International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.5, No.6, June 2016 **DOI:10.15693/ijaist.2016.v5.i6.7-19**

ROLE OF IPV6 IN CYBERCRIME

Rajkumar G Verma
Network Administrator
Symbiosis International University
Pune, India.

Abstract

Ipv6 provides a platform for new Internet functionality that will be needed in the immediate future and provide flexibility for further growth and expansion. Huge data lying on open internet and almost all the organization and individual are connected with each other by means of network of networks internet. In digital era there are both things one that people are close to each other and share everything which they feels even they see or real time interaction with each other.

Other aspect of Internet network there should be a secureness of data integrity, confidentiality, secured information flow allthis can be achieved with the help of minimization of cybercrime.

Cybercrime includes wide range of activities this activities may be classified as a fundamental breaches of personal, groups privacy ,trade secret theft, economic espionage ,governments policies, corporations ,illegally gathered digital information to blackmail individual or organization when all this information are stored on a computer or networks are used as tool to acquire profitable information which leads a criminal activity .Cybercrime involve a computer network s, which may be very few numbers of acts on integrity, confidentiality, accessibility, veracity and availability of digital data or systems.

Communications take place on network with the help of Internet protocol, Ipv6 is a latest technology consisting lots of features, which will benefit in secure communication as well as cybercrime forensics investigation.

A new IPV6 standard having robustattributes,unique and pure without any proxies and Network address translation individual system IPv6 address can be configured which will helps in cybercrime forensic investigation as well as in digital forensic science.Interesting properties with respect to email identification, individual system unique address having new header format, large address space, stateless and state full configuration, IPSec header, neighboring node interaction, global addressing with end-to-end connectivity, Zone Identifier or Scope ID, EUI-64 address based Interface Identifiers, Mobile IPV6 helps to gather the authentic and authorized information for cyber forensic investigation.

Keywords: IPV6, TUBA, EUI, NAT, DIGITAL FORENSIC.

INTRODUCTION

Billions of devices and objects , internet of things , always ON, broadband connected sensor networks multiple addresses per device are reaching very fast to this world for all this a robust and secure ipv6 technologies will helps them in a bigger way.

Internet protocol dependent on future technologies need a long-term evolution, multimedia applications, roaming irrespective of network access methods there must be a continuity of real time sessions.

In Mobile Ipv4 technologies there is a limitation of mobility like no proper route optimization means no direct routing, needs a foreign agent i.e. extra router, no unique IP address to wireless device or a

mobile device. In ipv6 direct routing from correspondent node to mobile node can be optimized, no need of extra router foreign agent, each mobile device can be utilized as a single unique ipv6 address

Ipv4 addresses having the issues like address space which is simple 32 bit address space, network transparency, complex routing and processing overhead ,security and mobility issues all this is solved by newer protocol ipv6.

LIMITATION OF IPV4

IPv4 does not anticipate the recent exponential growth of the internet and the impending exhaustion of the current ipv4 address space. The need for better support for prioritized and real –time delivery of data sometime referred to as quality of service (QOS)-exist for ipv4, real time traffic support relies on the 8 bits of the historical ipv4 Type of Service (TOS) field and the identification of the payload, typically using a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) port. Type of Service filed has a limited functionality & differentiated services code Point (DSCP) is used for the prioritized delivery and handling the packets.

Cryptographic services for Internet layer is an optional in ipv4, which is know as Internet Protocol Security (IPSec) is a optional for IPv4. IPSec is private communication over a public medium.

Packet sniffing, IP spoofing, connection hijacking are weakest feature for ipv4.

Limited subnet address space can leads port scanning may be the vulnerable in a network.

Generally Denial of Service (DoS) attack is more in a broadcast environment.

In Mobile Ipv4 technologies there is a limitation of mobility like no proper route optimization means no direct routing needs a foreign agent i.e extra router, no unique ip address to wireless device or a mobile device .

Recent Exponential growth of the Internet and the wipe out of the ipv4 address space, rising smart devices on internet and appliances ensures that the public ipv4 address space will be absolute.

Implementations of IPv4 can be done by either manually configured or use a stateful address configuration protocol such as Dynamic Host configuration Protocol (DHCP).

DESCRIBING OF IPV6

Ipv6 is the next generation protocol for the Internet technologies .The protocol is installed as software application in most of the devices and operating systems. Currently transition mechanisms available for configuration and deployment.

