International Journal of Research

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

A Review of Ipv6: Feature and Importance

Anshul Patro
Student (B.Tech 8th sem) Department of Electronics And Computer Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email: anshulpatro@gmail.com

Vineet Kataria
Student (B.Tech 8th sem) Department of Electronics And Computer Engineering
Dronacharya College of Engineering, Gurgaon-123506, India
Email: k.vineet27@gmail.com

ABSTRACT

IPv6 is necessary for protocol design, simulating, improving network performance and building application. In this paper we describe the basic knowledge about the IPv6. Then, we analyze the features and the importance of IPv6. NAT is also described in this paper. IPv6 address space is so large that it's not possible to list every address for probing. This method lays a stable foundation for the succeeding probing program to improve efficiency, completeness and avoid redundancy. Tunnelling is the one of the best feature of IPv6. We propose the method of finding the tunnels based on IPv6 path MTU (maximum transfer unit) discovery mechanism to improve the veracity of the result.

Key points:
Internet Engineering Task Force (IETF); Subnetting Addressing; NAT (Network Address Translation);Tunnelling

INTRODUCTION:

Internet Protocol version 6 (IPv6) is the latest version of the Internet Protocol, the Communications Protocol that provides an identification and location system for computers on networks and routes traffic across the Internet .IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion.IPv6 is intended to replace IPv4 which still carries more than 96% of Internet Traffic. As of June 2014, the percentage of users reaching Google services with IPv6 surpassed 4% for the first time. Every device on the Internet is assigned an IP address for identification and location definition.[1] With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses than the IPv4 address space has available were necessary to connect new devices in the future. By 1998, the Internet Engineering Task Force (IETF) had formalized the successor protocol. Internet Protocol version 6, is a new addressing protocol designed to incorporate whole sort of requirement of future internet known to us as Internet version 2. This protocol as its predecessor IPv4, works on Network Layer (Layer-3). Along with its offering of enormous amount of logical address space, this protocol has ample of features which addresses today's shortcoming of IPv4.[2]

Why new IP version?

So far, IPv4 has proven itself as a robust routable addressing protocol and has served human being for decades on its best-effort-delivery mechanism. It was designed in early 80‟s and did not get any major change afterward. At the time of its birth, Internet was limited only to a few Universities for their research and to Department of Defence. IPv4 is 32 bits long which offers around 4,294,967,296 (232) addresses.[3] This address space was considered more than enough that time. Given below are major points which played key role in birth of IPv6:

Internet has grown exponentially and the address space allowed by IPv4 is saturating. There is a requirement of protocol which can satisfy the need of future Internet addresses which are expected to grow in an unexpected manner.

Using features such as NAT, has made the Internet discontiguous i.e. one part which belongs to intranet, primarily uses private IP addresses; which has to go through number of mechanism to reach the other part, the Internet, which is on public IP addresses.

IPv4 on its own does not provide any security feature which is vulnerable as data on Internet, which is a public domain, is never safe. Data has to be encrypted with some other security application before being sent on Internet.

Data prioritization in IPv4 is not up to date. Though IPv4 has few bits reserved for Type of Service or Quality of Service, but they do not provide much functionality.

IPv4 enabled clients can be configured manually or they need some address configuration mechanism. There exists no technique which can configure a device to have globally unique IP address.

Why not IPv5?

Till date, Internet Protocol has been recognized has IPv4 only. Version 0 to 3 used while the protocol was itself under development and experimental process. So, we can assume lots of background activities remain active before putting a protocol into production. Similarly, protocol version 5 was used while experimenting with stream protocol for internet. It is known to us as Internet Stream Protocol which used Internet Protocol number 5 to encapsulate its datagram. Though it was never brought into public use, but it was already used.[4]

Here is a table of IP version and their use:

DECIMAL	KEYWORD	VERSION
0-1		Reserved
2-3		Unassigned
4	IP	Internet Protocol
5	ST	ST Datagram Mode
6	IPv6	Internet Protocol Version 6
7	TP/IX	TP/IX :The Next Internet
8	PIP	The P Internet Protocol
9	TUBA	TUBA
10-14		Unassigned
15		Reserved

BLOCK DIAGRAM:

