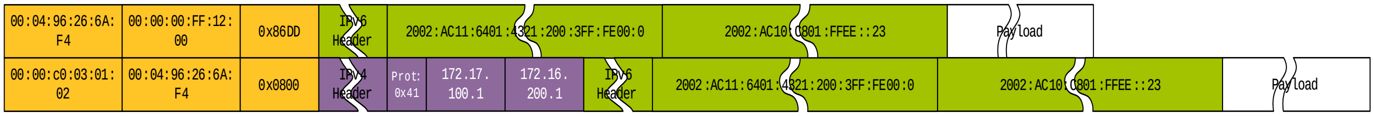


Figure 11: IPv6 and 6to4 Encapsulated Frames

All three of these transition mechanisms were successfully proven in the Moonv6 network.

Conclusion

As IPv6 is tested, certified and deployed, a key determinant of emerging protocol standardization and commercial adoption is pushing testing and validation to new levels. To further these efforts, the Moonv6 test events at the UNH-IOL have provided and will continue to provide an aggressive test scenario built around service providers' requirements and real-world deployment characteristics.

The largest hurdles to IPv6 deployment and adoption that Moonv6 has identified have been either specific device implementation or user configuration issues. Naturally, the transition to IPv6 will involve a learning curve for system and network administrators. That said, there is still a great need for future testing in firewalls, security, PKI, IKE, IPsec, SIP, multicast, streaming video, mobility and other applications and routing protocols.

Distinct advantages to service providers regarding IPv6 include the enhanced addressing space that will be needed for new applications and overseas customers. IPv6 also plays a key role in restoring the Internet's network address organization and enabling secure reachability across disparate networks. Service providers will continue to require accepted metrics of interoperability from their equipment vendors. The U.S. DoD, if it continues on its stated course of transitioning completely to IPv6 by 2008, will continue to drive interest in IPv6 in the North American market.

Terminology

AS Autonomous System. A set of routers under a single technical administration that has a coherent interior routing plan and presents a consistent picture of what destinations are reachable through it.

BGP Border Gateway Protocol. BGP version 4 is currently the most popular External Gateway Protocol (EGP) for IP Routing.

DoD United States Department of Defense.

DISR DoD Information Technology Standards Registry. Formerly the Joint Tactical Architecture. The list of standards that the U.S. DoD uses as requirements in its networks.

DNS Domain Name Server.

DSCP Diff-Serv Code Point. Used to differentiate different types of traffic. Uses the ToS bits in a packet header.

DHCP Dynamic Host Configuration Protocol

ICMP Internet Control Message Protocol. ICMP Echo Requests and Replies facilitate troubleshooting at Layer 3 for both IPv4 and IPv6. IPv6 has built extra features into ICMP.

IGP Interior Gateway Protocol.

IPSec Internet Protocol Security

IPv4 Internet Protocol Version 4. The first widely deployed Layer 3 data networking protocol. The 32 bit address is creating an address limitation on the growth and development of the modern internet and creating an interest in IPv6.

IPv6 Internet Protocol Version 6. A next generation Layer 3 data networking protocol. The 128 bit address space and additional features in the design creates a flexible alternative to IPv4.

JITC Joint Interoperability Test Command

JUICE	Joint Users Interoperability Communications Exercise
NAT	Network Address Translation. This concept is used to temporarily solve the problem of lack of IP addresses.
NAv6TF	North American IPv6 Task Force. The NAv6TF supports and drives the IPv6 US Summits in North America, promotes IPv6 with industry and government, provides a technical and business center of expertise for the deployment of IPv6, provides white papers, briefings, and presentations for public consumption, and works with the IT sector to understand the effects of IPv6 transition on the enterprise. The NAv6TF is implementing a plan of action for IPv6 deployment through Moonv6.
NTP	Network Time Protocol. Used to a protocol designed to synchronize the clocks of network nodes from a central server or set of servers.
OSPF	Open Shortest Path First. An Internal Gateway Protocol (IGP) for IP Routing primarily used in large enterprise and service provider networks.
PKI	Public Key Infrastructure
SIP	Session Initialization Protocol. Primarily used to setup and facilitate Voice over IP (VoIP).
SNTP	Simple Network Time Protocol. A lightweight version of NTP.
SMTP	Simple Mail Transfer Protocol. A protocol designed to transfer e-mail reliably and efficiently between servers.
SYN	Synchronize bit in a TCP handshake.
TCP	Transmission Control Protocol. A connection-oriented Layer 4 protocol.
TSP	Tunnel Server Protocol.
UDP	User Datagram Protocol. A connectionless Layer 4 protocol.
VLAN	Virtual Local Area Network.

