White Paper – Security Risks of Not Migrating to IPv6

AFCEA International, Cyber Committee
Gilliam E. Duvall, The National Defense University – iCollege
Patrick McNabb, Booz Allen Hamilton, Inc.
Tiffiny Smith, Booz Allen Hamilton, Inc.
Ingvar Hellquist, The Swedish National Defence College

What is IPv6 and why is it needed?

Internet Protocol version 4 (IPv4) is the primary communication protocol for the Internet. IPv4 provides 4.3 billion addresses. When IPv4 was initiated, no one ever expected to use that many addresses. When IPv4 was originally developed as an experiment for a small group of organizations to communicate, no one ever anticipated the explosion of devices that would drive the need for additional unique addressing options. In addition to standard desktop computers, servers, routers, and network devices that require IP addresses, the proliferation of mobile devices and consumer electronics and appliances that require IP addresses have driven the depletion of the available IPv4 space.

The Internet Engineering Task Force (IETF), Regional Internet Registries (RIRs), Internet service providers (ISPs) and many others made several innovative initiatives to expand the life of IPv4. Efforts included network address translation (NAT), tighter control of address allocation, reclaiming unused address space and port address translation. However, nothing could prevent the inevitable depletion of addresses.

On February 3, 2011 the Internet Assigned Number Authority (IANA) allocated the remaining "class A" block of IPv4 address space (http://www.nro.net/news/ipv4-free-pool-depleted). IANA provides Internet address to the RIRs and will now only have Internet Protocol version 6 (IPv6) addresses to provide. The depletion of IPv4 addresses was anticipated many years ago. The IETF has been maturing IPv6 for many years in preparation for this transition. Since the main driver to change to IPv6 is address depletion, it is good to know that IPv6 provides 2128 (approximately 340 undecillion or 3.4×1038) addresses. This is expected to provide an acceptable amount of address space for the foreseeable future.

In addition to address space by itself, IPv6 will allow devices to communicate directly, as was the original intent of the Internet. Additionally, IPv6 is designed with the ability to incorporate Quality of Service (QoS) improvements and recommended use of Internet Protocol Security (IPSec) architecture for all Ipv6 nodes [RFC4301], performance aspects that had to be added on to IPv4 to correct design limitations.

IPv6 Transition Methods

The ideal IPv6 implementation is to install the protocol as a stand-alone Internet protocol solution in an enterprise environment. However, many organizations do not see the need to convert their enterprise networks to the IPv6 protocol because they see Internet accessibility as still being "good enough." As the mobile device market place advances the current IPv4 address allocation will not be enough to keep up with customer demand for Internet accessibility for all sorts of devices. Many security vendors are waiting for increased customer demand before implementing support for IPv6. Since IPv4 and IPv6 are not compatible protocols, organizations must plan a way to move from IPv4 to IPv6. While there are some vendors that support full IPv6 implementation solution, many do not support IPv6 at all or only offer strategies for a hybrid transition to an IPv6 solution using the current IPv4 architecture.

There are three currently three IPv4 to IPv6 transition technology strategies: 1) the dual-stack network architecture, 2) the translation technology architecture, and 3) the packet tunneling architecture.

1) Dual-Stack Network Architecture

The dual-stack network architecture is a recognized enterprise co-existence strategy. Dual-stack refers to running the two protocols, IPv4 and IPv6, in parallel. Essentially, both protocols are active. Usually one protocol is preferred and network traffic attempts to use the preferred protocol first. If traffic cannot complete its path with the preferred method, the traffic will try again using the secondary protocol. The primary reason the traffic would not reach its destination using the preferred protocol is because some network segment in the traffic's path does not support the preferred protocol. For example, an email from a client PC that is dual-stacked and prefers IPv6 will try to send its traffic to the recipient PC via IPv6. If any portion of the email's path does not support IPv6, such as a router, a server, or even the receiving client, the traffic will not complete its path and the sending client will send the message again, but using IPv4 this time.

The advantage to dual-stack is that the equipment that exists for the IPv4 network can likely be used for the IPv6 network, assuming it is already IPv6 capable. This method allows an organization to use IPv6 where it can, but allow organizations more time to migrate from legacy systems since the IPv4 infrastructure remains.

2) Translation Architecture

The translation technology architecture approach is the process which converts an IPv4 packet to an IPv6 packet and vice versa for network traffic purposes. This is typically done by a device at the network border. The advantage of using translation is the only change the organization has to make is the addition of the translation devices.

3) Tunneling Architecture

The tunneling architecture solution is a method that encapsulates IPv6 packets inside IPv4 transmission streams. Several options exist for tunneling protocols such as 6to4, Teredo, Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and generic routing encapsulation (GRE). The advantage of this method is also the low cost and ease of implementation. The risk of this method is security. Allowing tunneling on the network may disguise threats from network administrators and defense sensor devices. For this reason tunneling is considered a high risk IPv6 transition method.

