A review of IPv6 security concerns

R.P. van Heerden[1], I.M. Bester[2], I.D. Burke[1]

[1]DPSS,CSIR
Pretoria, South Africa
E-mail: rvheerden@csir.co.za
E-mail: iburke@csir.co.za

[2]Computer Engineering,
University of Pretoria, Pretoria, South Africa
E-mail: naas.bester@gmail.com

Abstract:

This study focus on the security concerns of IPv6. A broad introduction to IPv6 is made then briefly the differences between the IPv6 and IPv4 protocols are looked at, their known vulnerabilities and this identifies some security concerns when implementing IPv6. Even after 13 years, IPv6is still considered a new network protocol. With this in mind not much is known about IPv6. Since the IPv4 address space will be used upwithin the next few months, IPv6 should finally become more mainstream.

Keywords: ipv6, security, Internet protocols, Internet security

Introduction

Darrin Miller, Security Researcher, CIAG, Cisco System stated: "IPv6 makes some things better, other things worse, and most things are just different, but no more or less secure"(Deering & Hinden, Internet Protocol Version 6 (IPv6) Specification, 1995).The Internet Engineering Task Force (IETF)proposed a new internet protocol in 1990s(Deering & Hinden, Internet Protocol Version 6 (IPv6) Specification, 1998).Internet Protocol Next Generation (IPng)wascreated, which then became Internet Protocol version 6 (IPv6)and is the successor to IPv4. Its development is ongoing for more than 13 years and this protocol is still described as the new generation protocol since most of its implementation is still in engineering laboratories and by academia. Less than approximately 1% of all internet traffic is IPv6 based. The migration to IPv6 is happening at a very slow pace.

The Internet Protocol

TheOpen Systems Interconnection Model (OSI)is a way of sub-dividing a communications system into smaller parts called layers. Similar communication functions are grouped into logical layers. A layer provides services to its upper layer while receiving services from the layer below. On each layer, an instance provides service to the instances at the layer above and requests service from the layer below.

Figure 1 shows the 7 OSI layers and accompanying protocols.Internet Protocol (IP) forms part of the third layer, the Network Layer.

What is Internet Protocol?

A protocol (in the context of a computer network) is a set of rules governing the exchange or transmission of data electronically between devices. IPis the principal communications protocol used for relaying data packets across anetwork. It is responsible for routing packets across network boundaries. It is the primary protocol that establishes the Internet.

IPv4 is currently the dominant protocol of the Internet, but is envisioned to be succeeded by IPv6.

Why was IPv6 Developed?

IPv6 was developed because IPv4 does not have enough addresses available to sustain the ever growing internet and all the devices that needanunique IP address to connect to it. IPv4 has a theoretical upper limit of about 4 billion (4,000,000,000) unique addresses but in practice IPv4 is unlikely to support a sustainable population of no more than about 250 million uniquely addressed nodes (Loshin, Protocol, and Practice, 2004)..

