Owk Kiran Kumar, Yarlagadda Jayachandra Chowdary, Posani Viswa Teja, Thumalakunta Praveen Blessington, Thumati Ravi / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 6, November- December 2012, pp.1489-1494

IPv6 – the next generation Internet Protocol

Owk Kiran Kumar, Yarlagadda Jayachandra Chowdary, Posani Viswa Teja, Thumalakunta Praveen Blessington, Thumati Ravi

[*] and [**] are Final Year B.Tech Students, Dep't of ECE ,KL University, Vaddeswaram, AP, India.
[***] are Associate Professors, Dep't of ECE, KL University, Vaddeswaram, Andhra Pradesh, India.

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 traffic3, 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

Introduction:

Under the Action Plan eEurope 2005, it was recognized by the Commission that "IPv6 is essential on the road leading to network-based technologies, products and services that will contribute to an "everywhere", user-cent'ric Information Society".

This gave rise to the European Commission's Communication to the Council and the European Parliament (COM/2002/96) – "Next Generation Internet – priorities for action in migrating to the new Internet protocol IPv6", which creates a context for the EU Members to take action in focusing on broadband availability and the development of IPv6. These developments require a concerted action aiming at the structuring, consolidation and integration of European efforts on IPv6, notably through:

1. Increased support towards IPv6 in public networks and services;
2. The establishment and launch of educational programmers on IPv6;
3. The adoption of IPv6 through awareness raising campaigns;
4. The continued stimulation of the Internet take-up across the European Union;
5. Increased support to IPv6 activities in the Framework's Programme;
6. The strengthening of the support towards the IPv6 enabling of national and European Research Networks;
7. An active contribution towards the promotion of IPv6 standards work;
8. The integration of IPv6 in all strategic plans concerning the use of new Internet services.

In order to take some of the proposed actions, various European Countries have created an IPv6 Task Force group open to the different market players, including manufactures, operators, providers, applications developers, academic institutions, etc.

Following the European Commission's Communication, the present document explains the different aspects involved in IPv6 implementation that could lead to guidelines on the priorities for implementing and adopting IPv6 in public networks and services. The consequences for the market parties, including the users are also discussed.

2. IPv6 – the next generation of IP

"In the general sense, an internet is a computer network that connects several networks. The Internet is a publicly available internationally interconnected system of computers plus the information and services provided to their users using a TCP/IP suite of packet switching communications protocols[1]".

To interconnect two or more computer networks it is necessary to have a routing device to exchange traffic, and steer traffic via several

different nodes on the path across a network to its destination. The devices used to interconnect different networks are routers. Others devices with specific functions like gateways or bridge are also used. All network elements such as routers, switches, gateways, bridges, LAN cards, need to have at least one IP address.

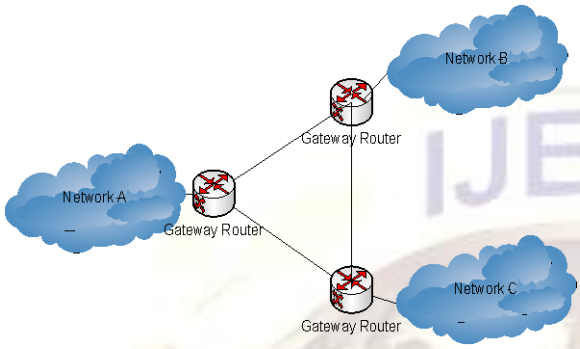


Figure 1: Use of routers

Different IP packet networks are normally interconnected by Routers that have added functionality to permit accounting between the interconnected networks. In other configurations they act also as interworking devices between different protocols.

2.1 Major benefits of the IPv6 – Why change?

The new version of IPv6 was conceived to replace the previous IPv4 standard that was adopted two decades ago as a robust, easily implemented standard.

However IPv4 is being used successfully to support the communications systems in the emerging information society and has been updated to extend its useful life (e.g. NAT mechanism, IPsec protocol), MPLS, Tunneling). However its capabilities are somewhat limited in the following areas:

- Exhaustion of the IPv4 address space;
- Growth of the Internet and the maintenance of routing tables
- Auto-configuration
- Mobility
- Security
- Quality of service

and the purpose of developing |IPv6 is to overcome these limitations.

