North American IPv6 TASK FORCE

Title: **NAv6TF NTIA IPv6 RFC Response Addendum 1**

Security, Transition, Interoperability and Research Agenda

Editor: **Jim Bound**

Date: **05/10/04**

Version: **FINAL**

Contents

Executive Summary

This is the North American IPv6 Task Force's (NAv6TF) www.nav6tf.org addendum #1 response to the NTIA IPv6 RFC. This response is to answer follow up questions regarding the IPv6 RFC as follows: International Interoperability, IPv6 Transition Security, Public Key Infrastructure, and US Government IPv6 suggested IPv6 research agenda. This response is accompanied by three other NAv6TF submissions: IPsec Security Briefing with Notes Documentation, IPsec and Internet Key Exchange Update Briefing, and IPv6 Security White Paper.

1. International Interoperability

During the initial discussions of Cyber security supporting IPv6 within the President's Critical Infrastructure Board 2001 and 2002 with industry participants, the question was asked "what is the affect to the U.S. if other geographies support IPv6 for their Internet infrastructure?". The context had several perspectives, which the NAv6TF responded to in the public response:

http://www.nav6tf.org/slides/NAV6TF_PCIPB_INPUT_PART_II.pdf .

The NAv6TF responded first to the affect of IPv6 on the global economy, and second to the affect of IPv6 interoperability for U.S. multinational companies. As the Internet moves to a mobile society it will require IPv6 and Mobile IPv6, as the NAv6TF has suggested in previous responses. The transition, products, and services to support the evolution of mobility will generate revenue, investments, and competitive positioning for leadership across the global mobility markets. If the U.S. geography does not provide an IPv6 infrastructure and leadership for that deployment, then it will not benefit from the eco-systems created from the evolution of that mobile society, and possibly may not be able to support that evolution within the U.S. geography in a time-to-market manner for gross product revenue to the nation. Another concern from the lack of IPv6 infrastructure and services is as IPv6 becomes the dominant Internet protocol in non U.S. geographies, interoperability can become an issue for U.S. multinational companies, or any form of Internet communications to and from the U.S.

The U.S. is driven by an open and free enterprise market, and the NAv6TF would not support the U.S. Government creating mandates within the private sector for IPv6 deployment. But, the NAv6TF does recommend that the U.S. Government broadcast and support widely, within its final analysis of IPv6 through NTIA, that the effects of IPv6 on the global economy and multinational interoperability could be a potential issue or opportunity for the U.S, if IPv6 adoption is to slow or non-existent within the U.S. private sector.

The NAv6TF also recommends that the U.S. Government, as its own business and entity, follow the leadership of the Department of Defense and design a plan to begin the deployment of an IPv6 capable infrastructure for Internet communications by some specified date. That deployment can begin with research development, and network pilots as specified in section 4 of this response, simultaneously with the deployment of IPv6 capable systems, which can continue to be used with IPv4, but begin to provide a path to IPv6 from product installation within the U.S. Government.

2. IPv6 Transition and Security

The IPv6 Forum and NAv6TF are currently reviewing the IPv6 transition mechanisms, which provide a set of tools to assist the transition to IPv6, and a report on all implemented mechanisms will be provided at a later date. The NAv6TF believes that one size does not fit all for transition and different mechanisms (e.g. 6to4, Teredo, Tunnel Broker, DSTM, and ISATAP) are required for different IPv6 adoption and deployment scenarios. In this response the NAv6TF will focus on the tunnels mechanisms.

But three common abstractions exist for all transition mechanisms using tunnels:

1. *Encapsulation and Decapsulation tunneling of an IP packet is required on the network.*
2. *IPv4 or IPv6 can be the communications protocol between the two tunnel end points.*
3. *An architectural defined IPv6 prefix may be required for some mechanisms..*
4. *A globally routable IPv4 address is required for Internet networks.*
5. *Tunnel set up or inherent state is required for operation.*
6. *End-2-End security trust model can be supported over the tunnels.*

Tunnels have the same network security concerns as any packet with the added difficulty that the tunnel should be secure, and the end points secure to each other. The tunnel is a third party in the E2E communications model and it is prudent to verify two tunnel endpoints are in fact secure on an Internet network.

