Asian Journal of Information Technology 11 (3): 100-107, 2012
ISSN: 1682-3915

Internet Protocols: IPv4 vis a vis IPv6

S. Dutta, P.K. Mishra, G.M. Prasad, S. Shukla and S.K. Chaulya
Central Institute of Mining and Fuel Research, Dhanbad, India

Abstract: Next generation internet protocol IPv6 provides great solution to the problems associated with IPv4. Large address space of IPv6 solves the problem of lack of IP addresses which was a major concern with the enormous growth of the internet. The new version of protocol provides innumerable benefits like auto-configuration, simple header, multicasting, quality of service, etc. which improve the overall functionality of IPv6. In the present study, the benefits of IPv6 on IPv4 have been discussed in detail including the lacuna of IPv6 in present day scenario. The future challenges have also been identified during the implementation of IPv6.

Key words: Internet protocol, IPv6, IPv4, security, transition

INTRODUCTION

Internet Protocol version 4 (IPv4) is under practice in most of the government and private organization (Postel, 1981). IPv4 was first developed in 1970s and its functionality was first published in 1981. This IPv4 with an address space of 4000 millions supposed to last for a very long time. However, the huge growth of the internet and the way addresses in IPv4 are assigned time to time (Class A-C) which in turn resulted serious lack of address. This impeding shortage of address space was recognized by 1992 as a serious limiting factor to the continued usage of the Internet run on IPv4. There are several technique like PPP/DHCP (address sharing), CISDR (Classless Inter-Domain Routing), NAT (Network Address Translation) ware developed but problem of lack of addresses cannot be overridden.

Beside this it has also limitation in security, Quality of Service (QoS), multicasting, auto configuration, mobility, etc. For this reason, Internet Engineering Task Force (IETF) initiated in 1994 to design and develop a suite of protocols and standards presently known as Internet Protocol version 6 (IPv6) (Raicu, 2002). IPv6 increases the IP address size from 32 (IPv4) to 128 bits. Increasing the size of the address, total number of unique addresses is increased from 4.3×10^9 (IPv4) to 3.4×10^38. It also gives the facility of easy configuration, simpler packet header, mobility and many more. However, at present it is not at all possible to replace whole IPv4 networking infrastructure with IPv6. Therefore, it is the challenge to migrate IPv4-based infrastructure to those supporting IPv6. IETF IPng Translation Working Group has been working on different transition mechanism so that integration between IPv4 and IPv6 would be smooth and successful. Different mechanism like dual stack, tunneling, translation has been proposed for that and researches on it still going on (Metz, 2003). Security is also a major concern in any network. IPv6 introduces IPSec protocol to provide interoperable, high quality, cryptographically based security for IPv6 (Kent and Atkinson, 1998).

ADDRESS

IPv6 has 4 time larger address space (128 bits) than IPv4 (32 bits). IPv4 provides 4, 294, 967, 296 (4.3×10^9) possible address whereas IPv6 provides 340, 282, 366, 920, 938, 463, 463, 374, 607, 431, 768, 211, 456 (3.4×10^38) possible address. The text form of the IPv4 address is nnn.nnn.nnn.nnn where 0< = nnn< = 255 and n is in decimal, leading zeros may be omitted. Maximum number of print characters is 15, not counting a mask. Whereas the text form of the IPv6 address is xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where each x is a hexadecimal digit, representing 4 bits. Leading zeros may be omitted. The double colon (::) may be used once in the text form of an address to designate any number of 0 bits. For example, ::ffff:10.120.78.40 is an IPv6 IPv4-mapped address. IPv6 address structure provides great flexibility for hierarchical addressing and routing.

HEADER

In Internet protocol, IP address of the source and the destination of the data packet are placed in front of the data field and this information is called header. Figure 1 and 2 show IPv4 and IPv6 header. IPv6 header contains less field respect to IPv4. From Fig. 1 and 2 it is seen that many of the field that are present in IPv4 header is not present in IPv6.