The areas where IPv6 offers improvement are:

- **Expansion capacity for addressing and routing** – the IP address space is expanded from 32 bits to 128 bits, enabling a greatly increased number of address combinations, levels of hierarchical address organization and auto-configuration of addresses;
- **Simplified header format** – the IPv6 basic header is only 40 bytes long in spite of the greatly increased address allocation;
- **Enhanced options support** – several different, separate "extension headers" are defined, which enable flexible support for options without all of the header structure having to be interpreted and manipulated at every router point along the way;
- **Quality of service** – the Flow Label and the Priority fields in the IPv6 header are used by a host to identify packets that need special handling by IPv6 routers, such as non-default quality of service or "real-time" service. This capability is important in that it needs to support applications that require some degree of consistent throughput, delay, and jitter;
- **Auto-configuration** – adds the concept of dynamic assignment of part of the address space, based on geographic and topographic features of a given physical connection
- **Elimination of the need for NATs (network address translators)** – since the IP address space supports approximately 3.4×10^{38} possible combinations, the need for private addressing schemes behind NATs is unnecessary on grounds of address conservation;
- **Improved security with mandatory IPsec implementation** – IPv6 provides for integral support for authentication, privacy and data integrity measures, by requiring all implementations to support these features;
- **Mobility** - mobile computers are assigned with at least two IPv6 addresses whenever they are roaming away from their home network. One (the home address) is permanent; the other (the IPv6 link-local address) is used temporarily. In addition, the mobile node will typically auto-configure a globally-routable address at each new point of attachment. Every IPv6 router supports encapsulation, so every router is capable of serving as a home agent on the network(s) to which it is attached.

2.2 IP addressing architecture

An IP address is a binary number, which identifies any user's computer directly connected to the Internet. An IPv4 address consists of 32 bits, but it is usually represented by a group of four numbers (8 bits hexadecimal), from 0 to 255 ranges and separated by full stops. An example of this representation is showed bellow

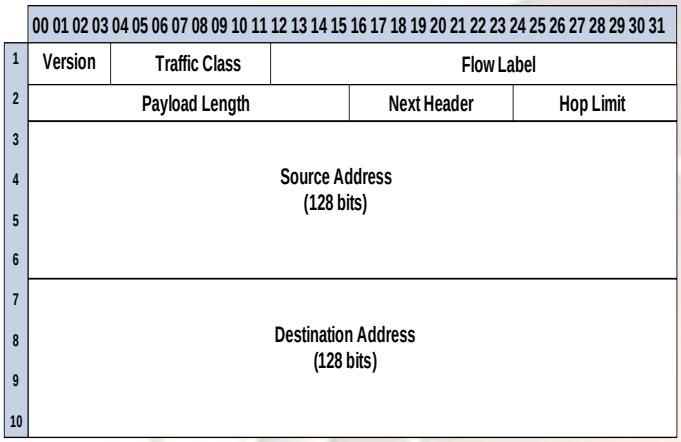
124.32.43.4

Several domain names can also be linked to the same IP address, in effect similar to having more than one name for the same person.

The most recognized change from IPv4 to IPv6 is the length of network addresses. The IPv6 addresses have 128 bits length. The 128 bits provide approximately $3.4x10^{38}$ separate values. An IPv6 address consists of eight numbers in the hexadecimal format, from 0 to 65535 (decimal) ranges and separated by a colon ":". An example of this new representation is showed following:

FECA: 0000:234A:0043:AB45: FFFF: 9A3E:000B

In other to compare with the IPv4 header next figure 3 shows the IPv6



format header:

Figure 3: IPv6 Structure

3. Services and Equipments

The "converging" new generation communication networks are using and planning to use an IP based network infrastructure with multi-functional end-devices, always on, always reachable peer-to-peer, with mobility, quality of service and end-to-end security. Even non telecom industries such as music, radio and television will be supported in the IP environment. There are applications that need or will benefit from IPv6 such:

- Mobile broadband IP;
- Mobile IP broadcast;
- Peer to peer VoIP;
- Digital radio;
- iTV and IPTV;
- Grids;
- P2P multiplayer games;
- RFID;
- Control networks;
- Remote manufacturing systems;
- Sensor networks;
- Microsoft (native support of IPv6 in the next version of Windows – Longhorn).