New variant of IPv6 are

- Extended address format space from 32 bits to 128 bits.
- Auto configuration State full and Stateless Configuration
- Simplification of header format.
- Improved support for options and extensions

IPV6 classified into three categories:

Unicast
Multicast
Anycast

Address Privacy:

Unique Stable IP addresses
Deploy through, annual configuration, a DHCP server or Stateless Address Autoconfiguration using EUI-64 interface identifier.

Temporary transient IP addresses

Deploy using the random number that changes in regular intervals and can be used in place of the stable interface identifier.

NOTATION OF IPV6

Ipv6 use the hexadecimal encoded scheme, a base-16 numbering system common in networking and computing. Ipv6 address can range not only from 0-9,but also from A-F.In IPV6 notation, address are grouped typographically on 16 bit boundaries with a colon (:). Since addresses are 128 bits long, this means there are 8 groups, every group using hex digits. For example 2001:9BD7: 6004:2015:2000:76DD:FEAC: E90A

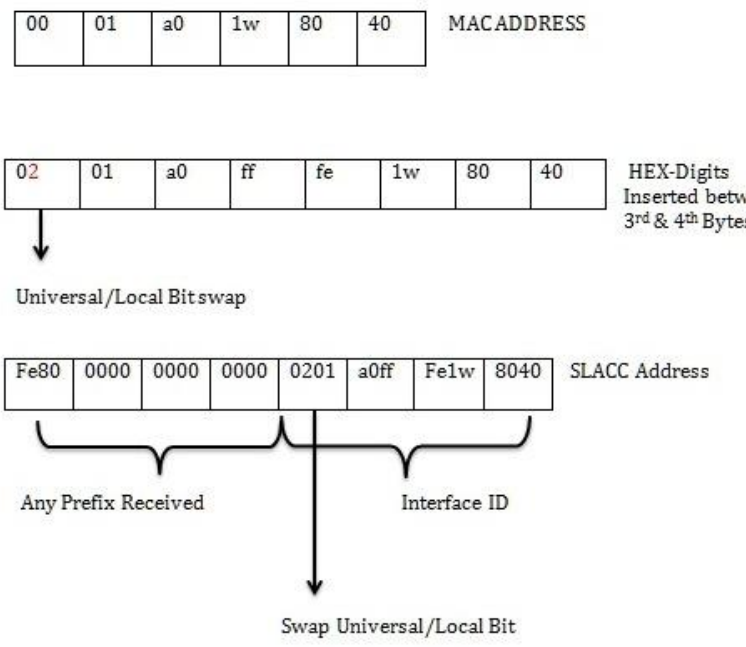
UNIQUE NOTATIONS OF IPV6 WITH EXTENDED UNIQUE IDENTIFIER (EUI)

EUI-64 bit is a unique identifier defined by the Institute of Electrical and Electronics Engineers (IEEE). Addresses in the prefix range 001 to 111 should use a 64-bit interface identifier that follows the EUI-64 (Extended Unique Identifier) format expect for multicast addresses with the prefix 1111 1111).

During Stateless Address Auto configuration for a link-local address on an Ethernet interface using its Mac address, the 64-bit interface identifier has to be created from the 48-bit Ethernet MAC address.

First, the HEX digits 0xfffe are inserted between the third and forth bytes of the MAC address. Universal/local bit, the second low-order bit of 0x00, which is a first byte of the MAC address, is complemented .The second low-order bit of 0x00 is 0 which when complemented, becomes 1 as a result the first byte of the MAC address becomes 0x02.

For example IPv6 interface identifier corresponding to the Ethernet MAC address 00-01-a0-1w-80-40 will be 02-01-a0-ff-fe-1w-80-40 with the prefix fe80::/64 and interface identifier 02-01-a0-ff-fe-1w-80-40 , is fe80::201:a0ff:fe1w:8040.



128 Bits Enough?

If we use Host Density ratio, or HD Ratio. This is a number that increases from zero to one as the address space fills.

$$HD := \frac{\log(\text{number of allocated objects})}{\log(\text{Maximum number of allocable objects})}$$

Empirical Calculations for telephone number allocation and network address assignment show that a HD Value of 0.8 is reasonable but a HD value of 0.85 is overcrowded.

For Ipv4 a HD ratio of 0.8 corresponds to $2^{32 * 0.8,}$ or about 50 million hosts. The Internet Domain Survey, http://www.isc.org/ds/, suggest that we passed this point some time ago and we are now at a point where HD>0.85. A comfortable density of 0.8 for ipv6 would correspond to $2^{128*0.8}$ or about 1,000 hosts for every point of the earth.