But, the security strength required for a particular trust level still remains with the security of either the IPv4 or IPv6 packet or effects from the resultant payload. Once the tunnel set up and end points are satisfied to be secure (for that entities security requirements) then the decapsulated packet requires all the security available for that communications. This means that for IPv6 the same security infrastructure processing and applications must be provided for IPv6, once IPv6 packets are processed within a node and within the network.

If an entity has a firewall or intrusion detection system for IPv4 and that is required, then that infrastructure has to be available for IPv6. This will mean current security methods for IPv4 will be required for IPv6. In addition IPv6 may introduce new security requirements, depending on where and how IPv6 is deployed, as an enhanced IP layer communications model, but please see NAv6TF NTIA IPsec Briefing with documented notes submitted to NTIA by Graveman and Esposito. The premise that IPv6 transition creates a security problem is false, but rather the lack of security mechanisms for IPv6 is the security potential problem.

IPv6 deployment will need to meet a higher bar than IPv4 had to meet for deployment regarding security, but IPv6 deployment should not wait for complete security solutions for all target markets. Each entity adopting IPv6 needs to review and make a list of their security requirements, as part of their IPv6 adoption and deployment plan and road map. As there is no one size fits all transition mechanism, there is not one size fits all security road map for all entities.

IPv6 will support as part of the transition IPv6 Proxy's and in some rare cases IPv6 to IPv4 Network Address Translation. The security requirements for these are well understood for IPv4 and the same rules of engagement for security will be required for IPv6.

3. Public Key Enablement and Infrastructure

Imperative to IPv6 efforts within the U.S. Government and private sector is IPsec as the E2E security solution for robust secure communications. But, also Public Key Enablement (PKE) and Public Key Infrastructure (PKI) to support a method for nodes to obtain keys and then use the IPsec defined Internet Key Exchange (IKE) methods to exchange those keys. Waiting on a standards body is a non-starter. It is the NAv6TF impression that the U.S. Government has a PKE and PKI policy and strategy. What is required to test this potential solution on the Moonv6 www.moonv6.org network pilot for IPv6, and thus on vendor and integrator platforms supporting IPsec. There is also some type of PKE and PKI API specification required to retrieve the key from some source (PKI) and to know any policy switches a platform should configured to enable PKI (PKE).

IPv6 mandated the use of IPsec to support E2E secure communications at the IP layer of the Internet model, which provides a reliable level of security between two peers (but see Graveman and Esposito IPsec Briefing). In addition there exists the IKE methods supporting IPsec that permits two peers to share keys for IPsec communications. But, what is missing is a PKE plan to support a PKI across the U.S. geography assuring the implementation of IPsec with the deployment of IPv6.

Smart cards are a good idea and will work for client nodes, but NAv6TF believes there also should be a network access method for router and server nodes, which are difficult to provide PKI via Smart Cards.

So what we need is as follows:

API spec and parameters to read public keys at the client and the network, and a set data structures defining that key.

Web interface for servers and routers that use TLS and Access Controls, as examples, to log into from Servers and Routers to download keys. Then the API above can be used to set it up (the DNS is also an option for initial testing).

The other way to get the key is by using a certificate authority server using X.509 for testing and that has defined PKE and PKI from several vendors, the way to access those could be via AAA clients, as another example.

In addition to PKE and PKI it would be good to begin to relay to the vendors what they need to do to support Intrusion Detection Services (IDS) on an IPv6 network.

All of these requirements are essentially portrayed at the NIST http://csrc.nist.gov/pki/ site. But, there is an urgent and immediate need for IPv6 PKE and PKI. The NAv6TF suggests and recommends the U.S. Government could assist the industry and private sector at large to establish an IPv6 PKE and PKI methodology, strategy, and implementation plan. But, it is important to note that the need is great today and will be more critical each day as IPv6 deployment matures in the global market and for the mobile society evolution in process currently.