There are also a few technologies that will support the migration to IPv6 like:

- Power line Communication;
- Wi-Fi;
- Wi-Max;
- ZigBee;
- Unlicensed Mobile Access (UMA).

4. Migration

The current IP-based network will gradually migrate from IPv4 to IPv6. Signaling interworking will need to be supported between the IPv6 network and the existing IPv4 network. Mapping of signaling between IPv6 and IPv4 is required. From the deployment point of view, there are three stages of evolution scenarios:

- First stage (stage 1): IPv4 ocean and IPv6 island;
- Second stage (stage 2): IPv6 ocean and IPv4 island;
- Third stage (stage 3): IPv6 ocean and IPv6 island.

There are several migration mechanisms from the IPv4 protocol to IPv6 protocol. The most discussed techniques are:

- Dual stack – to allow IPv4 and IPv6 to coexist in the same devices and networks;
- Tunneling – to avoid order dependencies when upgrading hosts, routers or regions;
- Translation – to allow IPv6 only devices to communicate with IPv4 only devices.

Most of these techniques can be combined in a migration scenario to permit a smooth transition from IPv4 to IPv6. In the following subsections these three techniques are described briefly.

4.1 Dual Stack Technique

In this method it is proposed to implement two protocols stacks in the same device. The protocol stack used for each link depends on the device used at the other end of the link. Figure 4 shows this arrangement.

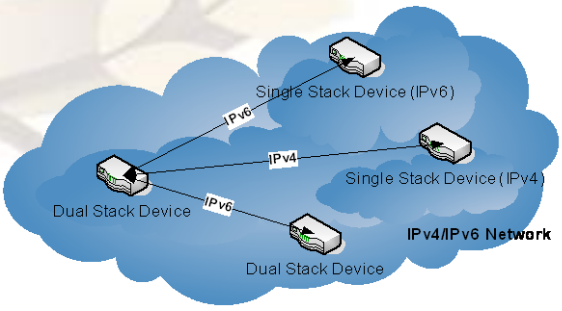


Figure 4: Dual stack operation

4.2 Tunnelling Techniques

Tunneling techniques are used in two phases in the migration to a fully IPv6 network. In

the first phase the core of the network uses the IPv4 protocol and there are only small islands IPv6. Figure 5 shows this phase. The IPv6 protocol is encapsulated in IPv4 tunnels.

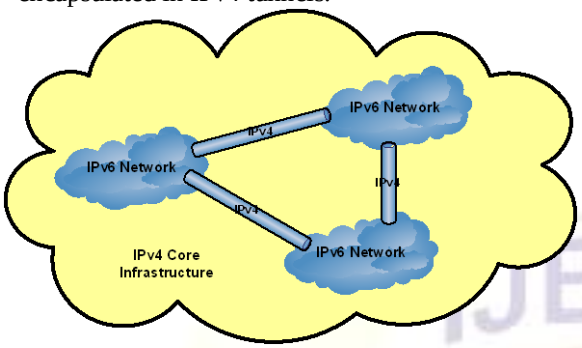


Figure 5: IPv4 Tunneling with islands of IPv6 in and IPv4 core network (phase 1)

In a second phase, when many nodes in the core of the network have already changed to IPv6, the situation is reversed and
IPv4 is encapsulated in IPv6 tunnels. The following figure shows this second phase.

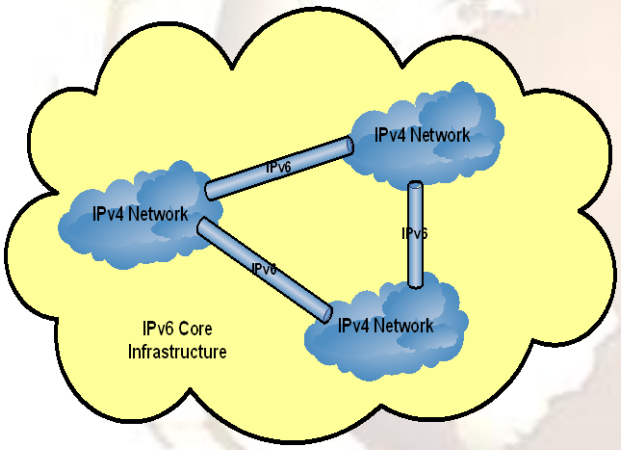


Figure 6: IPv6 Tunneling with islands of IPv4 in and IPv6 core network (phase 2)

4.3 Translation Techniques

This technique uses a device, the NATPT (Network Address Translation – Protocol Translation) that translates in both directions between IPv4 and IPv6 at the boundary between an IPv4 network and an IPv6 network. Figure 7 shows this arrangement.