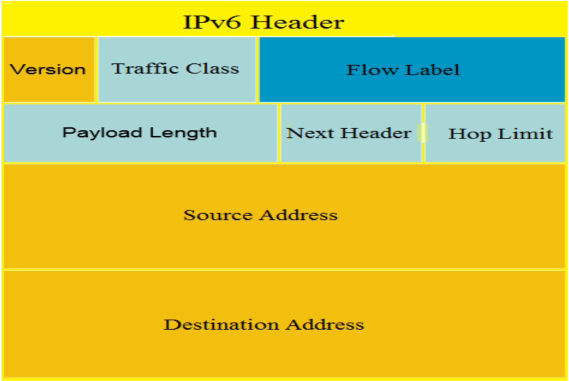


Fig 2. Block diagram of IPv6

IPv6 ADDRESS REPRESENTATION:

- 16 bit fields in case insensitive colon hexadecimal representation[5] 2031:0000:130F:0000:0000:09C0:876A :130B0
- Leading zeros in a field are optional: 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 represented as ::, but only once in an address: 2031:0:130F::9C0:876A:130B is ok 2031::130F::9C0:876A:130B is NOT ok

0:0:0:0:0:0:0:1 →:: 1 (loopback address) 0:0:0:0:0:0:0:0 →:: (unspecified address)

- IPv4-compatible (not used any more) 0:0:0:0:0:0:192.168.30.1 = ::192.168.30.1 = ::C0A8:1E01
- In a URL, it is enclosed in brackets (RFC3986) http://[2001:db8:4f3a::206:ae14]:8080/index.html Cumbersome for users Mostly for diagnostic purposes Use fully qualified domain names (FQDN)
- ⇒ The DNS has to work!!

Prefix Representation of prefix is same as for IPv4 CIDR Address and then prefix length
IPv4 address: 198.10.0.0/16

IPv6 address: 2001:db8:12::/40

IPv6 - FEATURES:

The successor of IPv4 is not designed to be backward compatible. Trying to keep the basic functionalities of IP addressing, IPv6 is redesigned entirely. It offers the following features:

- **Larger Address Space:** In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4×1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world.[6] According to an estimate, 1564 addresses can be allocated to every square meter of this earth.
- **Simplified Header:** IPv6‟s header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 providing the fact the IPv6 address is four times longer.
- **End-to-end Connectivity:** Every system now has unique IP address and can traverse through the internet without using NAT or other translating components. After IPv6 is fully implemented, every host can directly reach other host on the Internet, with some limitations involved like Firewall, Organisation’s policies, etc.[7]
- **Auto-configuration:** IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way absence of a DHCP server does not put halt on inter segment communication.
- **Faster Forwarding/Routing:** Simplified header puts all unnecessary information at the end of the header. All information in first part of the header is adequate for a Router to take routing decision thus making routing decision as quickly as looking at the mandatory header.
- **IPSec:** Initially it was decided for IPv6 to must have IPSec security, making it more secure than IPv4. This feature has now been made optional.
- **No Broadcast:** Ethernet/Token Ring is considered as broadcast network because they support Broadcasting, IPv6 does not have any Broadcast support anymore left with it. It uses multicast to communicate with multiple hosts.
- **Any cast Support:** This is another characteristic of IPv6. IPv6 has introduced any cast mode of packet routing. In this mode, multiple interfaces over the Internet are assigned same any cast IP address. Routers, while routing,

sends the packet to the nearest destination.

- **Mobility:** IPv6 was designed keeping mobility feature in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with same IP address. IPv6 mobility feature takes advantage of auto IP configuration and Extension headers.
- **Enhanced Priority support:** Where IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it. In IPv6, Traffic class and Flow label are used to tell underlying routers how to efficiently process the packet and route it.[8]
- **Smooth Transition:** Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This assures that mechanism to save IP addresses such as NAT is not required. So devices can send/receive data between each other, for example VoIP and/or any streaming media can be used much efficiently. Other fact is, the header is less loaded so routers can make forwarding decision and forward them as quickly as they arrive.
- **Extensibility:** One of major advantage of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options whereas options in IPv6 can be as much as the size of IPv6 packet itself.

IPv6 – COMMUNICATION:

In IPv4, a host which wants to communicate with some other host on the network, needs first to have an IP address acquired either by means of DHCP or by manual configuration. As soon as a host is equipped with some valid IP address, it is now able to speak to any host on the subnet.[9] To communicate on layer-3, a host also must know the IP address of the other host. Communication on a link is established by means of hardware embedded MAC Addresses. To know the MAC address of host whose IP address is known, a host sends ARP broadcast and in revert the intended host sends back its MAC address.