Risks of not Transitioning Directly to IPv6

The risks of not pursuing a direct implementation path to the new protocol exist in two key areas: 1) security risks in using IPv6 transition technology architectures, and 2) risks to U.S. technology research and development (R&D) leadership by not developing a competitive IPv6 industry knowledge base

1) Transition Architecture Risks

All three transition technology architectures seek to defer direct implementation of the IPv6 protocol in favor of retaining an IPv4 network equipment base. For this reason all three transition methodologies carry the same central cyber security risks. The central disadvantage to these methods is that the organization is essentially running two networks, an IPv4 one and an IPv6 one. Both protocols have to be secured, monitored and managed. Depending on the availability of network tools and trained technicians the operational cost to maintain expected performance levels for two network types can be significant.

The information security implications of running a two-protocol hybrid are also not fully understood. Baseline security requirements need to be established for the IPv4 environments then the baselines need to be examined for their ability to adapt to the new IPv6 infrastructure. A gap analysis needs to be conducted to determine where the existing security measures of a transition solution will fall short compared to an IPv6 only solution. As organizations evaluate integrating IPv6 into their infrastructure, they must consider whether IPv4 based infrastructures will inject security issues into the IPv6 environment and vice versa. In addition to common IPv4 vulnerabilities, there are some security features inherent in IPv6 (e.g., encryption of packet content) that if fully implemented will make the IPv4 monitoring side of a transition architecture inoperable. The attacker community poses a serious risk to all organizations connected to the Internet and is quickly adapting its techniques to the IPv4 to IPv6 transition architecture environment.

Without direct implementation of IPv6 and no mandate of which of the three conversion technologies to use Internet infrastructure will become even more complicated and non-standard as organizations select individual conversion technologies. In addition to the limitations

discussed previously, the overall disadvantage of technical solutions which do not provide a direct transition to IPv6, but rely on combinations of Dual-Stacking, Translation, and Tunneling will be the creation of a fragile Internet. While the effects of combining Dual-Stacking, Translation, and Tunneling on large-scale IPv6 conversion is unknown, it certainly will require implementation of multiple technical solutions to mitigate individual weaknesses identified earlier and anticipate aggregate Internet performance issues in a combined technology solution.

The mixture of conversion methods across multiple organizations creates two problems. First, there will be increased complexity to the Internet address routing table infrastructure. Failure of any one of the conversion methods could result in a cascading breakdown or delay, thus degrading overall Internet performance. Second, there will be increased IPv4 operating costs to maintain complexity of backward compatible system technologies.

2) Risks to the Industry IPv6 R&D Knowledge Base

Since the invention of the Internet, the United States government and its industry partners have been leaders in IP product innovation and service development. This has been due to the early-adoption of technology by U.S. companies.

Currently, there are multiple international corporations and foreign government owned entities already in full IPv6 compliance hardware and software production for implementing public and private section business endeavors. As IPv6 use increases, organizations will look to vendors with significant experience in IPv6 installation, service, and application issues. A U.S. industry knowledge base which overly concentrates on maintaining current IPv4 solutions (vice a IPv6 conversion strategy) runs the risk of being left behind and could lose a competitive advantage in an world seeking innovative, robust IPv6 products and services where a competitive edge in government and business depends on the increased Internet accessibility, QoS and IPSec capabilities offered by IPv6.

There are several specialty areas where the U.S. IPv6 industry knowledge base needs to be in positions of leadership. These disciplines include program management, enterprise application development, and security configuration planning.

An experienced IPv6 program management industry base is critical to successful IPv6 transition. This requires close coordination and cooperation among all stakeholders. It is critical that an organization clearly define roles and responsibilities, a transition management structure, as well as all of the processes to be performed. The organization should define stakeholders responsible for policy and guidance, as well as for executing and enforcing it through an established budgetary and acquisition review processes. A formal transition plan should lay out a coordinated transition across the organization with roles and responsibilities clearly defined. Coordination and integration of efforts may be achieved through the creation and use of a set of IPv6 cross-organizational working groups, under a senior-level IPv6 Transition Team to address critical issues during the transition.