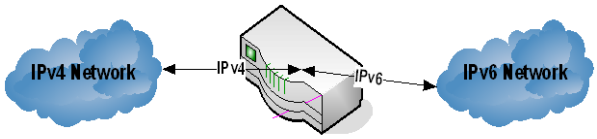


Figure 7: the arrangement with Network Address Translation – Protocol Translation

4.4 Some Proposals

As it was stated before that the solution for the migration from IPv4 to IPv6 will be a combination of the techniques described above.

The most preferable solution on the backbone of the IP Network is the use of the dual stack technique by ISPs and Network operators. This solution is already possible, because almost all hardware providers have already updated the software to support this technique.

In the access network, considering that there are many routers at the user's premises and these routers do not support IPv6 at present, the best solution is the use of the translation technique by access devices. In a further phase is possible to switch to the dual stack technique.

5. Security

"Security is the most common concern with regard to the Internet and to financial transactions via the Internet in particular. Security issues such as authenticating users, controlling access to resources, encrypting communications, and generally ensuring the privacy of transactions all need to be addressed" (European Commission).

The IPv6 is considered to have "Native Security" included by adding different extensions headers in the protocol. This security has the following characteristics:

- It works end-to-end – it is possible to have IPsec services between a pair of hosts; the authentication is separate from the encryption;
- It has an Authentication Header (AH) – this header refers to the entire packet; providing data integrity and authentication and mitigating the replay;
- It has an Encapsulating Security Payload (ESP) Header - encapsulated payload packet (tunnel); providing data integrity and authentication and/or confidentiality; mitigating the replay and limits sniffing when confidentiality is enabled.

Network Address Translation (NAT) appears to add little value in the IPv6 environment. With the increased capacity of addressing, there is no need to continue to use NATs to conserve addresses.
The Firewalls have following functions:

- They enforce uniform policy at perimeter;
- They stop outsiders from performing dangerous operations;
- They provide a check point and scalable, centralized control.

In an IPv6 network end-to-end connectivity, tunneling and encryptions can conflict with this policy. To avoid these limitations, in an IPv6 network it is necessary to combine the firewall functions and the router functions in the same equipment and to locate it in the edge of the private network. See figure 8 below:

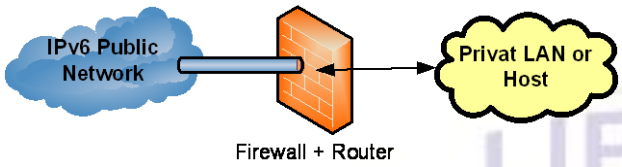


Figure 8: Combined firewall and router

6. IPv6 and the NGN

The current IP network is in a process of transition from IPv4 to IPv6. Mobile access networks are one of the major potential application areas for IPv6. This is mainly due to the large address space of IPv6. Besides, a large percentile of packets in such networks will carry real time traffic such as voice or video. These applications are expected to be important for IPv6, as they may depend heavily on the QoS mechanism in IPv6 networks. Nevertheless 3GPP is considering using IPv4 addresses initially instead of IPv6 addresses.

From the signaling point of view, the IPv6 protocol has many features related to QoS and other capabilities. By utilizing IPv6 features, such as ease of defining explicit route, flow labeling capability and improved support for extensions and options like hop-by-hop option header or destination option header, it is possible to improve the efficiency of IPv6 networks without modifying the existing signaling protocols.

7. Standards and tests

The IETF (Internet Engineering Task Force) created a working group to develop the IPv6 protocol. The "IPv6 Working Group" is responsible for the specification and standardization of the Internet Protocol version 6 (IPv6). IETF produced several specifications and protocols; these can be found at the following URL:

http://playground.sun.com/pub/ipng/html/specs/specifications.htm

The core IPv6 standards are widely implemented and are starting to see global deployment.