Incase of IPv4, source and destination field contains 32 bits where in IPv6 it is 128 bits. Therefore, in IPv4, 232

Corresponding Author: S. Dutta, Central Institute of Mining and Fuel Research, Dhanbad, India

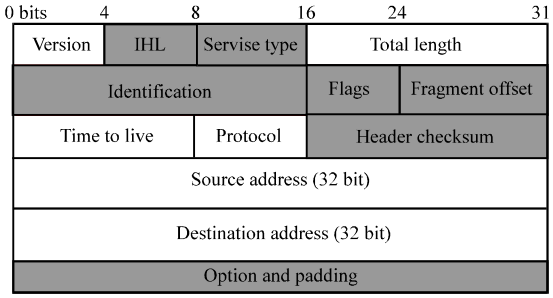

Fig. 1: IPv4 header

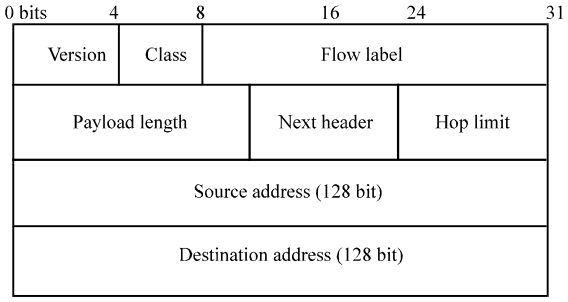

Fig. 2: IPv6 header

combinations of address can be represented where as in IPv6, possible combinations of addresses are 2128. Though in IPv6, source and destination addresses express 4 times longer than IPv4 but length of the header is not increased much because header format of IPv6 is very simple. In IPv6 there is no option field as in IPv4. To add various optional services information this option field is used in IPv4. On the other hand, extension header that is called basic header is responsible for this facility. Header Checksum field present in the IPv4 but not in IPv6. The 16 bit checksum field is used for error checking of the header. It is a number which is calculated using the number in the header. Again, header contains a number called Time to Live (TTL). However, TTL number changes whenever packet goes through the router. Therefore, header checksum has to be recalculated whenever packet goes through a router. In IPv6, Header Checksum field is removed because TCP layer checks errors of various information including sender address and destination address. IPv4 contains another field called Type of Service (TOS) which is used for priority of the packet like packet have to be delivered with express speed or in normal speed. This field is also required for cost, reliability, throughput, delay or security. IPv6 provides same functionality by its field Traffic Class. IPv6 introduce a new field called Flow Label. It has 20 bit length. By using this field, packet's sender or intermediate devices can specify a series of packets. The flow is uniquely identified by the combination of a source address and a non-zero flow label.

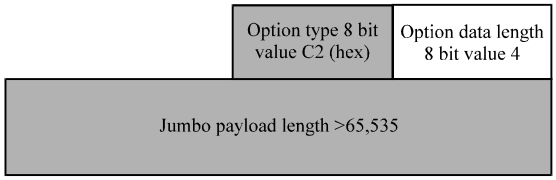

Fig. 3: Format of the Jumbo payload option

JOMBOGRAMS

In IPv4, packets are limited to 65, 535 (2^{16}-1) octets of payload. Jumbo payload is an optional feature of IPv6. It allows to exchange packets with payload of nearly 4 GB (2^{32} -1 = 4, 294, 967, 295 bytes) by making use of 32 bits of length field. Because of its large size it is called Jumbograms. Jumbograms is used to improve the performance over high-MTU (Maximum Transmission Unit) network. Jumbo payload option must not be used in those packets which carries fragment header. Figure 3 depicts the format of a Jumbo pay load option.

QUALITY OF SERVICES (QOS)

IPv6 is powerful because of its increased address space and the flow as well as traffic labeling capability. The quality of services is integrated in IPv6. In IPv6 header there are two-field: traffic class and flow label which gives the facilities of certain quality of service. Because of new flow label field and enlarged traffic class field allow more efficient and finer grained differentiation of various types of traffic in the main IPv6 header. Nodes in IPv6 can distinguish certain packets so that router can take special care of those packets using those two fields (Cooper and Yen, 2005).