4. U.S. Government IPv6 Research Recommendations

The NAv6TF recommends the U.S. Government define a research agenda for IPv6 that would assist the U.S. private sector to achieve medium and long term IPv6 evolutionary requirements and that would benefit U.S. Governments interests regarding IPv6.

- The development of additional IPv6 network pilot sites working with the DOD and NAv6TF to support and use the Moonv6 network pilot to execute IPv6 functions on a real IPv6 Internet network. Suggested initial network pilots are FAA, SSA, DHS, NTIA/NIST, and VA.
- Open public security implementation lab to support the research and development, and testing of security protocols, PKE/PKI/IPsec, and Intrusion Detection for IPv6 networks.
- Open public Department of Homeland Security implementation lab for research and development, and testing to determine how IPv6 can assist with the technology evolution to support Home Land Security.
- Open public mobile IPv6 wireless lab to support the research and development, and testing of mobile networking, and eventually providing some mobile IPv6 wireless network deployment for the private sector from the benevolence of government (e.g. kids.com, National Weather/Public Radio).
- Open public IPv6 transition lab to support the current IPv6 transition mechanisms, porting of critical U.S. Government open applications, and to research potential emerging IPv6 Transition requirements and methods working with the private sector.

NAv6TF Organization, Acknowledgements, and Contact Information

Organization History

In July of 2001, at U.S. Navy SPAWAR IPv6 Seminar in Charleston, SC, and then again in December 2001, at a U.S. Army Seminar at FT. Monmouth, NJ, the initial creation of the North American IPv6 Task Force (NAv6TF) www.nav6tf.org was solidified. The NAv6TF is a Task Force under the auspices the IPv6 Forum www.ipv6forum.com and provides for the promotion, consultation, a center of technical expertise, white papers, business and marketing support, educational support, and guidance on for the adoption and deployment for IPv6. Additional information can be found at the side bar regarding the Steering Committee, Objectives, Target Industries, and Workgroups.

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 and others developed the idea for Moonv6 www.moonv6.com during its work to support the U.S. Government Cyberspace Security Office and Department of Defense as two entities the NAv6TF worked with in the IT sector to promote, consult, and define IPv6 technology deployment issues and objectives as a Task Force. The NAv6TF provided volunteer resources that participated in the Moonv6 technology and network requirements to assist the University of New Hampshire and Department of Defense to design the Moonv6 network, developed the Moonv6 Web Page, provided an initial vendor base within the

NAv6TF to support Moonv6, provided engineers to support the Moonv6 U.S. sites and test centers, worked with Internet2 community to support Moonv6, and has been an IPv6 conduit for all entities across the North American geography for Moonv6 and IPv6 in general, and fulfill the role of overseer as a body for Moonv6.

The actual definition of Moonv6 was defined at the previous mentioned NAv6TF meeting with the Cyberspace Security Office and Department of Defense participants during discussions to determine how serious should the U.S. take IPv6 as a mission. The question posed to the particip ants was should we treat IPv6 as we did going to the Moon in 1969? Later when it was decided to investigate how to deploy a U.S. wide IPv6 Network Pilot at a meeting at the University of New Hampshire in March of 2003, including NAv6TF, University of New Hampshire, and Department of Defense principals, the term Moonv6 was selected to name this Network Pilot.

The NAv6TF is also working with other IPv6 Forum Task Forces around the world to support the adoption and deployment of IPv6. NAv6TF has signed a Memorandum of Understanding with the China IPv6 Council as one example.

Acknowledgements:

The editor would like to thank the NAv6TF membership who have made many significant contributions to IPv6 with papers, briefs, and presentations from which much of the material for this response came from in this response. Specifically acknowledgements to significant NAv6TF subject matter experts contributions used for this response: John Baird, Rich Graveman, Gene Cronk, and Latif Ladid. Also thanks to all vendors worldwide who have shipped IPv6 products to support the deployment of IPv6.

Contact Information and Editors

Jim Bound

IPv6 Forum Chief Technology Officer

Chair NAv6TF

Hewlett Packard Fellow

Jim.Bound@nav6tf.org