# IPv6 and deep packet inspection

Thomas B. Martin
Holy Family University

**ABSTRACT**

The current version of the Internet, IPv4 was depleted of addresses on February 3, 2011.[1] The shortage of addresses has led to the introduction of IPv6 which has 128-bit (16-byte) source and destination IP addresses. Many organizations do not see a reason to convert to IPv6, and believe they are not running IPv6.[2] Whether an organization knows it or not, any laptop/PC running Vista or Windows 7 is a vulnerability from which attacks can come that will be invisible to IPv4 networks.

Since the Internet today uses IPv4 for 99% of the traffic[3], it will be a slow migration to IPv6. Three transition strategies are being employed: header translation, dual stack and tunneling of IPv6 inside IPv4.[4] Tunneling is the most precarious method for today's IPv4 networks. The IPv6 packet is included inside the message field of an IPv4 packet. The contents of the IPv6 packet will not be noticed by an IPv4 firewall or intrusion detection system. Hidden IPv6 traffic running across an organization's network can wreak havoc, allow malware to enter the network, and be the basis for a denial of service attack.[5] The only defense against such attacks is deep packet inspection (DPI).

The widespread use of DPI is inevitable. The first serious security breach caused by tunneled IPv6 inside an IPv4 packet is certain to come in the near future. This event will be a stimulus to organizations to defend against such attacks.

Keywords: IPv4, IPv6, deep packet inspection, cyber terrorism, security

[1] http://www.icann.org/en/news/releases/release-03feb11-en.pdf
[2] S. Bradner and A. Mankin, "The Recommendation for the Next Generation IP Protocol", RFC 1752, Jan. 1995
[3] https://www.arin.net/knowledge/about_resources/ceo_letter.pdf
[4] Bihrouzan A. Forouzan, "TCP/IP Protocol Suite", 4th Edition, McGraw Hill, ISBN: 978-0-07-337604-2, 2010
[5] C. Caicedo, J. Joshi, and S. Tuladhar, "IPv6 Security Challenges", Computer, IEEE Computer Society, February 2009

## 1. THE IMPENDING WORLD OF IPV6

### a. Additional Addresses

The current version of the Internet, IPv4, was depleted of addresses on February 3, 2011.[1] The shortage of addresses has led to the introduction of IPv6 which has 128-bit (16-byte) source and destination IP addresses. This address space is: $2^{128}$ or about $3.4\times10^{38}$ (340 trillion trillion trillion).

IPv6 will create an era of "throw-away" IP addresses. Every light bulb, door lock, package of lunch meat, quart of milk, jar of mustard could be given an IPv6 address and an RFI chip that communicates the status. The lunch meat could indicate it is going stale, the mustard jar could transmit that it is past the recommended use period, the battery in our flashlight could send a "replace me" message to an RFID reader, the light bulb could indicate it is near end of life, the fire detector could transmit "my battery needs to be replaced," etc.

With every new technology, there are new security threats and vulnerabilities. Inequality of IPv4 distribution of addresses has caused other countries to embrace IPv6 before the United States. China is the world leader in IPv6 because of the need for more IP addresses, which cannot be supplied by IPv4, the current version of the Internet. The implications of the USA being behind in this field are ominous for security of organizations.

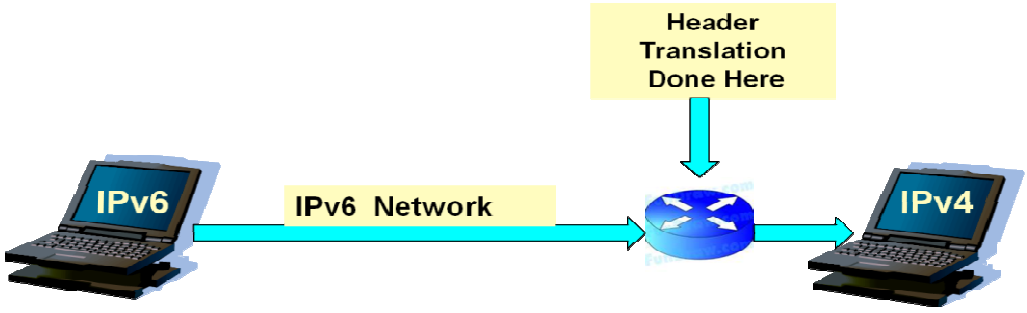
### b. IPv4 & IPv6 Will Coexist for a Long Time

Since the Internet today uses IPv4 for 99% of the traffic[6], it will be a slow migration to IPv6. Many organizations do not see a reason to convert to IPv6, and believe they are not running IPv6. However, Microsoft Vista and Windows 7 have IPv6 compatibility enabled as the default setting. Whether an organization knows it or not, any laptop running Vista or Windows 7 is a vulnerability from which attacks can come that will be invisible to IPv4 networks.