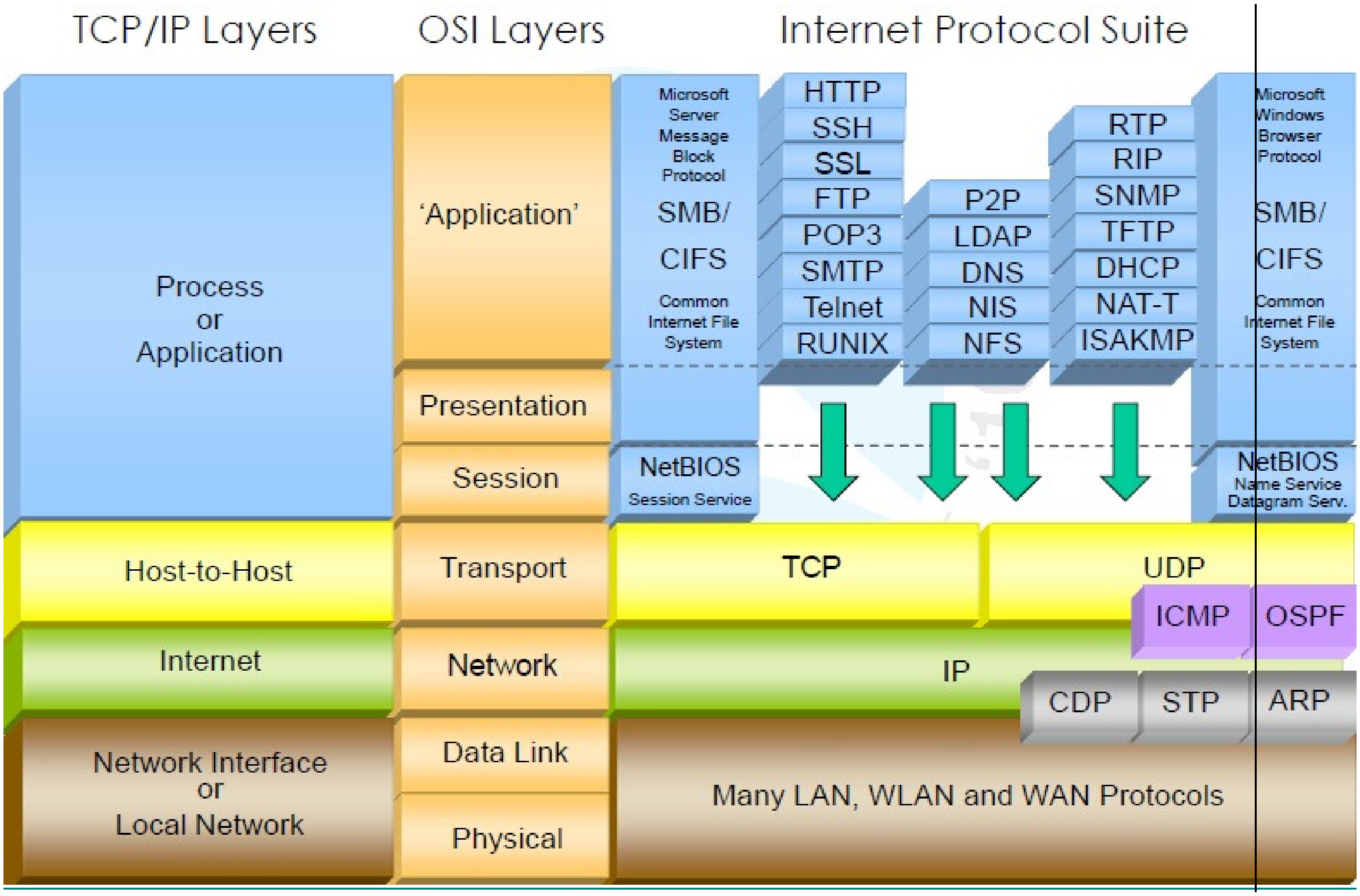


Figure 1 - Open Systems Interconnection model (OSI model)(Leutert, 2010)

What about Network Address Translation?

Network Address Translation was developed to alleviate the effects of IPv4 address depletion.Network Address Translation(NAT) basically translates one or more addresses into another, typically a private address into a public address and vice-versa. Many users and sites do this today on a small scale. An end-user laptop may have a private address which is translated by the home router into a public address provided by theInternet Service Provider (ISP). The public address is unique and this is the address depended on for global Internet connectivity. So what happens when the ISP runs out of addresses? Before address exhaustion, it would simply apply for and receive new addresses (Lee, 2011).

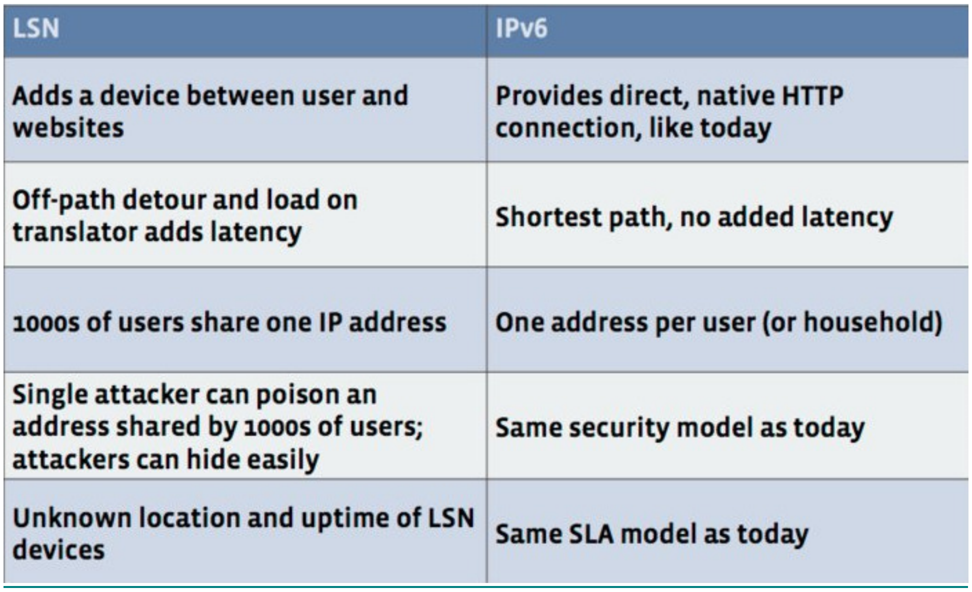
The Internet Assigned Numbers Authority(IANA) will assign the last of the available IPv4 addresses during 2012 after which there are no more new IPv4 addresses available (Marsan, Network World, No more IPv4 addresses, 2011).

Large Scale NAT

This is basically address translation upon address translation, also called Carrier Grade NAT. Intermediate endpoints like home routerswillalso get a private address instead of a public one and then translate its traffic at a new heavy-duty Large Scale Network Address Translation(LSN) device that lives elsewhere on the Internet. Thousands of users will share a single IP address through this massive translator. What is unclear is whether this will provide the same performance, reliability, and security currently on the Internet (Lee, 2011).

LSN compared to IPv6 as a solution

IPv6 has been years in development and is considered a longer-term and more reliable solution than LSN. Adopting IPv6 means that people with IPv6 addresses can talk to IPv6-enabled or dual-stack sites without LSN translators. Figure 2describes some other aspects of LSN compared to end-to-end IPv6 connectivity (Lee, 2011).



LSN	IPv6
Adds a device between user and websites	Provides direct, native HTTP connection, like today
Off-path detour and load on translator adds latency	Shortest path, no added latency
1000s of users share one IP address	One address per user (or household)
Single attacker can poison an address shared by 1000s of users; attackers can hide easily	Same security model as today
Unknown location and uptime of LSN devices	Same SLA model as today

Figure 2 Large scale NAT vs. End-to-End IPv6

IPv6 represents the last and best hope for continued, unencumbered Internet growth. Not going this route will lead to islands of IPv4 "NAT'ed" or similar networks with various toll gates and bridges that offer a small aperture to the rest of the world(Marsan, Network World, What if IPv6 simply fails to catch on?, 2011).

Why is the migration happening so slowly?

The major stumbling block to the deployment of IPv6 is that it is not backwards compatible. That means network and website operators have to upgrade their network equipment and software to support IPv6 traffic, and so far most have been unwilling to do so (Marsan, What if IPv6 simply fails to catch on?, 2011).

There exists a Catch-22of supply and demand for IPv6 content/traffic.Network equipment vendors don't put their weight behind producing affordable large range IPv6 compatible equipment, because enterprises would not buy it. Web based enterprises donot upgrade their equipment to IPv6 compatibledevicesbecause no or little endpoint users will be able to use it. Most equipment in homes today will not support IPv6. Then it goes back, most endpoint users would nott buy expensive equipment that support IPv6 if their ISP does not and if most of the internet websites are still hosted through IPv4 technology. Security is a concern but it is not the driving force behind the slow migration.There is no definite start or end date for the migration and it is predicted that it will still go on for years.