In IPv6, there’s no broadcast mechanism. It is not a must for an IPv6 enabled host to obtain IP address from DHCP or manually configured, but it can auto-configure its own IP. Then, how would a host communicates with others on IPv6 enabled network?

ARP has been replaced by ICMPv6 Neighbor Discovery Protocol.

Neighbor Discovery Protocol

A host in IPv6 network is capable of auto-configuring itself with a unique link-local address. As soon as it is equipped with an IPv6 address, it joins a number of multicast groups.[10] All communications related to that segment happens on those multicast addresses only. A host goes through a series of states in IPv6:

- Neighbor Solicitation: After configuring all IPv6‟s either manually, or by DHCP Server or by auto- configuration, the host sends a Neighbor Solicitation message out to FF02::1/16 multicast address for all its IPv6 addresses in order to know that no one else occupies same addresses.
- DAD (Duplicate Address Detection): When the host does not listen from anything from the segment regarding its Neighbor Solicitation message, it assumes that no duplicate address exists on the segment.
- Neighbor Advertisement: After assigning the addresses to its interfaces and making them up and running, the host once again sends out a Neighbor Advertisement message telling all other hosts on the segment, that it has assigned those IPv6 addresses to its interfaces.

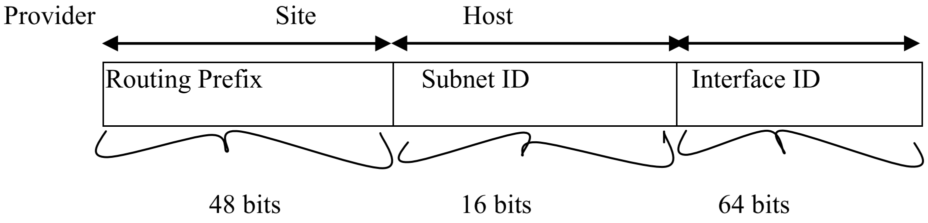
Once a host is done with the configuration of its IPv6 addresses, it does the following things:

- **Router Solicitation:** A host sends a Router Solicitation multicast packet (FF02:: 2/16) out on its segment to know the presence of any router on this segment. This helps the host to configure the router as its default gateway. If its default gateway router goes down, the host can shift to a new router and makes it the default gateway.[11]
- **Router Advertisement**: When a router receives a Router Solicitation message, it responses back to the host advertising its presence on that link.
- **Redirect:** This may be the situation where a Router receives a Router Solicitation request but it knows that it is not the best gateway for the host. In this situation, the router sends back a Redirect message telling the host that there is a better next-hop router available. Next-hop is where the host will send its data destined to a host which does not belong to the same segment.

IPv6 – SUBNETTING:

In IPv4, addresses were created in classes. Classful IPv4 addresses clearly define the bits used for network prefixes and the bits used for hosts on that network. To subnet in IPv4 we play with the default classful netmask which allows us to borrow hosts bit to be used as subnet bits. This results in multiple subnets but less hosts per subnet. That is, when we borrow host bit to create a subnet that costs us in lesser bit to be used for host addresses. [12]

IPv6 addresses uses 128 bits to represent an address which includes bits to be used for subnetting. Second half of the address (least significant 64 bits) is always used for Hosts only. Therefore, there is no compromise if we subnet the network.



16 Bits of subnet is equivalent to IPv4‟s Class B Network. Using these subnet bits an organization can have more 65 thousands of subnets which is by far, more than enough.

Thus routing prefix is /64 and host portion is 64 bits. We though, can further subnet the network beyond 16 bits of Subnet ID, borrowing hosts bit but it is recommended that 64 bits should always be used for hosts addresses because auto-configuration requires 64 bits. [13]

IPv6 subnetting works on the same concept as Variable Length Subnet Masking in IPv4.

/48 prefix can be allocated to an organization providing it the benefit of having up to /64 subnet prefixes, which is 65535 sub-networks, each having 264 hosts. A /64 prefix can be assigned to a point-to-point connection where there are only two hosts (or IPv6 enabled devices) on a link.