SECURITY

Security is a vital aspect of internet. At the time of its designing, internet was thought to be a friendly environment so, no security was embedded in the original architecture (Sotillo, 2006). Now internet is used in everywhere, i.e., security is very much required. However, Secure Sockets Layer (SSL) IPSec, etc. are introduced because of security prospects but they seem to be inefficient. New version of Internet IPv6 solves several issues related to security that affect IPv4-based networks including its lack of network level security. In this study, different security issue and performance of IPv4 and IPv6 are discussed.

Scanning: The first point of attack is reconnaissance. In IPv4, researchers use ping technique by which

researchers can scan for active hosts or port or which services are active. In IPv4, port scanning is very easy and it takes very little time to complete because of its address space. Most IPv4 segments are Class C with 8 bits allocation for host addressing. Scanning a typical IPv4 subnet at a rate of one host per second, translates into 2^8×1 sec/1 Host×1 min/60 sec = 4.267 min. However, in IPv6 network, IPv6 subnets use 64 bits for allocating host addresses. Consequently, a typical IPv6 subnet requires 2^64×1 sec/1 Host×1 year/ 31, 536.000 sec = 584, 942, 417, 355 years (Sotillo, 2006). So, it is very difficult to scan this large address space (Popoviciu *et al*., 2006). But it is not impossible, administrator can perform scan very easily using different technique like numbering their hosts (prefix) :: 1 upwards, statelessly auto-configuring (Thomson and Narten, 1998) hosts using vendor prefixes (Chown, 2004) (Bellovin *et al*., 2006).

Unauthorized access and ICMPv6: Unauthorized access is restricted mainly using the security polices firewall. Security polices are quite same in IPv4 and in IPv6 but the maturity of IPv6 security devices are limited. Again in IPv4 network, Internet Control Protocol (ICMP) messages can be blocked. Blocking of ICMP messages improves the security of Ipv4 network. However, in case of IPv6, ICMPv6 (Conta and Deering, 1998) is a integral part of the inner working including Neighbor Discovery (Narten *et al*., 1998), Multicast Listener Discovery (Deering *et al*., 1999) (Vida and Costa, 2004) Path Maximum Transmission Unit (PMTU) Discovery (McCann *et al*., 1996) and Stateless Address Configuration (Thomson and Narten, 1998; Lancaster, 2006). Those mechanisms are dependent on some ICMPv6 messages. Again some messages like packet too big (required for the procedure of path maximum transmission unit discovery) or parameter problem (required if any unrecognized option occurs in the IPv6 packet header) must be allowed for the proper operation in the network (Durdagi and Buldu, 2010). The attacker can misuse this fact. Attackers could create an ICMPv6 tunnel encapsulating malicious traffic to avoid detection from security devices and is a big security problem for IPv6.

Fragmentation: Routers perform IPv4 fragmentation depending on the Maximum Transmission Unit (MTU). For this reason, security is hampered causing out of order fragments, overlapping fragments, Dos attack and so on. Generally, in the network, fragmented traffic is not a problem. However, if there is a large amount of fragmented traffic then it is a sign of an intrusion attempt. At that moment most IPv4 and IDs reconstruct the fragmented traffic and probability of threat can be determined using it (Lancaster, 2006; Shannon and Moore, 2002). Packet fragmentation by intermediary nodes is not allowed according to IPv6 protocol specification. In IPv6, network packet fragmentation is only possible at the source node. A fragmented packet always consists of an unfragmentable part containing an IPv6 header plus any extension header. In the original packet, extension header exists in the fragmentable part shows in Fig. 4. Using it, attackers can hide certain attribute from security device that does not perform stream reassembling correctly (Lancaster, 2006). So, many threats that exist in IPv4 are also available in IPv6 too.

Auto-configuration and Neighbor Discovery: In case of IPv4, Address Resolution Protocol (ARP) is used to map Ipv4 address to MAC address same purpose as auto-configuration and neighbor discovery. One of the great features of IPv6 is its automatic-configuration. Most important thing about IPv6 is its support of plug and play mechanism, i.e., it is possible if researchers plug a node in IPv6 network it will configure automatically without human intervention. Neither researchers have to configure each host separately nor researchers have to create a static entry in the DHCP server. IPv6 supports two types of auto-configuration.