Header Structures

The common way to represent these headers is to draw them as a succession of 32-bit words. The top word is transmitted first and the left most byte of each word is transmitted first (Peterson & Davie, 2000).

2.5.1 IPv4 Header

IPv4 provides 32-bit address space and has a theoretical upper limit of about 4 billion (4,000,000,000) unique addresses but in practice IPv4 is unlikely to support a sustainable population of no more than about 250 million uniquely addressed nodes. The IPv4 header structure is described below and shown in Figure 3.

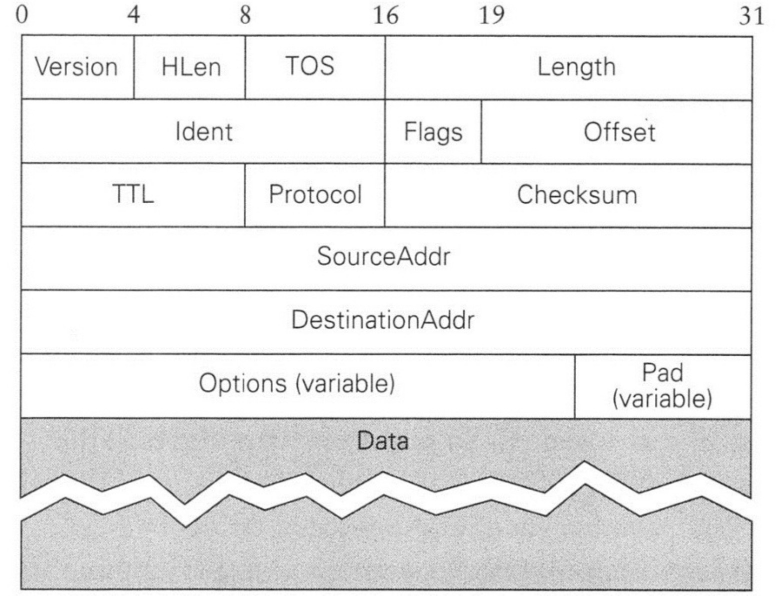


Figure 3

- **Version**: The Version field specifies the current version which is 4 in this case. The header processing software checks this first and then knows how to process the rest.
- **HLen**: The HLeng specifies the number of 32-bit words in the header. Minimum is 5 where 5×32=160 bits or 20bytes. The maximum is 15 where 15×32=480 bits or 60 bytes.
- **TOS**: Differentiated Services Code Point formerly known as TOS (Type of service) is used to indicate if a packet should receive some sort of special or priority processing.
- **Length**: This is a 16-bit field defining the total length of the datagram (header and data). The minimum is 20bytes and the maximum is 65,535 bytes.
- **Ident**: The Ident is used for identifying fragments of the original datagram.
- **Flags**: The Flags is a 3-bit field used to control and count fragments of the datagram.
- **Offset**: The Offset is a 13-bit field that specifies the offset of a particular fragment relative to the beginning of the original unfragmenteddatagram. The first fragment has an offset of zero.
- **TTL**: The TTL (Time to Live) reflects historical intention where the time the packet was allowed to exist on the network was considered but it has become more of a hop count than a timer.
- **Protocol**: The Protocol field is a key that identifies to which of the OSI higher-level protocol the IP packet should be passed to. Examples are TCP and UDP.
- **Checksum**: The checksum field is the 16-bit one's complement of the one's complement sum of all 16-bit words in the header.It is used for error checking the header. If an error is detected the packet is discarded and must be resend.
- **SourceAddr**: The SourceAddr (Source Address) is the IPv4 address of the sender. It is included so that the recipient can decide if it wants to receive data from this sender and also to know where to reply to if it wants to reply. Note that during transit a NAT device could change this address.
- **DestinationAddr**: The DestinationAddr (Destination Address) is the IPv4 address indicating the receiver of this packet. Note that during transit a NAT device could change this address.

- **Options** and **Pad** (variable): There may be a number of options at the end of the header but these are not used often.

IPv6 Header

Migration to IPv6 support is a gradual process, and mechanisms to gracefully support IPv6 in IPv4 networks have been an important part of the IPv6 development project from the start.IPv6 provides a 128-bit address space and can address 3.4×1038 nodes.

The IPv6 header structure is described below and shown in Figure 4.