SCOPE IDENTIFIERS

IPv6 allows scoped address, which are only meaningful in a particular specific context. How

ipv6 knows a particular specific host on a link if the computers connected to several links .we having the link-local address like FE80::1 for a host but when this host is connected to number of links then we can add a flag to programs like ping,to allow the specification of an interface.

For instance, the RED and WINDOWS stacks allow the specification of link as part of the address by including a scope identifier. On a RED derived stack, as found on Unix systems, FE80::1%en2 means the address FE80::1 on the network attached en2. On WINDOWS derived stacks the scope-id is usually given as a number, so FE80::1%9 means address FE80::1 on IPv6 interface 9.

Scope Identifiers is one of the methods to index an authentic specific operating system machine on a link.

ADDRESS ARCHITECTURE

IPv6 there are a number of address spaces, usually express as prefix with CIDR network length.

Table 1.1 The breakup of the Ipv6 Address Space by IANA

PREFIX	INTENDED USE
::0/96	Unspecified/loopback/compatible-IPv4 address
2000::/3	Global Unicast
FE80::/10	Link-local Unicast
FF00::/8	Multicast
FC00::/7	Local IPv6 Unicast addresses (In Process)
::FFFF:0.0.0.0/96	Mapped IPv4 Addresses
400::/7	Reserved for IPS Allocations
200::/7	Reserved for NSAP allocation
2001::/16	Production via Regional Internet Registries*
2002::/16	6to4transition mechanism*
3FFE::/16	6bone test network*

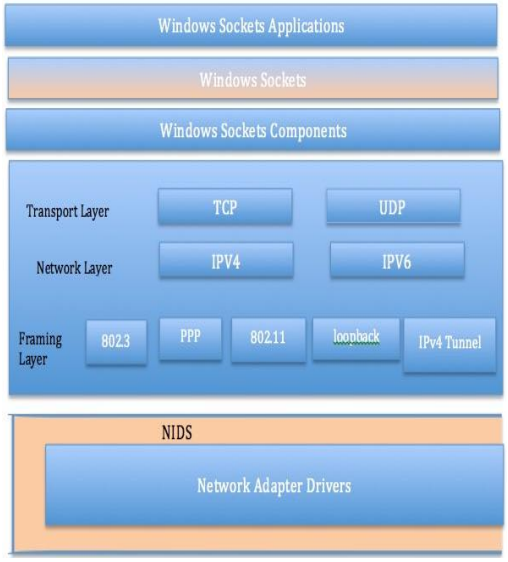
*Allocated IPv6 Global Unicast addresses

ARCHITECTURE OF THE IPV6 PROTOCOL FOR WINDOWS

The TCP/IP driver file, Tcpip.sys, contains both IPv4 and IPv6 internet layers.Tcpip.sys operates between Windows Sockets and the Network

Device Interface Specification (NDIS) layers in the windows network architecture. The architecture of Tcpip.sys consists of the following layers:

- Transport Layer Contains the implementation of TCP and UDP.
- Network Layer Contains implementation of both IPv4 and IPv6.
- Framing Layer Contains modules that frame IPv4 or IPv6 packets. Modules exist for IEEE 802.3 (Ethernet), IEEE 802.11,point-to-point protocol (PPP), and mobile broadband Links. Modules also exist for logical interfaces such as the loopback interface and IPv4-based tunnels. IPv4-based tunnels are commonly used for IPv6 transition technologies.



BASIC IPV6 STACK SUPPORT

Internet Engineering Task Force (IETF) standards for IPv6 protocol stack functionality, including the following:

- The Ipv6 Header
- Unicast, multicast and any cast addressing
- The internet Control message Protocol for IPv6(ICMPv6)
- Neighbor Discovery (ND)
- Multicast Listener Discovery (MLD) and MLD version 2 (MLD v2)
- Stateless address Auto configuration

IPV6 STACK ENHANCEMENTS

Explicit Congestion Notification supports when the TCP segment is lost due to congestion at a router and performs congestion control, which dramatically lowers the TCP sender's transmission rate.

Dead Gateway detection through neighbor unreachability detection. Dead gateway detection can also be triggered by the failure of TCP connections.

Router Advertisements helps in default route preferences and route information options.

Strong host model for both sending and receiving, which will benefits in cyber forensic investigation like identification of sender host mail header part or destination host mail header part without the hurdles of network address translation or proxies systems.