Stateful autoconfiguration: This configuration needs human intervention. It also needs Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server for the installation and administration of the nodes (Droms *et al*., 2003). A list of nodes are stored in the DHCPv6 server so that it can supply configuration information. By tracking an address, researchers can know how long an address is being used and when it will be available for reassignment.

Stateless auto-configuration: Small organization and individual uses this type of configuration. Router Solicitation and Router Advertisement messages are exchanged in that configuration to obtain necessary information to communicate (Narten *et al*., 1998). Using the IEEE EUI-64 standard to define the network ID portion of the address it is reasonable to assume the uniqueness of the host address on the link.

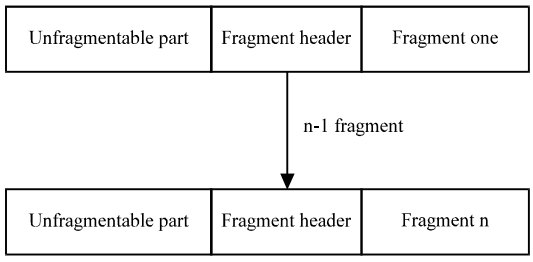

Fig. 4: Fragmentation in IPv6

It needs to check whether the address given in the node is unique or not. This is done by sending a neighbor solicitation packet (IPv6's equivalent of ARP) into the link if no response is received within a short timeout, the address is unique and hence safe to use. If a neighbor with the same address is found the system stops here and hence manual intervention is needed (the network is broken anyway, ethernet does not allow two nodes to have the same MAC (Media Access Control) address (Narten *et al*., 2007).

Broadcast amplification attacks (Smurf): Broadcast amplification attack that is known as Smurf attack is a DoS attack tool that takes advantage of the ability to send an echo-request message with a destination address of a subnet broadcast and a spoofed source address using the victim's IP. All end hosts on the subnet respond to the spoofed source address and flood the victim with echo-reply messages. In IPv6 there are no broadcast addresses (Convery and Miller, 2004). However, via multicast infrastructure Smurf attack can be achievable. Nevertheless this problem can be solved using ICMPv6 which allows error message to be sent back to the source address when certain packets are sent to multicast address (Ferguson and Senie, 2000; Lancaster, 2006).

IPSec

IPSec is a framework of open standards, developed by IETF. It secures data transmission over unprotected network. At the time of communication, participating IPSec device (peers) can achieve data confidentiality, data integrity and data authentication using it. No observation, modification or spoofing is required at the time of delivery of data with IPSec. Access control, data origin authentication, protection against replays, connectionless integrity, confidentiality (encryption), limited traffic flow confidentiality etc are the security services provided by IPSec. IPSec is the mandatory component of IPv6 (Cooper and Yen, 2005).

IPSec uses two protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). Authentication Header (AH) is used for connectionless Integrity, data origin authentication and an optional anti-replay service and Encapsulating Security Payload (ESP) is used for confidentiality (encryption), limited traffic flow confidentiality an anti-replay service. Those two protocols can be used separately or they can be used combined with each other for security in IPv4 and IPv6 (Kent and Atkinson, 1998). Figure 5 shows IPSec packet format.

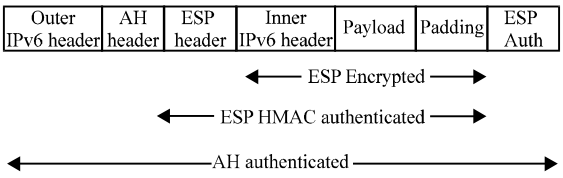

Fig. 5: IPSec packet format

Transport mode and site to site tunnel mode are the two types of modes supported by the protocol. IPSec functionality is similar in IPv4 and IPv6 however, IPv6 only supports site to site tunnel mode. In transport mode, protocol gives security functionality to the upper layer protocol whereas site to site tunnel mode is for tunneled IP packet (Kent and Atkinson, 1998).