References

RFC 854 J. Postel, J. Reynolds, TELNET Protocol Specification, May 1983.

RFC 959 J. Postel, J. Reynolds, File Transfer Protocol (FTP), October 1985.

RFC 1350 K. Sollins, The TFTP Protocol (Revision 2), July 1992.

RFC 1981 McCann, J., S. Deering, and J. Mogul, Path MTU Discovery for IPv6, August 1996.

RFC 2030 D. Mills. Simple Network Time Protocol Version 4 for IPv4, IPv6 and OSI, October 1996.

RFC 2328 J. Moy, OSPF, Version 2, April, 1998.

RFC 2401 S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, November 1998.

RFC 2406 S. Kent, R. Atkinson, IP Encapsulating Security Payload, November 1998.

RFC 2460 Hinden, R., S. Deering, Internet Protocol, Version 6 (IPv6) Specification, December 1998.

RFC 2461 Narten, T., Nordmark, E., and W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), December 1998.

RFC 2462 Thomson, S., T. Narten, IPv6 Stateless Address Autoconfiguration, December 1998.

RFC 2463 Conta, A., S. Deering, Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, December 1998.

RFC 2516 L. Mamakos, et. al, A Method for Transmitting PPP Over Ethernet (PPPoE), February 1999.

RFC 2616 R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee. Hypertext Transfer Protocol -- HTTP/1.1. June 1999.

RFC 2710 Deering, S., Fenner, W., Haberman, B., Multicast Listener Discovery (MLD) for IPv6, October 1999.

RFC 2821 J. Klensin. Simple Mail Transfer Protocol, April 2001.

RFC 2740 Coltun, R., Ferguson, D., Moy, J. OSPF for IPv6, December, 1999.

RFC 2858 T. Bates, Y. Rekhter, R. Chandra, D. Katz, Multiprotocol Extensions for BGP-4, June 2000.

RFC 2874 M. Crawford, C.Huitema. DNS Extensions to support IPv6 Address Aggregation and Renumbering, July 2000.

RFC 2893 R. Gilligan, E. Nordmark, Transition Mechanisms for IPv6 Hosts and Routers, August 2000.

RFC 3530 S. Shepler, B. Callaghan, D. Robinson, R. Thurlow, C. Beame, M. Eisler, D. Noveck. Network File System version 4 Protocol, April 2003.

RFC 1305 David L. Mills. Network Time Protocol (Version 3) Specification, Implementation and Analysis, March 2002.

RFC 2030 D. Mills. Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI, October, 1996.

DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 1, dated 1 June 2006.

Special Thanks To:

Jim Bound, Hewlett Packard and North American IPv6 Task Force Chair
Kamal Boiri, Panasonic Connectivity Verification Center of America (CVCA)
John Brzozowski, Comcast
Glenn Burdett, Spectracom
Ethan Burns, UNH-IOL
Capt Jeremy Duncan, JITC
Phillip Kazakov, Agilent
Matt Labbe, Extreme Networks
Tom Peterson, UNH-IOL
Ben Schultz, UNH-IOL
Greg Schwendimann, UNH-IOL
Erica Williamsen, UNH-IOL
Tim Winters, UNH-IOL

Picture in introduction provided by Tony Hain of Cisco Systems.