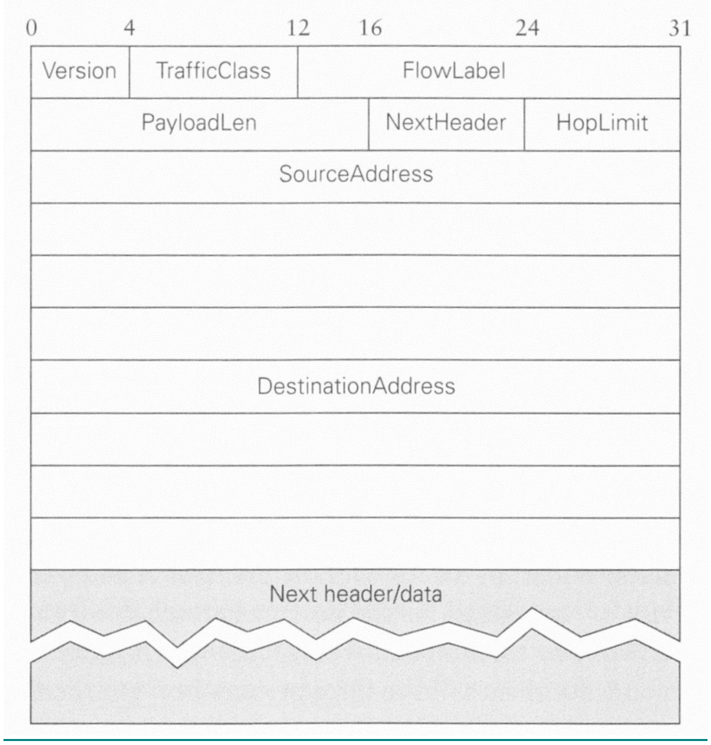


Figure 4

- **Version**: The Version field is set to 6 for IPv6.
- **TrafficClass**: The TrafficClass field identifies the priority and class of service of this packet.
- **FlowLabel**: The FlowLabel field is for future use in identifying packets that are part of a unique flow, stream, or connection
- **PayloadLen**: The PayLoadLen field defines the length in octets of the packet that follows the IPv6 header.
- **NextHeader**: The NextHeader field identifies the type of header that follows the IPv6 header. This replaces the Options and Protocol field of IPv4.
- **HopLimit**: The HopLimit field is a counter for the number of remaining hops the packet can traverse. This is simply the TTL of IPv4 renamed.
- **SourceAddress**: The IPv6 address of the node that originated this packet.
- **DestinationAddress**: The IPv6 address that this packet is destined for.

IP Security

The following was identified as prominent problems with IPv4 for which IPv6 are the solution(Loshin, Protocol, and Practice, 2004).

- The imminent exhaustion of the IPv4 addressing space.
- The imminent collapse of the Internet routing structure due to explosive growth of the non-default routing table.
- The problem of end-to-end interoperability across routing domains in which IP addresses may not be globally unique.

The way in which IPv6 is capable of solving these problems becomes clearer when keeping in mind their different header compositions as described in the previous sections(Peterson & Davie, 2000).

The migration from IPv4 to IPv6 has no determined end date. The process is slow. Table 1 lists some important documents for migrating to IPv6.

Table 1: IPv6 Documents

RFC#	**Title**
2071	Network Renumbering Overview- Why would I want it and what is it anyway?
2072	Router Renumbering Guide
2185	Routing Aspects of IPv6 Transition
2529	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels
2767	Dual Stack Hosts Using the Bump-in-the-Stack Technique (BIS)
2893	Transition Mechanisms for IPv6 Hosts and Routers
3056	Connection of IPv6 Domains via IPv4 Clouds
3142	An IPv6-to-IPv4 Transport Relay Translator

Three transition techniques were developed by the IETF:

- Dual-stack: The nodes have two protocol stacks (IPv4 and IPv6) enabled and use IPv6 to contact IPv6 nodes and use IPv4 to contact IPv4 nodes.
- Tunnels: Hosts or routers send and receive IPv6 packets using an overlay network of tunnels established over an IPv4 network or over label switched path (LSP) (in a Multiprotocol Label Switching [MPLS] network).
- Protocol translation: A protocol translator acts as an intermediary between the IPv4 and IPv6 worlds.

A list of vulnerabilities of running dual-stack:

- Protected against IPv4 attacks but not IPv6 attacks. A lot of users are not aware that their operating system is running both version of the protocol automatically.
- Denial of Service attacks

A list of vulnerabilities of running tunneling:

- Address spoofing
- Reflection attack

IPv6 and IPv4 both fall within the Network Layer of the OSI stack. If for example a network layer application is vulnerable in IPv4, it will also be vulnerable in IPv6.

A list of similar vulnerabilities:

- Attacks against the physical, data link or application layers
- Man-in-the-middle attacks
- Sniffing/eavesdropping
- Denial of Service (DoS) attacks
- Spoofed packets: forged addresses and other fields
- Attacks against routers and other networking devices

The way in which IPv6, as part of the network layer of the OSI stack, interacts with the layers above and below it can also introduce new vulnerabilities.

A list of vulnerabilities where the difference is only slightly:

- LAN-based attacks through the Address Resolution Protocol (ARP)or Neighbor Discovery Protocol (NDP)
- Attacks against Dynamic Host Configuration Protocol(DHCP)or DHCPv6
- Denial of Service (DoS) against routers (hop-by-hop extension headers rather than router alerts)
- Fragmentation (IPv4 routers performing fragmentation versus IPv6 hosts using a fragment extension header)
- Packet amplification attacks (IPv4 uses broadcast versus IPv6 uses multicast)

A list of vulnerabilities where the difference is unique to IPv6:

- Reconnaissance(since brute force with the larger address space is more time consuming) and scanning worms
- Attacks against the required componentInternet Control Message Protocol for IPv6(ICMPv6)
- Extension Header (EH) attacks
- NDP attacks (Auto configuration) are simple to perform
- Attacks on dual stack implementation migrating from IPv4 to IPv6.
- Mobile IPv6 attacks. Devices that roam are susceptible to much vulnerability.
- IPv6 protocol stack attacks because bugs and shortcomings might exist in the code.

IPv6 SECURITY CONCERNS

The following section categorizes security concerns regarding IPv6 implementation(Hogg, 2008)(KIM & KIM)(Zagar & Grgic, IPv6 Security Threats and Possible Solutions)(Zagar & Vidakovi, IPv6 Security: Improvements and Implementation Aspects)(Ford)(Choudhary & Sekelsky)(Szigeti & Risztics)(Zimmermann, 1980).It is discussed like a ripple effect starting at the protocol itself and rippling outwards through the network along the path of communication. Implementation of Current Best Practice(CBP) is strongly advised when planning or working onthese different parts of the IPv6 network. It is also encouraged to research the specific area of implementation in the context of the intended network. Hence, the description given is 'current best practice' because it is still changing.

Protocol Security

This concern involves the protocol itself, its structure and how it works. The implementation of ICMPv6 and Extension Headers are especially important. IPsec is mandatory in IPv6 and its implementation is very important. Its presence is carried over to some of the other sections as well.

Operating System Security

This concern is with the IPv6 security capabilities and setup of operating systems running on the different client and server machines composing the intranet. These machines hold the most valued information and the operating system is the connectionbetween the information and the rest of the network.