MOBILITY

In the last few years, interest on different wireless technology like Bluetooth, GPRS, WLAN, etc. and different mobile device is growing rapidly. A huge number of users uses internet wirelessly so, internet connection must remain even in the time of their movement. IPv6 gives facilities to the mobile users by which they have the abilities to change access point while they keep their network connection. Actually, IPv6 is designed considering the mobility problem. Address autoconfiguration and route optimization are the two advantage of mobile IPv6. Foreign agent and triangular routing are the two problem of mobility. Foreign agent requires a pool of direction which shorts number of address. This problem is solved in IPv6 using autoconfiguration mechanism. Triangular routing is another drawback. Route optimization avoids this drawback in IPv6. IPv6 extension header also helps in mobility. Authentication header provides sufficient security guarantee. Routing header is also used in IPv6 Mobility. IPv4 uses encapsulation for delivery but packet delivery is realized by routing header. This new mechanism reduces overhead. Firewalls problem is also avoided in IPv6 (Parra, 2004; Nada, 2007; Johnson and Perkins, 2004).

TRANSITION

One of the biggest challenges in the deployment of IPv6 is how to migrate IPv4-based infrastructures to those supporting IPv6 network. Again new version of Internet protocol IPv6 is not backwards compatible with current IPv4 protocol therefore, IPv4 hosts and IPv4 routers could not deal directly with the IPv6 traffic. It is unthinkable to replace all the Ipv4 based infrastructure with upcoming

IPv6 over night and it will be very costly too. IPv4 and IPv6 will co-exits for a long time because there is lots of running application which supports IPv4, so when IPv6 will come those applications should also be run with IPv6 (Govil and Govil, 2008). IETF IPng Transition Working Group has been working on several transition mechanisms so that integration of IPv6 with current protocol can be done successfully and run smoothly (Raicu and Zeadally, 2003). Some transition mechanism is discussed in this study.

Dual stack: Nodes with dual IP stacks will have both IPv4 protocol stack and an IPv6 shown in Fig. 6. In this technique, IPv4 address is converted into IPv6 compatible address, i.e., first 96 bits address becomes zeroes and last 32 bits forms a valid IPv4 address. Hence, at the time of communication with IPv6 nodes, they use IPv6 and at the time of communication with IPv4 nodes, they revert to IPv4 (Parra, 2004; Nordmark and Gilligan, 2003).

Network Address Translation-Protocol Translation (NAT-PT): NAT-PT is a hardware device which is installed between the boundary of IPv4 and IPv6 network. It is one type of router. Using it, all IPv4 users can directly access IPv6 network and all IPv6 users can access IPv4 network without modification of their respective local hosts (Govil and Govil, 2008) (Fig. 7). The translations made by NAT-PT makes some problem are discussed in this study (Parra, 2004):

- Bottle neck, unique failure point
- Fiability and scalability
- Limitation of the usable applications as the E2E communication is not possible when using NAT

Tunnel: Tunneling is a mechanism in which IPv6 packets are transported through IPv4 network to a remote Ipv6 host without requiring an Ipv6 infrastructure shown in Fig. 8. In this mechanism, IPv6 packets are encapsulated into an IPv4 packet and then this IPv4 packet is sent between the IPv4 tunnels.

Their will be an Ipv6/IPv4 header translating router at each end of the tunnel (Mills, 1992). Therefore, the routers of the Ipv4 network will handle the final packet without any problem. Figure 9 shows packet encapsulation in tunneling. Tunneling can be used in many ways (Mills, 1992).

Router to Router: In this mechanism, IPv6/IPv4 routers are at the both end of an IPv4 infrastructure and those routers tunnel Ipv6 packets between themselves. Figure 10 shows router to router tunneling technique.

Host to Router: In this mechanism, IPv6/IPv6 hosts tunnel IPv6 packet to the IPv6/IPv4 router via an IPv4 infrastructure. Figure 11 shows Host to Router tunneling technique.

Host to Host: In this mechanism, IPv6/IPv4 hosts are interconnected by an IPv4 infrastructure and send IPv6 packet between them. Figure 12 shows Host to Host tunneling technique.