Computers or network are used as tools on criminal activity refer to spamming and criminal copyright crimes, particularly those enabled via peer-to-peer network which will refer to Cybercrime
Where the target of criminal activity is the computer or network where contain unauthorized access, viruses, malware (malicious code) and denial-of-service attacks, spam emails, theft of service, financialfraud, all can be minimize with the Ipv6 technologies as they will deploy directly to the individual system with out any proxies and network address translations systems.

Direct allocation of ipv6 address to system solved most of the NAT implications like end-to-end network model, breaks end-to-end security

(IPSec), minimization of application gateway, merging of separate private networks can be carried out which is difficult in ipv4 network as there might be a address clashes.

Ipv4 technology has numerous vulnerabilities; exploitation of the vulnerability could lead to whole system compromisation. Ipv6 helps in restrictions of new vulnerabilities for attacker as this technology having the inbuilt IPSec features, sufficient header size, Field Type label and hexadecimal notations set up adequate protection. Support for Source Demand Routing Protocol (SDRP) sender can specify packet route, destination can return packet via same route, and security and header encryption can be achieved.

Identifications of fake mail can be trace out with the help of IPv6 protocol as there will be limited network address translation system or route filtration process involved in-between the source and destination packet address. As most of the ipv6 system having unique individual ipv6 address without any masking which is again a authentic responsible individual ipv6 system for any communication.

COMPARISON BETWEEN IPV4 AND IPV6 PROTOCOL WITH RESPECT TO CYBER FORENSIC INVESTIGATION

Serial Number	*Category*	*IPv4*	*Ipv6*
1	Address length	32 bits (4 Bytes)	128 bits (16 Bytes)
2	Total Number of Addresses	$2^{32=}$ 4.3 Billion Addresses	2^{128} = $3.4 * 10^{38}$ Addresses
3	Address Syntax	Ipv4 addresses are represented in dotted-decimal format.32-bit ipv4 address is divided along 8-bit boundaries. Each set of 8 bits is converted to its decimal equivalent and separated by periods. For example 192.168.0.0	For Ipv6 the 128 bits address is divided along 16-bit boundaries and each 16-bit block is converted to a 4-digit hexadecimal number and separated by colons. The resulting representation is called colon hexadecimal.

			The 128-Bit address is divided in binary form. Each 16-bit Block is converted to hexadecimal and delimited with colons. No case sensitive. For example 2001:AABB:0000:CCCC: 2456:FFFF: DD33: 6678
4	Address Type	Broadcast, Unicast, Multicast	Multicast, Unicast, Any cast. In any cast number of interfaces act as destinations but the packet is landed as per the routing protocol.
5	Address Resolution Protocol	Physical addresses like a Mac or Link address	MAC addresses gain by Neighbor Discovery Protocol using ICMPv6.
6	Configuration	Either by DHCP or Manually	Two way of Auto configuration: Stateless auto configuration with the

			ND router, Sate full auto configuration with the help of DHCPv6 server OR Manually.
7	Domain Name Service (DNS)	Mapping of name to IP and vice versa.	Format of Resource Records changed in DNS v6
8	Fragmentation	Sender and forwarding Routers are responsible for fragmentation if the packet is too big.	From sender point fragmentation can be done .
9	Internet Control Message Protocol (ICMP)	Error, request, request reply, destination unreachable messages are generated by the network devices through the ICMP protocol.	ICMPv6 having more attributes like packet processing, diagnostic activities, Neighbor Discovery process and Multicast message these type of reporting can be carried out.
10	Router Discovery	ICMP Router Discovery protocol provide default gateway to host on a	ICMPv6 use the Router solicitation and Router Advertisement for nodes

		network	on a network.
11	Internet Group Management Protocol (IGMP)	Host information, Multicast groups, Host membership exchange and update by the IGMP.	Multicast Listener Discovery(MLD) realize multicast listeners on the links that are directly attached
12	Network Address Translation (NAT)	It is a masking process of original IP address into another modifying masked IP address. Methods of translation like One-to-One NAT, one-to-many NAT, Port-restricted NAT	NAT not Required in IPv6 Technologies. No need of any IP masquerading & no need of proxy system. Transition technologies can be used for older ipv4 infrastructures.
13	Quality of Service	QOS demand packet prioritization bandwidth and priority for TCP/IP application.	Flow Label Field defines how specific packets are identified as well as carried by the routers. Benefits of flow label field will enhance the More tolerance to packet losses, less latency and

			congestion, real time applications.
14	Simple Network Management Protocol (SNMP)	It's an internet standard protocol for collecting and organizing information about managed devices on IP networks.	SNMP not used in IPV6 technologies.
15	IPSec	Optional	Important Protocol in IPv6, it involves a set of cryptographic protocols for making secure and key exchange information.
16	Mobility	Ipv4 does not support address Mobility	Use Mobile address with MIPv6 with faster routing, handover and structured mobility .
17	Extension Header	No extension Header	Variable Extension header added into Ipv6 header .It handles security and the function of options field in ipv4.