Network Security

This concern is with the organizations intranet or network inside the perimeter mostly regarding the Data Link Layer of the OSI[12]. The CSI/FBI 2007 Computer Crime and Security Survey reported that 64 percent of the surveyed organization's losses were partially or fully a result of insiders. The implementation of Neighbor Discovery Protocol(NDP) and DHCPv6 are especially important.

Perimeter Security

This concern is based on the old military strategy where the city borderis fiercely protected leaving the inside saved. It involves the perimeter around an organizations network where it connects with the internet or other organization networks. The implementation of IPv6 firewalls is especially important. New proposed security models might incorporate firewalls into an Intruder Detection System (IDS).

Internet Security

This concern is with the cloud. It involves the internet, traffic and equipment like routers. These threads could come from anywhere across the web, even form distributed threats working together. Configuration of routers is especially important.

Virtual Private Network Security

This concern is withVirtual Private Network(VPN) setup over IPv6 also known as ‘tunneling’; a secure private connection through a public network or an otherwise unsecure environment. The implementation of IPsec is especially important.

Mobile Security

This concern is with mobile devices like laptops and smart phones where the need to roam around while staying connected is growing fast. Here again the implementation of IPsec is especially important. Take note of the new Mobile Internet Protocol(MIP)implementation.

Conscientious Security

This concern is with the users and more importantly the administrators of the system. Their skills, discipline and awareness might be the last defense in a possible security disaster. Cultivation of such skills and users are encouraged.

World IPv6 Day

On 8 June, 2011, under the sponsorship of the Internet Society, top websites and ISP's around the world, including Google, Facebook, Yahoo!, Akamai and Limelight Networks joined together with more than a 1000 other participating websites in World IPv6 Day. This entailed a 24-hour global-scale'test flight' ofthe new Internet Protocol, IPv6(Internet Sociaty, About World IPv6 Day, 2011).

During this trial all the participating web sites served up their content using IPv6 as well as the current standard IPv4. The event was hailed a massive success, raised visibility of IPv6 and allowed network engineers to determine how well IPv6 works and to pinpoint technical difficulties such as misconfigured systems and delays for some end users trying to access participating Web sites (Marsan, Network World, Large-scale IPv6 trial set for June 8, 2011).

Data traffic statistics

For a bright 24 hour period, shown inFigure 5, the IPv6 network looked a little bit more like its IPv4 big brother. Web traffic grew during the day up until the midnight cutoff point where some of the major content providers withdrew their namespace support. At midnight UTC the web traffic falls off the cliff and the traffic mix returns to its pre-v6-day chatter (Malan, 2011).

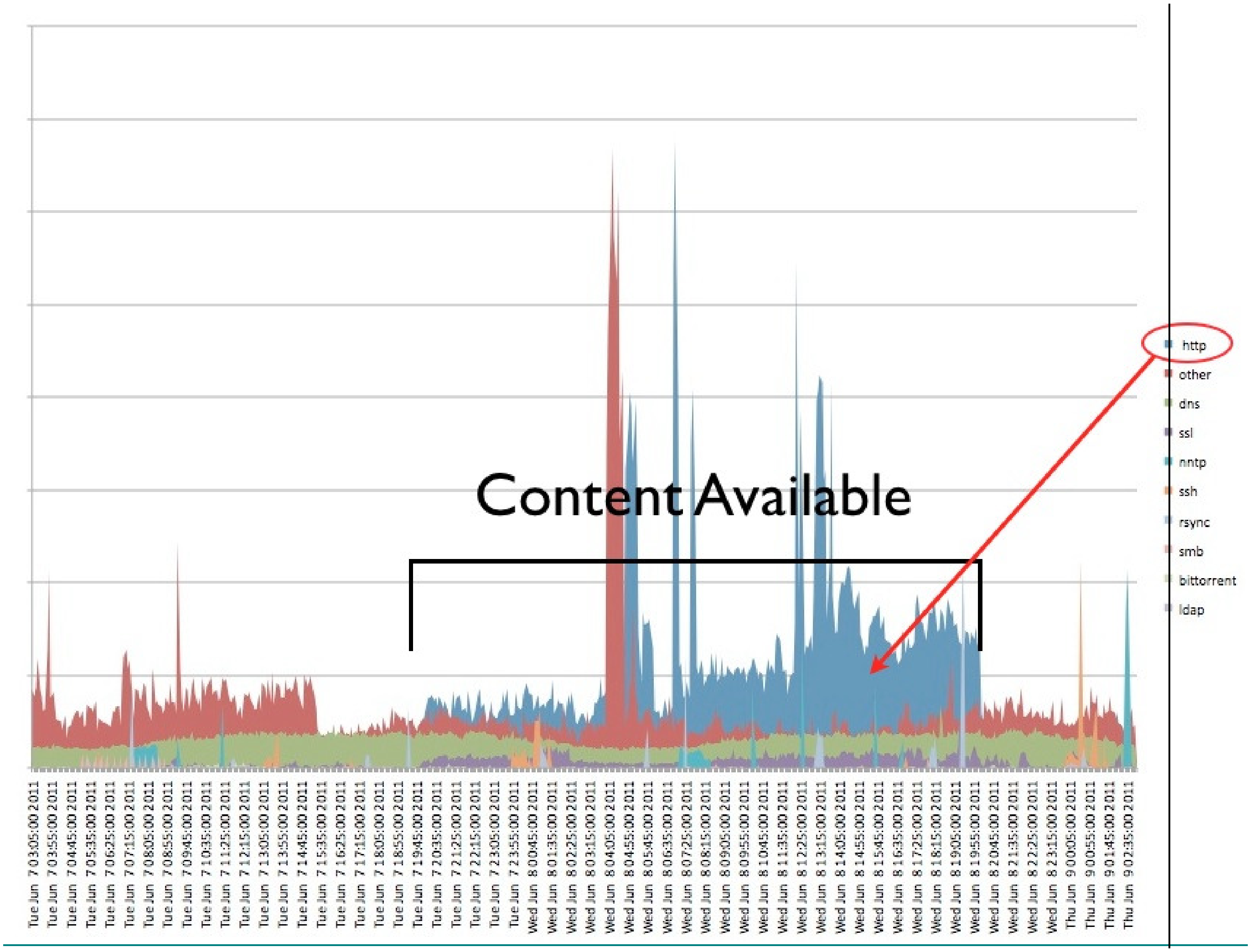


Figure 5Application breakdown for native IPv6 traffic from six carriers(Malan, 2011)