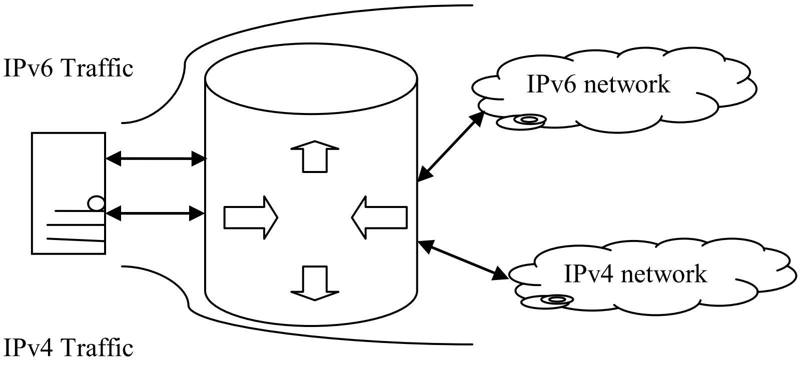
IPv6 – IPv4 to IPv6:

One problem in transition from IPv4 to IPv6 completely is that IPv6 is not backward compatible. This results in a situation where either a site is on IPv6 or it is not. Unlike an implementation of new technology where the newer one is backward compatible so the older system can still work with the newer without any additional changes.[14]

To overcome this short-coming, there exist few technologies which can be used in slow and smooth transition from IPv4 to IPv6:

Dual Stack Routers

A router can be installed with both IPv4 and IPv6 addresses configured on its interface pointing to the network of relevant IP scheme.



In above diagram, a Server which is having IPv4 as well as IPv6 address configured for it now can speak with all hosts on IPv4 network and IPv6 network with help of Dual Stack Router. Dual Stack Route can communicate with both networks and provides a medium for hosts to access Server without changing their respective IP version.

Tunnelling

In a scenario where different IP versions exist on intermediate path or transit network, tunnelling provides a better solution where user's data can pass through a non-supported IP version.

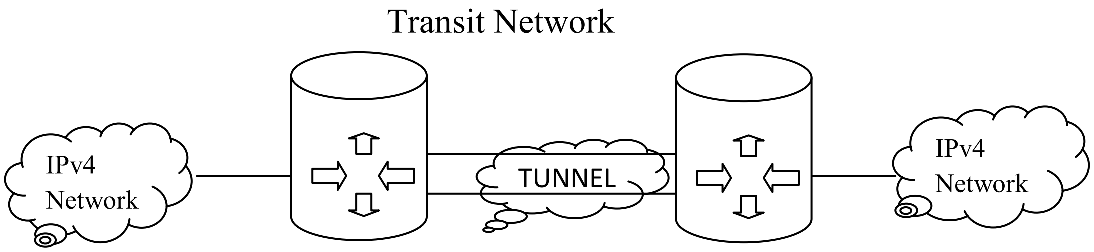


FIG: Tunnelling

The above diagram depicts how two remote IPv4 networks can communicate via Tunnel, where the transit network was on IPv6. Vice versa is also possible where transit network is on IPv6 and remote site which intends to communicate, are on IPv4.[15]

NAT Protocol Translation

This is another important method of transition to IPv6 by means of a NAT-PT (Network Address Translation – Protocol Translation) enabled device. With help of NAT-PT device, actual conversion happens between IPv4 and IPv6 packets and vice versa. See the diagram below:

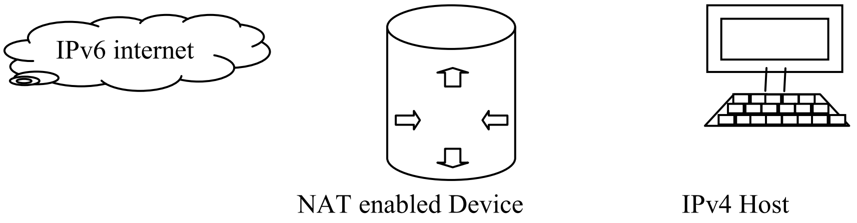


FIG: NAT - Protocol Translation

A host with IPv4 address sends a request to IPv6 enabled Server on Internet which does not understand IPv4 address. In this scenario, NAT-PT device can help them communicate. When IPv4 host sends a request packet to IPv6 Server, NAT-PT device/router, strips down the IPv4 packet, removes IPv4 header and adds IPv6 header and passes it through the Internet. When a response from IPv6 Server comes for IPv4 host, the router does vice versa

IPV6 – MOBILITY:

When a host is connected to one link or network, it acquires an IP address and all communication happens using that IP address on that link. As soon as, the same host changes its physical location, that is, moves into some different area / subnet / network / link, its IP address changes accordingly and all communication happening on the host using old IP addresses, goes down.