## 2. MIGRATION STRATEGIES FROM IPV4 TO IPV6

There are three techniques being used in the transition period from IPv4 to IPv6.[4] Each of these is shown in the graphics below.

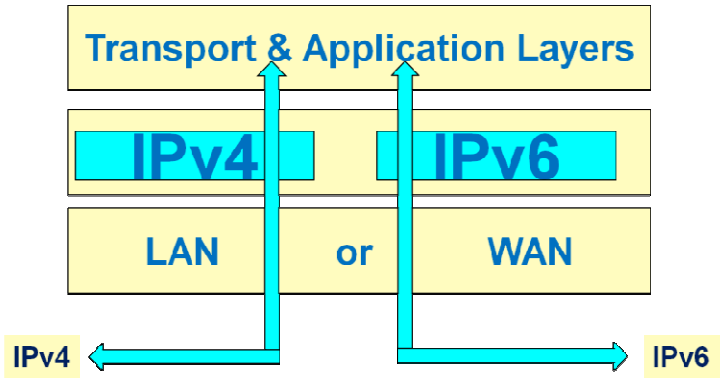
### a. Header Translation




[6] https://www.arin.net/knowledge/about_resources/ceo_letter.pdf

Header translation can be used when sending IPv6 traffic to an IPv4 network as the end destination. This transition strategy is not likely to become a preferred transition method, because the advantages of both protocols can be lost.

**b. Dual Stack**




Dual stack can be used when a network handles both kinds of traffic. Although dual stack is the transition method most likely to be widely deployed, it essentially doubles the network security problem.[5] On June 8, 2011 a "World IPv6 Day" will be conducted for 24 hours to test major organizations' capability to operate successfully using dual stack methodology.[7] Dual stack is expected to be the preferred method of transitioning to IPv6.

**c. Tunneling**


Tunneling is the most precarious method for today's IPv4 networks. The IPv6 packet is tunneled inside the message field of an IPv4 packet. The contents of the IPv6 packet will not be noticed by an IPv4 firewall or intrusion detection system. Cyber terrorists can use this vulnerability to deliver malware, penetrate databases, plant bots, etc.

## 3. WHY CAN IPV6 BE DANGEROUS?

Tunneling of IPv6 inside an IPv4 packet will be invisible to an organization using only IPv4. Hidden IPv6 traffic running across an organization's network can wreak havoc, allow malware to enter the network, and be the basis for a denial of service attack.

[7] http://isoc.org/wp/worldipv6day/

## 4. WHAT ACTIONS CAN BE TAKEN TO REDUCE THE THREAT OF INVISIBLE IPV6 TRAFFIC?

### a. Upgrade Today to IPv6

This is a costly, but effective solution, but the best of the choices. Very few organizations, however, have chosen this path because of the financial implications of upgrading their entire network in a short period of time.

### b. Block all IPv6 Traffic

This solution is only temporary and difficult to administer. Furthermore, it is ineffective against tunneled IPv6 traffic, unless a technique known as Deep Packet Inspection (DPI) is employed. We shall address DPI shortly.

## 5. DEEP PACKET INSPECTION – FRIEND OR FOE?

Internet communications employ packets with headers containing routing information, including source and destination addresses. Historically, only the header was examined by network routers. This is inadequate for the detection of tunneled IPv6 inside an IPv4 packet. Since we are in a world dominated by IPv4, the only way to detect tunneled IPv6 is to use Deep Packet Inspection.