In Figure 6Percentage of IPv6 traffic of all Internet traffic in six carriers~~Figure 6 Percentage of IPv6 traffic of all Internet traffic in six carriers~~roughly doubled during the v6-day period. However, doubling a fraction of a percent is still a fraction of a percent. Most end users probably have at least a mediating Domain Name System(DNS)caching device (home router or wireless base station) that may not elegantly switch back and forth from v4 to v6. The inertia and complexity of changing this element of the Internet is massive (Malan, 2011).

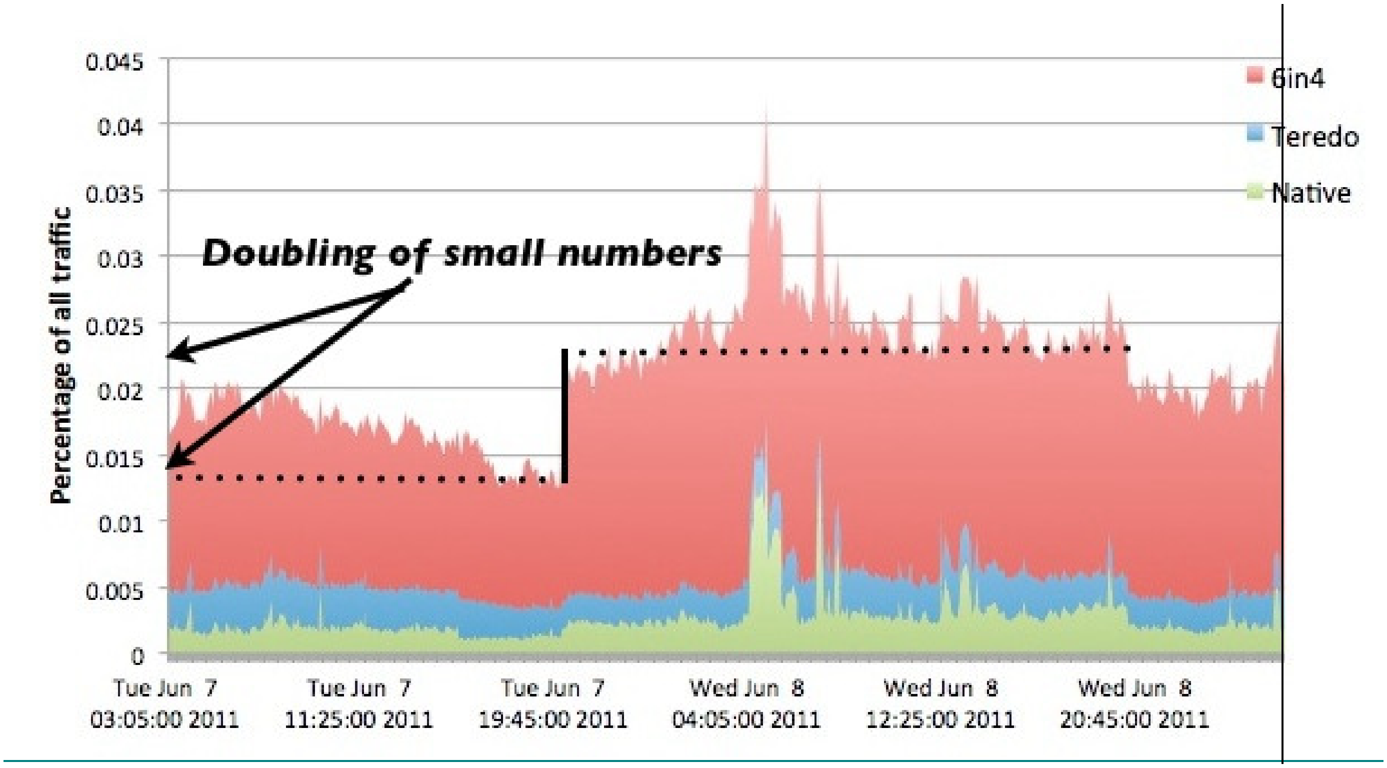
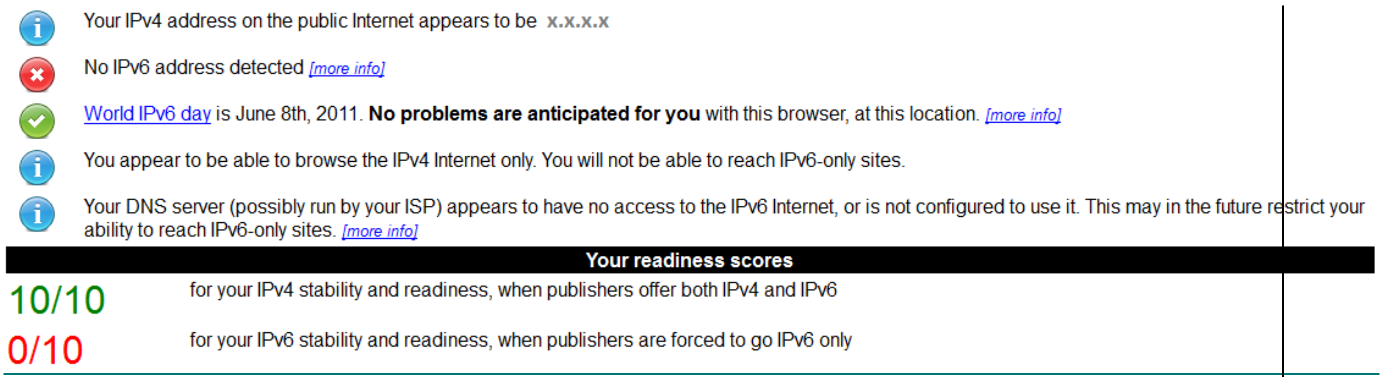


