Moonv6 Network Project

Moonv6 2005 Test Set Observations and Results

Executive Summary

Moonv6 is a collaborative project led by the North American Internet Protocol version 6 (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, Arizona, has deployed the largest multi-vendor IPv6 backbone to date. Together with the “IPv6 Ready” logo program, administered by the IPv6 Forum, the Moonv6 Project tests and promotes IPv6’s most promising features, including improved multi-media streaming, Internet protocol mobility, and an alternative to less scalable and less secure network address translation (NAT) strategies.

In an effort to refine this next generation of the Internet protocol (IP), IP equipment, manufacturers and network operators continue to collaborate with government agencies and independent laboratories on Moonv6 testing. This testing aims to improve the conformance, scalability, and internetworking capability of multiple commercial implementations of IPv6. The latest round of Moonv6 interoperability tests began on November 28, 2005 at the UNH-IOL and ran through December 2, 2005. December test objectives addressed the sustained interest in testing IPv6 technology in legacy environments and began new protocol testing, which extended IPv4 equivalency further into the access layer.

Eleven vendors participated in this latest round of interoperability tests. While previous Moonv6 events focused predominately on testing core network areas such as routing protocols, the objective of the December test event was to demonstrate advances in IPv6 applications. It tested Dynamic Host Configuration Protocol (DHCP), security, and some voice services. The tests demonstrated that these functionalities are fundamentally stable for small deployments. IPv6 was also tested in the following areas:

- Mobility
- DHCP
- DNS/DHCP resolution
- Application Layer (VoIP)
- Security (IPsec)

By passing mixed Voice-over-IP (VoIP) and data traffic over IPv6, these tests employed more realistic traffic streams than had been used in previous tests and successfully exhibited basic application layer functionality for some, but not all, participants. Progress was also made in establishing IPv4 equivalency in areas such as addressing. UNH-IOL engineers successfully demonstrated international VoIP calling over IPv6. The success of this call, made from New Hampshire to South Korea using commercial software, suggests the tremendous progress IPv6 has made. In addition, the test event highlighted some areas of improvement necessary for IPv6 in the future, particularly in applications.

Introduction

The Moonv6 December 2005 test event marked a milestone in the testing of IPv6, the next generation Internet protocol. For the first time, Moonv6 focused primarily on the access layer and IPv4 equivalency. The December event gathered the largest ever number of DHCPv6 implementations at a single location. It also included the first international VoIP call made over commercially available software from North America through the use of a 6to4 tunnel. Other areas of testing successfully demonstrated DHCPv6, DHCPv6 prefix delegation, DNS resolution, Voice-over-IPv6 mixed with data traffic, IPv6 mobility, firewall functionality, and IPSec interoperability.

Deployed in October 2003, the first phase of the Moonv6 project tested basic applications crucial to the commercial rollout of IPv6, including file transfer protocol (FTP), Telnet and videoconferencing applications. The second phase of the Moonv6 project began on February 2 and ran through April 7, 2004. With an international roster of service providers, the second phase focused on demonstrating high-speed links, advanced routing functionality, firewalls, quality of service (QOS), and other key features of IPv6 over a carrier-class architecture. Second phase test results revealed the functional stability of IPv6 and helped validate the protocol for the North American market.

Sixteen vendors participated in the third round of interoperability tests on Moonv6, titled the “November Test Set,” during November of 2004. This test event further proved that the basic functionality of IPv6 was stable and capable of running key data communications applications such as voice-based services and multicast. Moonv6 had revealed that the new protocol presented no major hurdles to deployment and adoption beyond specific device implementation or user configuration issues.

As the project moves forward, Moonv6 aims to extend virtual Internet backbone with the ability to do pre-production IPv6 testing for security, multimedia, roaming devices, and other services. In the future, Moonv6 will serve as a deployment test bed and continue to empower service providers and suppliers from sectors including industry, universities, research laboratories, Internet service providers and U.S. government agencies. Moonv6 will offer participants, who wish to test IPv6 capable technology:

- A neutral interoperability setting designed to reduce time to market and ease of deployment;
- compressed research, debugging and development cycles enabling faster and smoother creation of end-to-end networking solutions; and
- an ongoing platform for global IPv6 education and knowledge enhancement.

JITC Testing

The DoD IPv6 Capable Exercise (ICE) for Moonv6 was designed to evaluate the implementation of IPv6 within the industry from a product Commercial Off The Shelf (COTS) standpoint. By doing so, JITC would validate data analysis, test and evaluation procedures and create a DOD IPv6 Approved Products List (APL) by which program managers would be able to select IPv6 capable products tested by JITC and approved by the DoD.

