North American IPv6 TASK FORCE

Date: November 14, 2002
To: Richard Clarke
Cc: Marcus Sachs, Tiffany Brittany, and Howard Schmidt
From: Jim Bound, Mike Brig, and Latif Ladid (NAV6TF Steering Committee)
Subject: IPv6 Response to National Strategy to Secure Cyberspace Final V2.0

Richard,

On behalf of the North American IPv6 Task Force (NAV6TF) we provide our IPv6 technology response to the "The National Strategy to Secure Cyberspace" DRAFT September 2002. Our web page can be viewed at: http://www.nav6tf.org/.

IPv4 Infrastructure Problem for Cyberspace

The current IPv4 infrastructure requires adaptations to serve the needs of users on the Internet and those using the Network Infrastructure of IPv4. These adaptations are all too often band-aids to a problem that cannot be fixed with IPv4. IPv4 has served us well and no one could foretell the future of the current Internet, and that it would play a major role as a technology tool and catalyst for so many functions within our society.

The band-aids like Network Address Translation (NAT), the lack of Security as an integral part of the current Network Infrastructure, and the inherent costs of performing translations at the edge of a network are problematic. The current infrastructure requires state as a method of operation and this requires extensive management. The end result of NAT is that end-to-end connectivity between two entities was lost. But, the NAT paradigm is now part of many network infrastructures in the U.S., and would have to be considered for any transition to IPv6.
.
Here are some problems we see in the current Network Infrastructure:

- NAT does not provide network security.
- NAT reduces the possibility of end-to-end communications.
- NAT reduces the possibility of end-to-end security.
- NAT reduces the possibility of end-to-end applications (peer to peer).
- NAT reduces the possibility of seamless mobile computing.
- NAT causes scalability and performance problems at the edge of the network.

- NAT is a single point of failure and an attack for a network.
- NAT and IPv4 routing table size force many networks from utilizing dynamic routing and therefore make them more vulnerable to attack or failure.
- Security must be added and is not integral to the current IPv4 protocol.
- The current IPv4 protocol does not have the address space without NAT to support the projected uses of the Internet.

The above issues will be problematic to the mission of the Cyberspace Security paper and other missions within the U.S. Government, where Network Infrastructure is mission critical for the success of a strategy and meeting key objectives.

IPv6 Infrastructure Benefits for Cyberspace

IPv6 is capable of resolving the problems of IPv4 and trial network test beds have been in process since 1998. The key benefits to Cyberspace from IPv6 are as follows:

1. Extended Address Space 2^128 from 2^32 currently.
2. NAT is not required so all the losses above from NAT are provided back to users of the Internet and Network Infrastructure.
3. Security is built-in to IPv6 and required for compliance (MUST) at the network layer of IPv6. IPsec is that security protocol set.
4. Auto configuration of nodes is inherent within the IPv6 architecture and uses a stateless methodology, but stateful is also supported.
5. Mobility is inherent in IPv6 and part of the architecture.
6. IPv6 is built to be extensible so new functions can be added to the protocol to support emerging requirements.
7. IPv6 would improve security by enabling ISPs to statically assign address blocks to customers and reduce or eliminate the need for DHCP/dynamic IP address assignment.

The bottom line is that IPv6 is a required enhancement to help alleviate the basic problems of the current Network Infrastructure. Here are some examples:

An important person in government is using their laptop to communicate information from Logan Airport in Boston to colleague in Washington D.C. With IPv6 there is no NAT so the communications is end-2-end. The firewall at the Airport is busy doing what it should do and that is providing a Firewall and Public Key Infrastructure to users to access their keys and using IPsec as the user. The person in Logan can attach to Washington directly and verify their keys peer-to-peer (cannot do that with NAT) and begin secure communications end-to-end. In addition with IPv6, the person in Logan could change their mind and go to Boston to Hotel and put their laptop in stand by mode and be connected when back in the Hotel room, or continue correspondence from in the Taxi to the Hotel because of Mobile IPv6 inherent in IPv6.

There is a problem similar to 911 and the Air National Guard, Police, Fire Fighters, U.S. Marshals, and Special OPs must converge in an expedited manner and all receive the same communications channel instantaneously upon arrival to resolve the conflict or lend assistance, and be able to communicate with each other, and all this must be secure. The communications needs be ready to take place anywhere, anytime, anyplace. To think about private communications lines U.S. wide would be a cost beyond what we could bare, thus, the Internet could be used U.S. wide at critical times as those like 911. This cannot happen with NAT or the current Network Infrastructure. IPv6 could be used to establish instant secure communications because the backbone of the Internet and nodes Network Infrastructure are using IPv6 and the built-in Security. The defense-coordinated unit for conflict resolution can be automatically configured as a network for communications command channels and amongst themselves as a network entity, upon arrival to the location.

IPv6 is still new and vendors have just begun to ship products and in the U.S. we are far behind other world Governments in Europe and Asia.

IPv6 Deployment Strategy Recommendations

1. Add to the paper that IPv6 is critical to the future Cyberspace problem set. State current problem and the benefits from IPv6. This would be under a Network Infrastructure section within the paper defining the problem above.
2. Add to the paper recommendation to the Vendors, Application Developers, Security Developers, and Service Providers that IPv6 is a requirement to our U.S. Cyberspace and for our U.S. Network Infrastructure in general.
3. Add to the paper a recommendation that a U.S. Government IPv6 Transition process begin now and be documented in future addendum papers.
4. Add to the paper that IPv6 should not be deployed on production networks without trial test beds, but that IPv6 trial deployment should begin now and procurement policy include IPv6 as a box to be checked by suppliers in their strategy and future product releases.
5. Add to the paper the problems above with IPv4 and list the benefits of IPv6, and why the request for this technology is being stated.

.
The Joint Chiefs message to the DoD to begin IPv6 test beds and trial networks, but don't put it in production, until more tests and a transition strategy have been developed we adopt too within the NAV6TF. It is important for some period of time to develop further U.S. IPv6 test beds, before IPv6 is used for mission critical networks.

Sincerely,

NAV6TF Steering Committee Members

Jim Bound
Chair IPv6 Forum Technical Directorate
Hewlett Packard Staff Fellow
Jim.Bound@hp.com
603-884-0062

Latif Ladid
Trustee, Internet Society
President, IPv6 Forum
VP Ericsson
latif.ladid@village.uunet.lu
+352 30 71 35

Michael P. Brig
Next Generation Internet Program Manager
U.S. Navy SPAWAR
brigm@spawar.navy.mil
843-218-4675