Introduction of New protocol in IPv6

- Link-Local Multicast Name Resolution Protocol (LLMNR)

LLMNR is a new protocol provides an additional method allows name resolution on networks or on a temporary networks where a DNS server not present or Implemented.

- Ipv6-Literal.net Names

Name resolves to Ipv6 Address done by the IPv6Address.ipv6-literal.net converts the colons (:) in the address to dashes (-). For example, for the ipv6 address 2001:AABB:0000:CCCC: 2456:FFFF: DD33: 6678, the corresponding ipv6-literal.net name is 2001-AABB-0000-CCCC-2456-FFFF-DD33-6678.ipv6-litral.net.
When submitted by an application for name resolution, the 2001-AABB-0000-CCCC-2456-FFFF-DD33-6678.ipv6-litral.net name resolves to 2001:AABB:0000:CCCC: 2456:FFFF: DD33: 6678.

- Peer Name Resolution Protocol (PNRP)

In peers rely network host want to resolve the each other's network locations (addresses, protocols, and ports) from name or other types of identifiers. Peer Name Resolution Protocol (PNRP), a secure, scalable, and dynamic name-registration and name-resolution protocol. Secured and unsecured name can be published even the PNRP uses public key cryptography to protect secure peer names against spoofing.

- DNS Security Extensions (DNSSEC)

Authentication and verification done by the DNSSEC for any DNS query to minimize the various types of attacks that try to spoof an Internet. Some of the secure attributes for sending traffic data over Internet are originating authentication, authenticated denial of existence; data integrity can be carried out by these attributes. Security services deploy by the DNSSEC uses public key cryptography.

- (TCP, UDP with bigger Address or TCP/UDP over CLNP Addressed Networks) TUBA

In transition technologies packets are allowed to move from ipv4 to Ipv6 with the help of TUBA, dual –stack, no flag system, there is no change in TCP&DUP transport layer but replace IP with Connectionless Network Protocol (CLNP). Which is very near to equivalent of IP in the ISO networking stack.

- Common Architecture for the Internet (CATNIP)

One nice attempt made on merging three most important protocols namely IP, the OSI ISO protocols, and the Novell networking stack. It tells you theoretically possible for an end host using IPv4 to communicate transparently via RCP to end host-using IPX.

- Simple Internet Protocol Plus (SIPP)

SIPP was merging of two earlier suggested protocols SIP and PIP with 64 bits for addresses by default .It also
Adopted other proposed protocols such as IP-in-IP.

DISCUSSION

Authentic actionable results or outcomes can be carried out with the ipv6 addresses technologies. Actionable result or outcomes can be suitable for cybercrime investigation, which can be further used as authentic evidence in front of law enforcement agency.

We can restrict unlawful or unethical activity after the deployment of ipv6 technologies to individual systems.

These Technologies will be give necessary procedures, which are useful for investigators to scrutinize these to identify, seize and mark legal action against criminals involved in cybercrime.

Cryptographically generated addresses (CGA's) is to prove the owner ship of an address and to prevent spoofing and stealing of existing ipv6 address.

CONCLUSION

The attributes of IPV 6 Technologies, which contribute towards the cyber forensic investigations along with its implications, have been studied in detail. IPV 6 will prove to be more efficient in absence of proxies, Network address Translation Systems. Therefore it suits the best of requirements in the Cyber forensic investigations. For instance, it becomes extremely difficult to track the emails with the presence of proxies, Network address Translation Systems.

Payments Gateways take too long for transactions and cannot identify the fake transactions with the presence of proxies, Network address Translation Systems. This is where the significance of IPV 6 lies. The presence of service quality dimensions like the Scope identifier and zone identifier and EUI 64, enable IPV 6 to act as individual standalone unique IP address, which can be traced through the internet for email tracking, individual machines, payment gateways etc.

Voice overIP becomesan easier task and the data transfer can be vast with the help of IPV 6 technologies. Digital forensic technology IPV 6 does address the stores app information. With IPV 6, the Internet connectivity, Speed, Bandwidth prioritization, more secured systems can be witnessed.