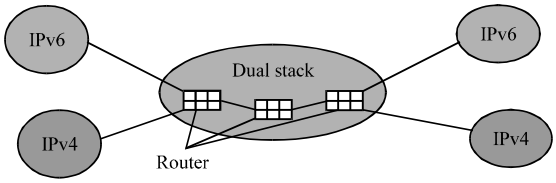

Fig. 6: Dual stack scenarioc

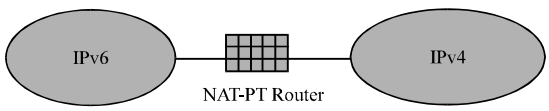

Fig. 7: NAT-PT scenario

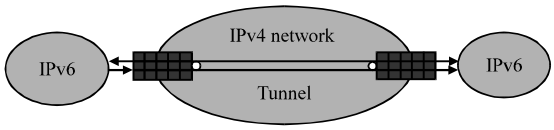

Fig. 8: Tunneling

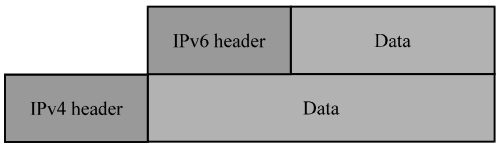

Fig. 9: Packet encapsulation

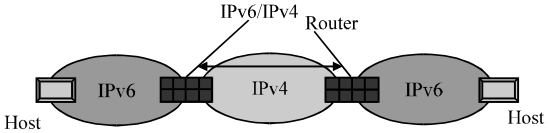

Fig. 10: Router to Router tunneling

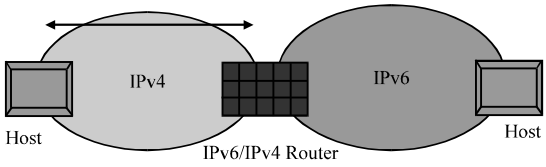

Fig. 11: Host to Router tunneling

Router to Host: In this mechanism IPv6/IPv4 router tunnel IPv6 packet to the final destination, IPv6/IPv4 hosts. Figure 13 shows Router to Host tunneling technique.

Configured tunneling: In case of router to router and host to router tunneling technique, IPv6 packets tunneled to an IPv6/IPv4 router. Tunneled endpoint is not the final destination of the IPv6 packet. An IPv6/IPv4 router is in the endpoint of the tunnel. This router than decapsulates the IPv6 packets. Therefore, at tunnel endpoint it is not the IPv6 packet's destination address. So, the address in the tunneled IPv6 packet do not provide the IPv4 address of the tunnel endpoint. Instead, node performing the tunneling provides configuration information that determines the tunnel endpoint address (Raicu and Zeadally, 2003). This type of technique is called configured tunneling.

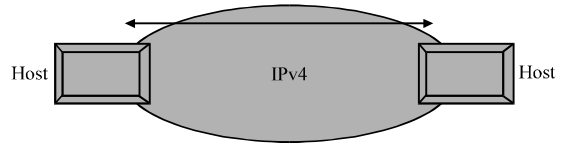

Fig. 12: Host to Host tunneling

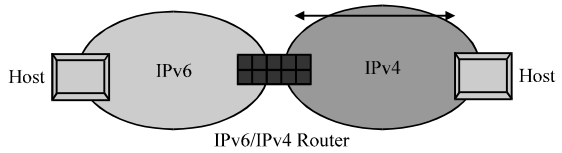

Fig. 13: Router to Host tunneling

Automatic tunneling: In case of Host to Host and Router to Host tunneling, tunnel's endpoint is the IPv6 packet's destination address. Therefore, in this case any explicit configuration is not required because in the IPv4 compatible IPv6 address, lower order 32 bits holds the destination node's IPv4 address (Nada, 2007). Destination address is derived automatically. This type of technique is called automatic tunneling.