IPv6 mobility provides a mechanism which equips a host with an ability to roam around among different links without losing any communication/connection and its IP address.[16]

Multiple entities are involved in this technology:

- **Mobile Node:** The device which needs IPv6 mobility.
- **Home Link:** This link is configured with the home subnet prefix and this is where the Mobile IPv6 device gets its Home Address.
- **Home Address:** This is the address which Mobile Node acquires from Home Link. This is permanent address of Mobile Node. If the Mobile Node remains in the same Home Link, the communication among various entities happens as usual.
- **Home Agent:** This is a router which acts as registrar for Mobile Nodes. Home Agent is connected to Home Link and maintains information about all Mobile Nodes, their Home Addresses and their present IP addresses.
- **Foreign Link**: Any other Link which is not Mobile Node's Home Link.
- **Care-of Address**: When a Mobile Node attaches to a Foreign Link; it acquires a new IP address of that Foreign Link's subnet. Home Agent maintains the information of both Home Address and Care-of Address. Multiple Care-of addresses can be assigned to Mobile Node, but at any instance only one Care-of Address has binding with Home Address.
- **Correspondent Node:** Any IPv6 enable device which intends to have communication with Mobile Node.

IPV6 – ROUTING:

Routing concepts remain same in case of IPv6 but almost all routing protocol has been redefined accordingly. We have seen in Communication in IPv6 segment, how a host speaks to its gateway. Routing is a process to forward routable data choosing best route among several available routes or path to the destination. A router is a device which forwards data which is not explicitly destined to it.

There exist two forms of routing protocols :

- **Distance Vector Routing Protocol:** A router running distance vector protocol advertises its connected routes and learns new routes from its neighbors. The routing cost to reach a destination is calculated by means of hops between the source and destination. A Router generally relies on its neighbor for best path selection, also known as "routing-by-rumours". RIP and BGP are Distance Vector Protocols.
- **Link-State Routing Protocol:** This protocol acknowledges the state of a Link and advertises to its neighbors. Information about new links is learnt from peer routers. After all the routing information has been converged, Link-State Routing Protocol uses its own algorithm to calculate best path to all available links. OSPF and IS-IS are link state routing protocols and both uses Dijkstra's Shortest Path First algorithm. [17]

Routing protocols can be divided in two categories:

- **Interior Routing Protocol:** Protocols in this category are used within an Autonomous System or organization to distribute routes among all routers inside its boundary. Examples: RIP, OSPF.
- **Exterior Routing Protocol:** Whereas an Exterior Routing Protocol distributes routing information between two different Autonomous Systems or organization. Examples: BGP. Routing protocols
- **RIPng:** RIPng stands for Routing Information Protocol Next Generation. This is an Interior Routing Protocol and is a Distance Vector Protocol. RIPng has been upgraded to support IPv6.
- **OSPFv3**: Open Shortest Path First version 3 is an Interior Routing Protocol which is

modified to support IPv6. This is a Link-State Protocol and uses Dijkstra's Shortest Path First algorithm to calculate best path to all destinations.

- **BGPv4**: BGP stands for Border Gateway Protocol. It is the only open standard Exterior Gateway Protocol available. BGP is a Distance Vector protocol which takes Autonomous System as calculation metric, instead of number of routers as Hop. BGPv4 is an upgrade of BGP to support IPv6 routing.

Protocols changed to support IPv6:

- **ICMPv6:** Internet Control Message Protocol version 6 is an upgraded implementation of ICMP to accommodate IPv6 requirements. This protocol is used for diagnostic functions, error and information message, statistical purposes. ICMPv6‟s Neighbor Discovery Protocol replaces ARP and helps discover neighbor and routers on the link.
- **DHCPv6:** Dynamic Host Configuration Protocol version 6 is an implementation of DHCP. Though IPv6 enabled hosts do not require any DHCPv6 Server to acquire IP address as they can be auto-configured. Neither do they need DHCPv6 to locate DNS server because DNS can be discovered and configured via ICMPv6 Neighbor Discovery Protocol. Yet DHCPv6 Server can be used to provide this information.
- **DNS:** There has been no new version of DNS but it is now equipped with extensions to provide support for querying IPv6 addresses. A new AAAA (quad-A) record has been added to reply IPv6 query messages. Now DNS can reply with both IP versions (4 & 6) without any change in query format.[19]