Remote systems, non-local systems can validated through the next generation protocol IPV 6 technology. Communication tools like mobile communication, VSAT communication, each node of Internet resources can be tracked through IPV 6 technology.

LIMITATIONS

To implement IPV 6, transition technology is required. To enable this, the throughputs of Hardware are to be upgraded to maximize the efficiency.

Upgradations to be made in the Application, Software, and program sockets.

Inputs on the advanced level Training of IPV 6 will have to be imparted on technical experts involved in Network security system, Security systems. This may further add to the cost structure.

Therefore Telecommunication systems, Internet Service Providers, and Organizations dealing with upgradation of technology may have to incur cost in getting the systems in place.

FUTRUE SCOPE

For the IPV 6, the need is of the Transition technology, (which is used in the hardware). Only then IPV 6 can be termed as a standalone performer.
With change in Topology, and rerouting in wireless add hoc mode the address mobility can be worked out for further studies, privacy extension to auto configuration can be checked.

Framework of cyber forensic investigation can be modified &can be used in analyzing the email tracking, email spoofing, and fakeemail. This can be done with the help of IPv6technologies.

REFRENCES

1. Cisar, P[etar]; MaravicCisar, S[anja] &Bosnjak, S[asa] (2014). Cybercrime and Digital Forensics – Technologies and Approaches, Chapter 42 in DAAAM International Scientific Book 2014, pp.525-542, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-901509-98-8, ISSN 1726-9687, Vienna, Austria
DOI:10.2507/daaam.scibook.2014.42

2. Agarwal, A.; Gupta, M.; Gupta, S. & Gupta, S. (2011). Systematic Refined Digital Forensic Investigation Model, International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 1, pp. 118-132

3. Bulbul, H.I.; Yavuzcan, H.G. &Ozel, M. (2013). Digital forensics: An analytical crime scene procedure model (ACSPM), Forensic Science International, Volume 233, Issue 1-3, pp. 244-256

4. Ms.AtenaShiranzaei &Dr. RafiqulZaman Khan, A Comparative Study on IPv4 and IPv6 , "January 2015".
5. Joseph Davies , *Understanding IPv6 Third Edition* (Microsoft Press)
6. "Top 10 features that make IPv6 'greater' than IPv4," K. Das, IPv6.com , [Online] , Available: http://ipv6.com/articles/general/Top-10-Features- that-make-IPv6-greater-than-IPv4.htm [Accessed By 21 June 2014].
7. Silvia Hagen , IPv6 Essentials , O'Reilly Media, Inc. *IPv6 Essentials, Third Edition*.
8. C. E. Caicedo, J. B. D. Joshi, and S. R. Tuladhar. "IPv6 security challenges," IEEE Computer 42.2 ,2009: 36-42.
9. "Comparison of IPv4 and IPv6", ibm , [Online] 29 April 2007 , Available: http://www-01.ibm.com/support/knowledgecenter/ssw_ibm_i_72/ rzai2/rzai2compipv4ipv6.htm [Accessed By 21 June 2014].
10. "Introduction to IP version 6," Microsoft , [Online] September 2003 , Available: http://Www.Microsoft.Com/En-In/Download/ Details.Aspx?Id=21536 [Accessed By 6 August 2014].
11. "Internet Group Management Protocol (IGMP)," micosoft , [Online] 21 January 2005 , Available: http://technet.microsoft.com/en-us/library/cc787925(v=ws.10).aspx [Accessed By 21 June 2014].
12. S. Pachori .,"Ipv4 vs Ipv6 comparison ,"04 Feb 2013.
13. The future is forever,World IPv6 Launch, [Online] and Available://www.worldipv6launch.org/measurements/
14. Internet Society, [Online] and Available: http://www.internetsociety.org/ipv6/archive-2011-world-ipv6-day
15. The IPv6 Forum, The New Internet, [Online] and Available: http://www.ipv6forum.com

Author Profile

Mr.Rajkumar G Verma ,Currently working with Symbiosis International university,SIMS.He received his Bachelor of Computer Science, Bachelor of Education, Master in Computer Management Degree from Pune University, MBA from Chennai Board, Currently doing M.Tech level program from National Institute of Electronics & Information Technology (NIELIT).His research Interest includes Networking & Security, Computer Forensic ,Parallel & Distributed Computing ,Gesture Recognition, Computing,Sensor,Wireless Communications. Email ID: rajkumar.verma@live.com or rajoov@gmail.com