Deep Packet Inspection (DPI) is the act of any packet network equipment which is not an endpoint of a communication using non-header content (typically the actual payload) for some purpose. This is performed as the packet passes an inspection point, searching for protocol non-compliance, viruses, spam, intrusions or predefined criteria to decide what actions to take on the packet, including collecting statistical information. This is in contrast to shallow packet inspection (usually called Stateful Packet Inspection) which just checks the header portion of a packet).[8]

Deep Packet Inspection operates at all layers of a network above the physical layer. Each packet is examined for the information in the entire packet, not just the headers. DPI places a processing burden on the device performing this task, and can be a source of latency in a network. In an ideal world, processing speed requirements of DPI would be met by increases in device technology in accordance with Moore's Law. The current situation is that delays in networks are mostly caused by processing delays.

DPI can also be used for commercial gain by classifying Internet traffic by type, with charging policies flowing there from. This would seem to violate the concept of Internet neutrality, but it is a direction that various ISPs have been favoring and lobbying to achieve.

The widespread use of DPI is inevitable. The first serious security breach caused by tunneled IPv6 inside an IPv4 packet is certain to come in the near future. This event will be a stimulus to organizations to defend against such attacks. It has already been a major source of attacks against the US Government.

[8] http://www.symantec.com/connect/articles/perils-deep-packet-inspection

## 6. LEGAL, SOCIAL, AND SECURITY IMPLICATIONS

It is inevitable that DPI will be widely employed out of necessity since organizations cannot switch overnight to IPv6. Another aspect is that DPI is a rich source of information for intelligence agencies and government surveillance. DPI is opposed by advocates of network neutrality and the ACLU.[9, 10]

## 7. ENCRYPTION AND IPV6

An issue that must be resolved by a security policy for an organization is encryption. Headers are never encrypted since they need to be read for routing purposes. Messages, however, can be encrypted. The reason that the United Arab Emirates and Saudi Arabia recently banned Blackberry was because Blackberry uses encryption and message content cannot be monitored. Government surveillance is not possible with encrypted traffic. RIM capitulated under pressure by the Saudis and agreed to place a server in Saudi Arabia, thereby providing the means for government surveillance of Blackberry traffic.[11] Skype also uses encryption; do not look for widespread acceptance of Skype in countries using total surveillance of citizens' electronic communications.

The access control policies for an organization should be determined by the message content that is found by DPI. Presumably, unencrypted messages of tunneled IPv6 inside an IPv4 would be easy to decide whether to forward to the addressee. If the message is encrypted, a policy must be established. The simplest solution is to block all tunneled traffic that has the message encrypted. This policy may have secondary negative effects on an organization's ability to communicate. If the encrypted message is allowed to enter the enterprise, a greater risk in taken, since inside the organization is an individual who may be trying to avoid the internal security policies.

## 8. OBSERVATIONS AND RECOMMENDATIONS

The transition period between IPv4 and IPv6 is full of future unknowns. Unanticipated security vulnerabilities are certain. Legal issues on the rights to privacy, surveillance, and Internet neutrality will all come into play. It will be an interesting next stage in the growth of the Internet. The threats caused by the advent of IPv6 must not be ignored by an organization. It is imperative to begin guarding against a major catastrophe caused by inattention to the forthcoming world of IPv6.

[9] http://www.aclu.org/technology-and-liberty/aclu-warns-against-intrusive-deep-packet-inspection
[10] http://www.aclu.org/net-neutrality
[11] http://www.msnbc.msn.com/id/38594687/ns/technology_and_science-tech_and_gadgets/

## 9. REFERENCES


1. http://www.icann.org/en/news/releases/release-03feb11-en.pdf
2. S. Bradner and A. Mankin, "The Recommendation for the Next Generation IP Protocol", RFC 1752, Jan. 1995
3. https://www.arin.net/knowledge/about_resources/ceo_letter.pdf
4. Bihrouzan A. Forouzan, "TCP/IP Protocol Suite", 4th Edition, McGraw Hill, ISBN: 978-0-07-337604-2, 2010
5. C. Caicedo, J. Joshi, and S. Tuladhar, "IPv6 Security Challenges", Computer, IEEE Computer Society, February 2009
6. https://www.arin.net/knowledge/about_resources/ceo_letter.pdf
7. http://isoc.org/wp/worldipv6day
8. http://www.symantec.com/connect/articles/perils-deep-packet-inspection
9. http://www.aclu.org/technology-and-liberty/aclu-warns-against-intrusive-deep-packet-inspection
10. http://www.aclu.org/net-neutrality
11. http://www.msnbc.msn.com/id/38594687/ns/technology_and_science-tech_and_gadgets/