CONCLUSION

Undoubtedly, IPv6 provides great solution to the problems associated with IPv4, especially its large address space solves the problem of lack of IP address which was a major concern with the enormous growth of the Internet. The new version of protocols provides innumerable benefits like auto-configuration, simple header, multicasting, quality of service, etc. that improve the overall functionality. IPv6 uses IPSec protocol and uses flexible extension header option for security purpose. Table 1 provides a glimpse of critical review of IPv6 over

Table 1: Critical review of IPv6 over IPv4

Internet protocol	IPv4	IPv6
Address space	32 bits long (4 bytes)	128 bits long (16 bytes)
Address	4.3×10^9 possible	3.4×10^38 possible
Header	More field	Less field
Checksum	Available	Not required
Option field	Available	Extension header available
TOS	Available	Traffic class available
Address lifetime	Not applicable	Two lifetimes: preferred and valid, preferred lifetime is valid
Address mask	Used	Not used
Address Resolution Protocol (ARP)	Map IPv4 address to MAC address	Replaced with Neighbor discovery
Address types	Unicast, multicast and broadcast	Unicast, multicast and anycast
Configuration	Manually or through DHCP	Auto-configuration
IPSec	Optional	Inbuilt IPSec support
File Transfer Protocol (FTP)	Support	Does not support
Fragmentation	Done only by sender and forwarding routers	Only by sender
Internet Control Message Protocol (ICMP)	Used to communicate network information	Similarly for IPv6, Internet Control Message Protocol version 6 (ICMPv6) provides some new attributes
IP header	Variable length of 20-60 bytes	Fixed length of 40 bytes
Loopback address	127.*.*.* (typically 127.0.0.1)	0000:0000:0000:0000:0000:0000:0000:0001 or ::1 (shortened version)
Packet flow identification	Not available	Available using flow label field
Mobility	Uses mobile IPv4	Uses mobile IPv6. Better router optimization, hierarchical mobility, efficiency and scalability latest 3G mobile technologies support
Maximum Transmission Unit (MTU)	Minimum MTU that routers and physical links were required to handle was 576 bytes	All links must handle a datagram size of at least 1280 bytes
Ping	Easy	Very time consuming
Quality of service (QoS)	Present	Traffic class and Flow label field. More efficient and finer
Renumbering	Manually, exception of DHCP	Automatic
Simple Network Management Protocol (SNMP)	SNMP is a protocol for system management	Currently, SNMP does not support IPv6. IPv6 routing uses static routes

IPv4. In practice that could help and provides better security than IPv4 but lots of security problem still exist and require consideration. Major challenges will arrive in the time of transition when both new version and old version of the Internet protocol will have to exist side by side. Different transition mechanism is proposed for that purpose but they are not perfect and it will be a very complex work. Now it is very early stage of IPv6 and many researches are going on in that subject too.

ACKNOWLEDGEMENT

The researchers are thankful to the Director, Central Institute of Mining and Fuel Research, Dhanbad for his kind support and encouragement.

REFERENCES

Bellovin, S.M., B. Cheswick and A.D. Keromytis, 2006. Strategies in an IPv6 internet. LOGIN, 31: 70-76.

Chown, T., 2004. IPv6 implications for TCP/UDP port scanning. IETF Internet Draft. http://www.ietf.org/proceedings/65/slides/v6ops-10.pdf.

Conta, A. and S. Deering, 1998. Internet control message protocol (ICMPv6) for the internet protocol version 6 (IPv6) specification. RFC: 2463, Internet Engineering Task Force.

Convery, S. and D. Miller, 2004. Ipv6 and Ipv4 threat comparison and best-practice evaluation (v1.0). CISCO. http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf.

Cooper, M. and D.C. Yen, 2005. Ipv6: Business applications and implementation concerns. Comput. Stand. Interfaces, 28: 27-41.

Deering, S., W. Fenner and B. Haberman, 1999. RFC2710-multicast listener discovery (MLD) for IPv6. http://www.faqs.org/rfcs/rfc2710.html.

Droms R., J. Bound, B. Volz, T. Lemon, C. Perkins, M. Carney, 2003. Dynamic host configuration protocol for IPv6 (DHCPv6). RFC 3315, http://www.ietf.org/rfc/rfc3315.txt.