From 24 October until 18 November, vendors of both the automated test industry (Agilent, Ixia, and Spirent) and network equipment from original equipment manufactures (Cisco, Hewlett-Packard, and Juniper) entered into testing arrangements with JITC.

RFC conformance testing results were varied. Because automated test suites were used from Ixia, Spirent and Agilent, it became apparent that it was very difficult to assign failures on each IPv6 RFC implementation from Cisco, Juniper, and Hewlett-Packard. Therefore, product testing priorities are being re-focused on interoperability and performance based on DoD criteria.

Test Scenarios and Results:

Consistent with earlier phases in Moonv6 testing, the core network connected all sites in a static manner during the December 2005 test event. During the construction of the final network topology, protocol-specific test plans were executed at both the UNH-IOL and the JITC Ft. Huachuca sites. Engineers at each test site performed test activities for network applications. In some instances, advanced functionality was also tested.

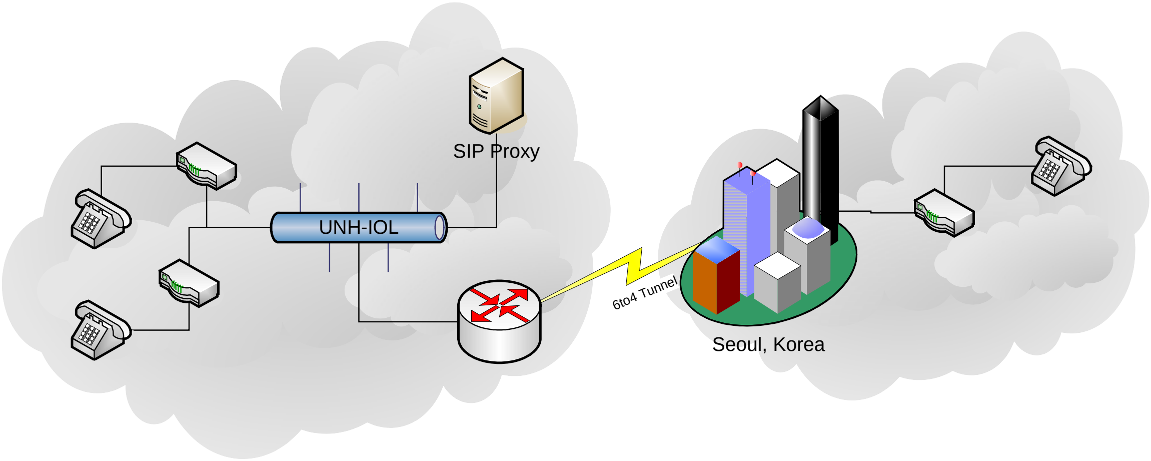
The majority of the issues that arose during the test event were predominately attributable to minor configuration mistakes. There was, however, a crucial interoperability failure during a few IPSec implementations. This failure was situated within the Neighbor

Discovery process. A number of implementations performed encryption on packets matching their Security Policy Database, whether or not the packet was a part of the Neighbor Discovery process. Other implementations automatically bypassed the IPSec traffic for Neighbor Discovery packets. This presented a problem when attempting to pair two devices with different stances on the encryption of Neighbor Discovery traffic. Specifically, while one device encrypted traffic and expected encrypted traffic in return, the other device neither encrypted traffic nor expected it to be encrypted. Consequently, the Neighbor Reachability failed and the devices were unable to communicate with one another.

Voice over Internet Protocol Testing

Voice over Internet Protocol (VoIP) transmits voice data over a packet switched network using the Internet Protocol. During the December 2005 test event, the Session Initialization Protocol (SIP) was used to successfully establish VoIP calls.

A commercial implementation of VoIP successfully initiated voice calls between two telephones in the UNH-IOL utilizing a SIP proxy. Calls were also connected to and from South Korea over a 6to4 tunnel utilizing a SIP proxy housed in the UNH-IOL. This marked the first international commercial VoIP call using IPv6 made from North America. Despite the successful completion of the calls between New Hampshire and South Korea, there were several voice quality issues. These quality issues were attributed to tunnel latency. During the test event, the system underwent a series of minor reconfigurations that resulted in successful calls established from a call generator to a telephone in the UNH-IOL by using a SIP proxy.