FUTURE ASPECTS:

IPv6 enabled Internet version 2 will replace today IPv4 enabled Internet. When Internet was launched with IPv4, developed countries like US and Europe took the larger space of IPv4 for deployment of Internet in their respective countries keeping future need in mind. But Internet exploded everywhere reaching and connecting every country of the world increasing the 'requirement of IPv4 address space. As a result, till this day US and Europe have many IPv4 address space left with them and countries like India and China are bound to address their IP space requirement by means of deployment of IPv6. Most of the IPv6 deployment is being done outside US, Europe. India and China are moving forward to change their entire space to IPv6. China has announced a five year deployment plan named China Next Generation Internet.

After June 06, 2012 all major ISPs were shifted to IPv6 and rest of them are still moving.

IPv6 provides ample of address space and is designed to expand today Internet services. Feature-rich IPv6 enabled Internet version 2 may deliver more than expected.

REFRENCES:

[1.] "European IPv6 Task Force", IPv6 TF-SC Consortium, Workshop Industry Focus, Paris, June, 27-28, 2006.

[2.] IPv6 Task Force Editorial Group, "Main Task force Report", Version 1.76, Document no.70, 11.2.2002.

[3.] Geoff Huston, APNIC, "IPv4 Address Depletion and Transition to IPv6", Internet Protocol Journal, Vol. 10, No. 3, pp. 18-28, 2007.

[4.] Geoff Huston, Telstra, "IPv4: How long do we have?⋯", Internet Protocol Journal, Vol. 6, No. 4, pp. 2-15, 2003.

[5.] Gregory R. Schloz, Clint Evans, Jaime Flores, Mustafa Rahman, "Internet protocol version 6", Internet Protocol Journal, Vol. 16, Issue 3, pp. 197 - 204, March 2001.

[6.] R. Droms, "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[7.] R. Droms et al., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)," RFC 3315, July 2003.

[8.] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, Dec. 1998.

[9.] Dongkeun Lee, Jaepil Yoo, Keecheon Kim, Kyunglim Kang, "IPv6 Stateless Address Auto-configuration in Mobile Ad-hoc Network (T-DAD) and Performance Evaluation", ACM

Proceedings of the 2nd ACM international workshop on Performance evaluation of wireless ad hoc, sensor, and ubiquitous networks (PE-WASUN'05), pp. 271-272, Oct 2005, ISBN:1-59593-182-1, Montreal, Quebec, Canada.

[10.] Mesut Gunes, Jorg Reibel, "An IP Address Configuration Algorithm for Zeroconf. Mobile Multi-hop Ad-Hoc Networks", Proceedings of the International workshop on Broadband wireless Adhoc networks and services, Sophia Antipolis, France, September 2002.

[11.] David C. Plummer, "An Ethernet Address Resolution Protocol", RFC 826, November 1982.

[12.] Jari Arkko, Tuomas Aura, James Kempf, Vesa-Matti Mäntylä, Pekka Nikander, Michael Roe, "Securing IPv6 Neighbor and Router Discovery", Proceedings of the first ACM Workshop on Wireless Security pp. 77-86, 2002. San Diego, CA, USA

[13.] Hao Chen and Ljiljana Trajkovic, "Simulation of Route Optimization in Mobile IP", IEEE Proceedings of the 27th Annual IEEE Conference on Local Computer Networks LCN 2002, pp. 847 - 848, 2002. DOI: 10.1109/LCN.2002.1181379. 6-8 November 2002, Tampa, FL, USA.

[14.] Jiann-Liang Chen, Yu-Feng Lee and Yao-Chung Chang, "Mobile IPv6 network: implementation and application", International Journal of Network Management, Volume 16, Issue 1, pp. 29-43, DOI:10.1002/nem.586.

[15.] Tuomas Aura, Cryptographically Generated Addresses (CGA)", IETF Securing Neighbor Discovery WG, internet draft, June 2003, http://tools.ietf. org/html/draft-ietf-send-cga-00.

[16.] R. Hinden, S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[17.] J. Postel, "Domain Name System Structure and Delegation", RFC 1591, Mar-1994

[18.] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661, July 1994.

[19.] Davies, J., "Understanding IPv6", Microsoft Press, Redmond, WA, 2003.