IPv6 project planning experience necessary to ensure that transition to an IPv6 infrastructure optimizes performance, interoperability, security, scalability, and reliability. The network design must consider IPv6 addressing and naming services, information assurance requirements and software applications. The IPv6 transition must not be disruptive to the everyday business of the organization. The issues to be addressed during transition include:

- Maintaining end to end network and application interoperability during the transition period
- Maintaining interoperability with business partners networks
- Ensuring no additional security vulnerabilities are introduced by transition

Industry expertise will be needed in transitioning enterprise system and developing end user applications that use IP as the communication protocol to IPv6. The transition to IPv6 will also have positive impacts on networking applications that are critical to the operations of any enterprise. Examples of these networking applications include:

- Network security applications such as firewalls, IDSs, and PKI.
- Network management and operations applications and utilities.
- Network Internet infrastructure applications such as web servers, mail servers, and FTP servers.
- Network system applications such as DHCP and Network Time Protocol (NTP).

The cost and management expertise required to transition all of these applications to support IPv6can be substantially higher than that for the transition of the networking infrastructure. An assessment of all applications must be made to ensure interoperability with the new more secured IPv6 environment. Finally, due to the many built-in security controls within IPV6 network security and administrative personnel will need to have updated training. The training will enable the organization to implement better security practices on the network level. This will also help in lowering the potential threats to their network.

Recommendations

The authors have three recommendations concerning IPv6 technology adoption and implementation. First, since the IPv4 address space is almost exhausted the only long-term solution is to deploy IPv6. IPv6 is not backwards compatible with IPv4, which means organizations will have to change their network infrastructure and systems to deploy IPv6. Rather than wait for the inevitable, organization should begin now to understand the risks and the risk mitigation strategies. Ideally, direct implementation of IPv6 should be implemented, but if a

hybrid IPv4/IPv6 technology implementation is planned, NIST recommends these actions to enable an organization to make a smooth, secure and successful transition[1].

- Apply different types of IPv6 addressing (privacy addressing, unique local addressing, sparse allocation, etc) to limit access and knowledge of IPv6-addressed environments.
- Develop a granular ICMPv6 filtering policy for the enterprise.
- Use IPsec to authenticate and provide confidentiality to assets that can be tied to a scalable trust model (an example is access to Human Resources assets by internal employees that make use of an organization's Public Key Infrastructure (PKI) to establish trust).
- Identify capabilities and weaknesses of network protection devices in an IPv6 environment.
- Enable controls that might not have been used in IPv4 due to a lower threat level during initial deployment (implementing default deny access control policies, implementing routing protocol security, etc.).
- Pay close attention to the security aspects of transition mechanisms such as tunneling protocols.
- On networks that are IPv4 only, block all IPv6 traffic. However, even if you block the IPv6 protocol at level 3, some areas of IPv6 protocol "slip through" will occur (e.g., addresses of various headers and inside protocols such as SMTP, SIP, etc.). This opens up new kinds of threat such as buffer overflows.

Organizations planning to deploy IPv6 will want to begin a dialog with their security vendors to support IPv6 as early as possible. Industries with track records of developing and securing IPv6 will be critical in successful IPv6 adoption and deployment.

The second recommendation addresses how IPv6 can be deployed. One starting point is to deploy IPv6 alongside IPv4, starting on a small scale at the periphery and working towards the core. IPv6 requires a systematic and controlled deployment for good accessibility and security therefore deploy IPv6 in four phases:

- Inventory: review the IT environment and investigate measures for a deployment that will maintain security and accessibility. Adapt procurement documentation with requirements for IPv6 and review the need for training.
- Plan: determine the type of addresses, produce an address plan, order IPv6 Internet connection. Procure new equipment and services and review processes, routines and security requirements.
- Activate: first activate IPv6 in the Internet connection, configure and commission firewalls and other network equipment. Then activate IPv6 in public e-services such as

[1] NIST SP 500-267, A Profile for IPv6 in the U.S. Government – Version 1.0, available at http://www.antd.nist.gov/usgv6/usgv6-v1.pdf.

DNS, external websites and for email. After that, enable users on the internal network to access external IPv6 services on the Internet. Check and monitor the deployment.

- Manage: monitor, follow up, adapt and deal with disruptions.

Be aware of consequences with respect to accessibility, security, and implementation cost. Deploy and manage IPv6 with the same level of quality as IPv4. Take into consideration that security work is an ongoing process. An additional protocol entails increased complexity. The cost of deployment depends on several factors. For example, the need for new hardware and software, the number of e-services, the size and complexity of the network, requirements for security and accessibility, training and the support of consultants.

The third recommendation surrounds maintaining an environment that fosters the Internet technology leadership position that has been held for so long by U.S. industries. This is an effort involving both public and private sector organizations. There should be an active IPv6 adoption and migration effort by the U.S. government. This will send a demand signal to industry and advance innovative R&D efforts to provide new services and products based on the IPv6 technology for the Internet of the future.

Proposals for further work

The public sector should deploy IPv6 to make it possible to communicate with everyone on the Internet. This means an increased demand for products and services with IPv6, which will accelerate progress. IPv6 should be considered in government framework contracts.