IPv6 Mobility Demonstration

IPv6 mobility (MIPv6) is a protocol that enables a node to be reached at a single IPv6 address while switching physical networks. MIPv6 is performed between three types of devices, the Mobile Node, the Home Agent device, and the Correspondent Node. The Mobile Node switches networks while retaining reachability with a single address. This device communicates with the Home Agent device, located on the edge of the Mobile Node's home network. The Home Agent tunnels traffic to the Mobile Node while it is away from home. The Correspondent Node is any node that establishes communication with a Mobile Node.

The December 2005 event tested an implementation of the Home Agent. This particular implementation, intended for a small quantity of Mobile Nodes, successfully operated with a Mobile Node emulator running at ten times its expected capacity. During the test the implementation also performed the route optimization process.

IPSec Testing

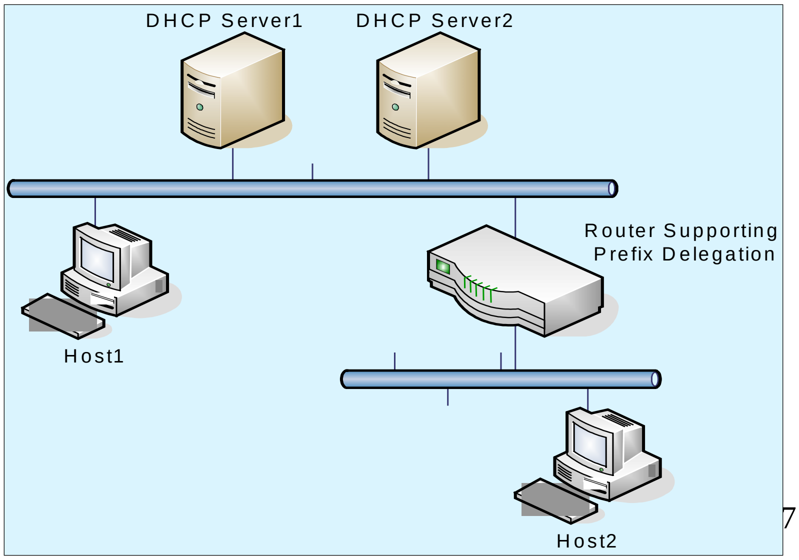
Securing Internet traffic at the IP level has become a necessity given the widespread use of the Internet as a business communication medium and the ever-growing levels of valuable personal data stored on remote servers. This latest round of Moonv6 testing saw IPSec vendors with a wide range of capabilities.

Event engineers observed successful interoperation between manual keyed implementations and those using Internet Key Exchange (IKEv1) with Pre-shared Keys. However, configuration errors emerged related to the manual keys, offering additional evidence and underscoring the need for reliable implementations supporting automatic-keying protocols.

The most prevalent issue encountered during the security testing centered on the encryption of Neighbor Discovery traffic. Several vendors encrypt all Neighbor Solicitations, Neighbor Advertisements, Router Solicitations, and Router Advertisements by default, particularly if they match a Security Protocol Database (SPD) entry. Other vendors bypass this type of traffic by default, even when it matches an SPD entry. Consequently, this discrepancy has led to significant interoperability problems.

DHCP Testing

The success of IPv6 in the enterprise and consumer markets is contingent upon IPv4 equivalency. A fundamental facet of equivalency is the automatic configuration of hosts, primarily through Dynamic Host Configuration Protocol (DHCP). The December event witnessed the largest group of DHCPv6 capable devices in a single location to date.



During testing, host vendors were able to acquire both Domain Name Server (DNS) Information and prefix information for DHCP servers. In a landmark event, a DHCP network that utilized prefix delegation was constructed between five separate vendor devices. The network router received a DHCP address prefix with 48 bits. The router then delegated 64 bit prefixes to its network hosts, in this instance Host 2. Host 1 also configured a DHCP server and received configuration information for other servers.

Firewall Functionality Testing

In our current Internet climate, not all packets can be trusted to have complete network access. Firewalls must therefore be utilized to block potential attacks and restrict the type of traffic flowing in and out of a network.

The December Moonv6 event witnessed several firewall implementations over a variety of cases. Both stateless and stateful firewall implementations were shown to correctly interoperate with various protocols including, Transmission Control Protocol (TCP), FTP DNS and IPSec. In addition, several performance metrics were examined including, maximum concurrent TCP Connections and maximum application transaction rate.