A European IPv6 Task Force has also been created. Delegates of the different national Task Forces take part. The link for the documents prepared for this TF is showed:

http://www.ec.ipv6tf.org/in/i-documentos.php

Another organization founded to promote de IPv6 protocol and implementation was the IPv6 Forum. IPv6 Forum is a world-wide consortium of leading Internet vendors, Research & Education Networks, with a clear mission to promote IPv6 by dramatically improving the market and user awareness of IPv6, creating a quality and secure Next Generation Internet and allowing world-wide equitable access to knowledge and technology.

To achieve these proposals the IPv6 FORUM will:

- Establish an open, international FORUM of IPv6 expertise;
- Share IPv6 knowledge and experience among members;
- Promote new IPv6-based applications and global solutions;
- Promote interoperable implementations of IPv6 standards;
- Co-operate to achieve end-to-end quality of service;
- Resolve issues that create barriers to IPv6 deployment.

The web site from this forum can be found in:

http://www.ipv6forum.com

The European Commission has been instrumental in providing necessary funding for the research and development of IPv6 related issues. In particular, and in response to the conclusions of the Stockholm Summit, the Commission stepped up its R&D efforts. A large number of IPv6 projects are currently operational, including two large-scale IPv6 trials, namely 6NET and Euro6IX.

These trials are fully complementary to the efforts deployed at national level and at European level in the context of initiatives such as GEANT.

8. Possible actions

In order to complete some of the actions proposed by the Commission and the European Task Force, guidelines should be developed to help the operators and the users gradually take the necessary steps to start the migration to IPv6 and in a near future to adopt the new version of IP protocol (IPv6).

Technical guidance is a valuable way to promote the adoption of IPv6 in public networks and services.

CONCLUSION:

The deployment of IPv6 is important to the future health of the Internet. The dwindling supply of available IPv4 addresses has been broadly documented, as have the challenges faced by those wishing to migrate to IPv6. In terms of hard data, however, industry and academia have had little visibility into the rate of IPv6 deployment in the Internet.

Near the conclusion of our one-year measurement period, we were seeing nearly 4 Tbps of traffic when averaged over a full day. We

therefore believe that our measurements provide the best available estimate of overall IPv6 traffic on the Internet.

This last point is particularly interesting. Our data seems to indicate that there is currently no significant migration of users from IPv4 to IPv6. However, since overall IPv4 traffic grew significantly, it also implies that IPv6 usage is growing at roughly the same rate as IPv4 (or perhaps slightly slower).

References

[1] 4. Bihrouzan A. Forouzan, "TCP/IP Protocol Suite", 4th Edition, McGraw Hill, ISBN: 978- 0-07-337604-2, 2010
[2] C. Caicedo, J. Joshi, and S. Tuladhar, "IPv6 Security Challenges", Computer, IEEE Computer Society, February 2009
[3] C. Balanis, Antenna Theory, Analysis and Design, 3rd edition, New York: Wiley, 2005.
[4] S. Bradner and A. Mankin, "The Recommendation for the Next Generation IP Protocol", RFC 1752, Jan. 1995
[5] 4S Telecom (P) LTD. BANGALORE User Manual

BIOGRAPHY

Owk Kiran Kumar* was born in 1992 in, Andhra Pradesh. He is pursuing his B.tech from K L University. He is interested in Communications and Wireless Networks.
Email: Owkkirankumar@gmail.com

Yarlagadda Jayachandra Chowdary** was born in 1991 at Krishna district. He is currently pursuing B.Tech from K L University. He is interested in Wireless systems and Telecommunication.
Email: jayachandrayarli@gmail.com

Posani Viswa Teja** was born in 1992 at Guntur District. He is currently persuing B.Tech from KL University. He is interested in Telecommmunication and Networking.
Email: posani.teja@gmail.com

Thummalakunta Praveen Blessington*** is working as Associate Professor in KL University. He is interested in VLSI and Networking
Email: praveentblessington@gmail.com

Thumati Ravi*** is working as Associate Professor in KL University. He is interested in Image Processing and in Signaling systems.
Email: raviblind@kluniversity.in