Figure 6Percentage of IPv6 traffic of all Internet traffic in six carriers(Malan, 2011)

Test your IPv6 Connectivity

The Internet Society made a test site (http://test-ipv6.com/) available for end users to test their IPv6 compatibility(Internet Sociaty, Test your IPv6 connectivity, 2011). Figure 7 shows the results of my local machine connected via a Wi-Fi router to an ADSL line.



ℹ Your IPv4 address on the public Internet appears to be x.x.x.x

✖ No IPv6 address detected [more info]

✓ World IPv6 day is June 8th, 2011. **No problems are anticipated for you** with this browser, at this location. [more info]

ℹ You appear to be able to browse the IPv4 Internet only. You will not be able to reach IPv6-only sites.

ℹ Your DNS server (possibly run by your ISP) appears to have no access to the IPv6 Internet, or is not configured to use it. This may in the future restrict your ability to reach IPv6-only sites. [more info]

Your readiness scores

10/10	for your IPv4 stability and readiness, when publishers offer both IPv4 and IPv6
0/10	for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Figure 7 Local Machine Test Results

Google after IPv6 Day

Google said it has decided to leave its main YouTube website enabled for IPv6 for the time being. Since 2008, Google has supported IPv6 on separate websites -- such as www.ipv6.google.com -- rather than on its main websites. Lorenzo Colitti, IPv6 Software Engineer at Google stated that “We saw 65% growth in our IPv6 traffic on World IPv6 Day"

(Marsan, Network World, Google, Facebook promise new IPv6 services after successful trial , 2011)

Google over IPv6 uses the IPv4 address of your DNS resolver to determine whether a network is IPv6-capable. If you enable Google over IPv6 for your resolver, IPv6 users of that resolver will receive AAAA records for IPv6-enabled Google services.Normally, if a DNS resolver requests an IPv6 address for a -Google web site, it will not receive one but a DNS resolver with Google over IPv6 will receive an IPv6 address,and its users will be able to connect to Google web sites using IPv6 as shown in Figure 8(Google, Google over IPv6, 2008).

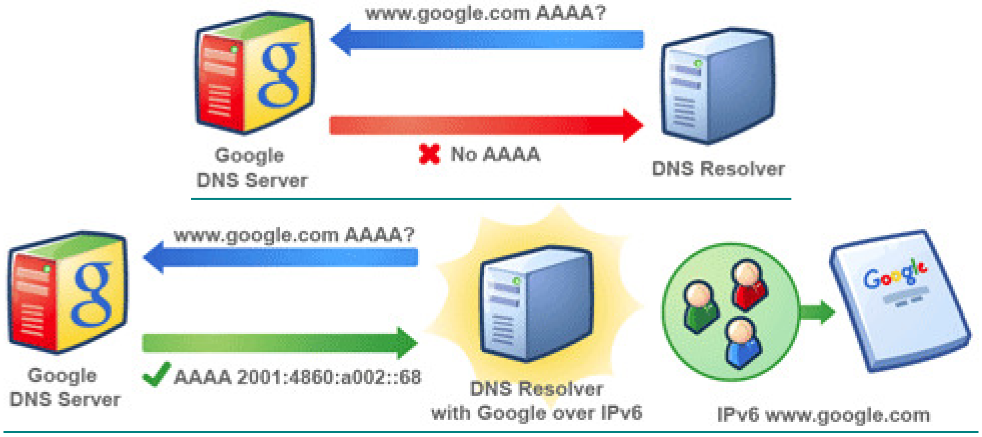


Figure 8: Google over IPv6

Facebook after IPv6 Day

Don Lee, senior network engineer at Facebook.stated: "At Facebook, we saw over 1 million of our users reach us over IPv6 ... There were no technical glitches in this 24-hour period. We were encouraged by the many positive comments on our blog. ... It is really interesting to see how passionate people were about IPv6 around the world."(Marsan, Network World, Google, Facebook promise new IPv6 services after successful trial , 2011). Because of the positive results from World IPv6 Day, Facebook has decided to support IPv6 on its Website for developers, which is developers.facebook.com.

Security on IPv6 Day

The general conclusion of the 24-hour trail is that security stayed intact. It is also generally known that this is too short a time to form any conclusive opinions regarding the matter. Some security feedback after IPv6 day follows.

“Latest reports state that the 24-hour global test run did not hit any major glitches, according to a spokesman for Arbor Networks, an Internet security company monitoring the IPv6 activity”(Moyo, 2011)."The Internet is under constant attack, and a lot of it is insignificant," Champagne says. "We did see some DoS attacks that were going on over IPv4, and when folks switched to IPv6, the attacks switched to IPv6. But it still wasn't material. We haven't seen any massive attacks."As this large-scale experiment draws to a close, no major outages or security breaches were reported at the 400-plus corporate, government and university websites participating in the IPv6 trial.Champagne says Akamai has not seen more broken IPv6 connections than expected, nor has it noticed any major attacks aimed at IPv6 (Marsan, Network World, No news is good news on World IPv6 Day, 2011).