Conclusion

The Moonv6 December 2005 test event was the first to center on the IPv6 access layer and the establishment of key IPv4 equivalencies. General findings include:

- A greater number of companies appear to be committed to enabling DHCPv6 for simplified network administration, demonstrating growing confidence and commitment to implementing the technology;
- IPv6 has matured to the point at which it can be used to complete a commercial VoIP call between North America and other continents across the globe;
- IPv6 is capable of carrying mixed voice and data traffic;
- DHCPv6, DHCPv6 prefix delegation and DNS resolution are equivalently functional in v6 verses v4;
- Basic mobility, firewall and security functionalities are operable.

In addition, to date the Moonv6 project has helped to verify FTP, Telnet and videoconferencing applications, high-speed links, advanced routing functionality, firewalls, quality of service (QOS), and other key features of IPv6 over a carrier-class architecture for the North American market.

Moonv6 remains an active and vital deployment test bed for service providers and suppliers that wish to test and demonstrate IPv6 capable technology. As an ongoing platform for global IPv6 education and knowledge, Moonv6 remains committed to helping to build a firm foundation of interoperability for the sound deployment of the next-generation Internet.

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.
BRAS	Broadband Remote Access Server.
DoD	United States Department of Defense.
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.
IS-IS	Intermediate System to Intermediate System
JTA	Joint Tactical Architecture. The list of standards that the U.S. DoD uses as requirements in its networks.

LDAP

Lightweight Directory Access Protocol. A standards based method of remotely accessing information directories based on the X.500 model.

MLD

Multicast Listener Discovery. An IPv6 registration method for hosts to receive multicast data destined to a certain multicast address. Replaces Internet Group Management Protocol (IGMP) for IPv4.

MPLS

Multi-Protocol Label Switching.

NAT

Network Address Translation. This concept is used to solve the problem of lack of IP addresses within an AS.

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.

PIM-SM

Protocol Independent Multicast, Sparse Mode. a protocol for efficiently routing multicast traffic groups that may span wide-area networks.

PPP

Point-to-Point Protocol. A standard encapsulation method for transporting IP traffic over point-to-point links.

PPPoE

PPP over Ethernet.

RIP

Routing Information Protocol. Currently an Internal Gateway Protocol (IGP) for IP Routing primarily used small home and office networks.

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.
SPT	Shortest Path Tree.
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.

draft-ietf-idr-bgp4-23 Y. Rekhter, T. Li, S. Hares, A Border Gateway Protocol 4 (BGP-4).

draft-ietf-mobileip-ipv6-24.txt D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6.

draft-ietf-pim-sm-v2-new-09.txt Bill Fenner, Mark Handley, Hugh Holbrook, and Isidor Kouvelas, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised), February 2004.

Joint Technical Architecture (JTA) List of Mandated and Emerging Standards (LMES) Version 5.1 (Draft) dated 21 July 2003.

Participants

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

iol	INTERNET 2™	JOINT INTEROPERABILITY TEST COMMAND Improving Combat Effectiveness Through Interoperability
NORTH AMERICAN IPV6 TASK FORCE	AIR FORCE COMMUNICATIONS AGENCY	SPAWAR

Agilent Technologies Innovating the HP Way	AlaxalA	CHECK POINT™ Software Technologies Ltd.	hp ® invent
IXIA	Juniper® NETWORKS	Lucent Technologies Bell Labs Innovations	MERCURY CORPORATION
NORTEL NETWORKS	Panasonic.	SPIRENT. Communications	symantec.

Special Thanks To:

Jim Bound, Hewlett Packard and North American IPv6 Task Force Chair
Alan Bavosa, Juniper Networks
Ethan Burns, UNH-IOL
Timothy Carlin, UNH-IOL
Ankur Chadda, Spirent Communications
Mary Clouter, Hewlett Packard
Diego Dugatkin, Ixia
Captain Jeremy Duncan, JITC
Andrew Gadzik, UNH-IOL
William Gauvin, Symantec
Byong-kuk Jeon, Mercury
Hector Mayorga, Alaxala
Eran Nafusi, Check Point
Tom Peterson, UNH-IOL
Chris Pyne, Lucent Technologies
Yurie Rich, Native6
Ben Schultz, UNH-IOL
Kashif Shaikh, Nortel
Marc Sordi, Hewlett Packard
Zlata Trhulj, Agilent Technologies
Chris Volpe, UNH-IOL
Erica Williamsen, UNH-IOL
Tim Winters, UNH-IOL