Durdagi, E. and A. Buldu, 2010. IPV4/IPV6security and threatcomparisons. Procedia-Soc. Behav. Sci., 2: 5285-5291.

Ferguson, P. and D. Senie, 2000. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC Editor, United States.

Govil, J. and J. Govil, 2008. An examination of IPv4 and IPv6 networks: Constraints and various transition mechanisms. Proceedings of the IEEE Conference on Southeastcon, April 3-6, 2008, Huntsville, AL, pp: 178-185.

Johnson, D.B. and C. Perkins, 2004. Mobility support in IPv6. IETF RFC 3775, Network Working Group. http://www.ietf.org/rfc/rfc3775.txt.

Kent, S. and R. Atkinson, 1998. Security architecture for the internet protocol. RFC 2401. http://www.janko.at/Humor/RFC/rfc2401.htm.

Lancaster, T., 2006. IPv6 and IPv4 threat review with Dual-stack considerations. COMP6009:Individual Research Project. http://www.mediamob.co.kr/FDS/newBlogContent/2007/0423/infoland/troy-Final-IRP-Report.pdf.

McCann, J., S. Deering and J. Mogul, 1996. Path MTU discovery for IP version 6. RFC 1981. http://www.ietf.org/rfc/rfc1981.txt.

Metz, C., 2003. Moving toward an IPv6 future. IEEE Int. Comput., 7: 25-26.

Mills, D.L., 1992. Network time protocol (version 3) specification, implementation and analysis. http://tools.ietf.org/pdf/rfc1305.pdf.

Nada, F., 2007. Performance analysis of mobile IPv4 and mobile IPv6. Int. Arab J. Inform. Technol., 4: 153-160.

Narten, T., E. Nordmark and W. Simpson, 1998. RFC 2461 Neighbor discovery for IP version 6 (IPv6). RFC 2461. http://www.ietf.org/rfc/rfc2461.txt.

Narten, T., E. Nordmark, W. Simpson and H. Soliman, 2007. Neighbor discovery for IP version 6 (IPv6). Standards Track, IETF RFC 4861. http://www.ietf.org/mail-archive/web/ietf-announce/current/msg04114.html.

Nordmark, E. and R.E. Gilligan, 2003. Basic transition mechanisms for IPv6 hosts and routers. http://tools.ietf.org/pdf/draft-ietf-v6ops-mech-v2-00.pdf.

Parra, J.I., 2004. Comparison of IPv4 and IPv6 networks including concepts for deployment and interworking. Proceedings of the INFOTECH Seminar Advanced Communication Services, July, 2004, Stuttgart, Germany, pp: 1-13.

Popoviciu, C., E. Levy-Avegnoli and P. Grossetete, 2006. Deploying IPv6 Networks. Cisco Press, Indianapolis, IN., USA.

Postel, J., 1981. Internet protocol, DARPA internet program protocol specification. RFC 791. http://www.ing.unp.edu.ar/asignaturas/rytd/RFC/rfc791_IP.pdf.

Raicu, I. and S. Zeadally, 2003. Evaluating IPv4 to IPv6 transition mechanisms. Proceedings of the 10th International Conference on Telecommunications, February 23-March 1, 2003, Tahiti, pp: 1091-1098.

Raicu, I., 2002. An empirical analysis of internet protocol version 6 (IPv6). Master Thesis, Wayne State University.

Shannon, K.C.C. and D. Moore, 2002. Beyond folklore: Observations on fragmented traffic. IEEE/ACM Trans. Network., 10: 709-720.

Sotillo, S., 2006. IPv6 security issues. http://www.infosecwriters.com/text_resources/pdf/Ipv6_SSotillo.pdf.

Thomson, S. and T. Narten, 1998. IPv6 stateless address autoconfiguration. RFC 2462. http://tools.ietf.org/pdf/rfc2462.pdf.

Vida, R. and L. Costa, 2004. Multicast listener discovery version 2 (MLDv2) for IPv6. RFC 3810. http://www.ietf.org/rfc/rfc3810.txt.