Some people had predicted that hackers were going to take advantage of World IPv6 Day. The thought was that if these large sites, which had historically been IPv4, were to become IPv6 accessible they would be vulnerable. Many organizations may have significantly sophisticated IPv4 defenses but their IPv6 defensive capabilities may not be sufficient. The attackers could perform reconnaissance on the public IPv6 addresses of these sites and see if they are more vulnerable with IPv6 than with IPv4. The SANS Internet Storm Center (ISC) and the Cisco Security Intelligence Operations (SIO) didnot report any security issues related to IPv6. However, that doesnot mean that attackers were not performing some reconnaissance and data gathering (Hogg, 2008).

CONCLUSION

Since so little IPv6 implementation is currently out there it is difficult to see the results of this new and complex protocol. Advising people to be aware of the security holes and implement current best practice is the only way to progress with the migration.

The Arab Spring was driven by the Internet and social media using mobile devices in the GSM/Internet Protocol. Cellular phones running Google,Android,Blackberry OS, Apple OS, and iPhone formed the base on which the social media network was used. Thus IPv6 migration may be pushed more by the migration to mobile devices than the use of traditional networks. The number of mobile devices that use GSM and Wifi could speed up the IPv6 migration.

The Internet Society also provides a list of frequently asked questions about IPv6 adoption.
They state that there have been several calls to action for organisations to plan actively for the widespread deployment of the new version of the basic Internet Protocol, IPv6. They intenselysupport such calls for action.The Internet Society also states:
"If deployment is delayed, the future growth and global connectivity of the Internet will be negatively impacted."(Internet Society, 2012).

References

Choudhary, A. and Sekelsky, A. (2010) Securing IPv6 network infrastructure: A new security model. *Technologies for Homeland Security (HST), 2010 IEEE Conference*, 500-506.

Deering, S. and Hinden, R. (1995) Internet Protocol Version 6 (IPv6), RFC 1883, URL: http://www.ietf.org/rfc/rfc1883.txt [Accessed: 15th November, 2011].

Deering, S. and Hinden, R. (1998) Internet Protocol Version 6 (IPv6), RFC 2460, URL: http://www.ietf.org/rfc/rfc2460.txt [Accessed: 15th November, 2011].

Ford, M. (2005) New Internet Security and Privacy Models Enabled by IPv6. *Applications and the Internet Workshops, 2005. Saint Workshops 200*5, 2-5.

Google (2008) Google over IPv6, URL: http://www.google.com/intl/en/ipv6/ [Accessed: 19th November, 2011].

Hogg, S. (2008) *IPv6 Security*, Indianapolis, Cisco Press.

Internet Society. (2011) 2011 World IPv6 Dat, URL: http://www.worldipv6day.org/ [Accessed: 19th November, 2011].

Internet Society. (2011) Test yout IPv6 connectivity, URL: http://test-ipv6.com/ [Accessed: 22th March, 2012].

Internet Society. (2012) Frequently Asked Questions on IPv6 adaoption and IPv4 exhaustion, URL: http://www.isoc.org/internet/issues/ipv6_faq.shtml [Accessed: 9th September, 2012].

Kim, Y.W, and Kim, H.J. (2005) Ipv6: No More Next Generation. *In the 7th International Conference on Advance Communication Technology (ICACT)*, 8-11.

Lee, D. (2011) World IPv6 Day: Solving the IP Address Chicken-and-Egg Challenge, URL: http://www.facebook.com/notes/facebook-engineering/world-ipv6-day-solving-the-ip-address-chicken-and-egg-challenge/484445583919 [Accessed: 5th March, 2012].

Leutert, R. (2010) Discovering IPv6 with Wireshark. *SHARKFEST'10*.

Loshin, P. (2004) *IPv6 Theory, Protocol and Practice*, San Francisco, Morgan Kaufmann.

Malan, R. (2011) World IPv6 Day: Final Look and "Wagon's Ho!", URL: http://asert.arbornetworks.com/2011/06/world-ipv6-day-final-look-and-wagons-ho/ [Accessed: 22th September, 2012].

Marsan, C.D. (2011) No news is good news on World IPv6 Day, URL: http://www.networkworld.com/news/2011/060811-ipv6-day-wrapup.html?nwwpkg=ipv6&ap1=rcb [Accessed: 22th September, 2012].

Marsan, C.D. (2011) Google, Facebook promise new IPv6 services after successful trail, URL:http://www.networkworld.com/news/2011/060911-world-ipv6-follow.html [Accessed: 22th September, 2012].

Marsan, C.D. (2011) No more IPv4 addresses, URL:http://www.networkworld.com/news/2011/020111-ipv4-apnic.html [Accessed: 22th September, 2012].

Marsan, C.D. (2011) What if IPv6 simple fails to catch on?, URL:http://www.networkworld.com/news/2011/052311-ipv6-fail.html?page=1 [Accessed: 22th September, 2012].

Marsan, C.D. (2011) Large-scale IPv6 trail set for 8 June, URL:http://www.networkworld.com/news/2011/060311-ipv6-day.html [Accessed: 14th July, 2012].

Moyo, A. (2011) Trouble-free world IPv6 day, URL: http://www.itweb.co.za/index.php?option=com_content&view=article&id=44423%3Atroublefree-world-ipv6-day&catid=100&Itemid=219 [Accessed: 14th July, 2012].

Peterson, L. and Davie, B. (2000) *Computer Networks A Systems Approach*, London, Academic Press.

Shankland, S. (2012) DDoS attacks spread to vulnerable IPv6 Internet, URL: http://news.cnet.com/8301-30685_3-57378307-264/ddos-attacks-spread-to-vulnerable-ipv6-internet/[Accessed: 16th October, 2012].

Zagar, D. and Grgic, K. (2006) Ipv6 Security Threats and Possible Solutions. *Automation Congress, 2006. WAC '06 World*, 1-7.

Zagar, D. and Vidakovic, S. (2005) IPv6 security: improvements and implementation aspects. *Telecommunications, 2005. ConTEL 2005*, 1:29-34.

Zimmermann, H. (1980) OSI Reference Model. *IEEE Transactions on Communications*, 28(4).