International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org Volume 2 Issue 3 ǁ March. 2013 ǁ PP.23-28

A Survey of Next generation Internet Protocol version 6

[1]K.Senthil Kumar, [2]S.RathinaGowri

[1,2]M.E. Computer Science and Engineering, Anna University
Paavai Engineering College, Pachal, TamilNadu, India

ABSTRACT: *This paper highlights the upgraded features, addressing methods, transition techniques of next generation Internet Protocol version 6 after performing a detailed survey.*

Keywords: *internet protocol, address space,routing, IPsec, transition*

I. INTRODUCTION

Internet Protocol Version6 is introduced due to the depletion of all internet protocol version4 addresses.IPV4 uses 32-bit addresses that allows 2^{32} unique addresses worldwide where as IPv6 uses 128-bit addresses, allowing for 2^{128} unique addresses that is 340 trillion trilliontrillion (or 340,000,000,000,000,000,000,000,000,000,000,000,000) addresses assuring that ipv6 will never run out of addresses in future. Apart from large address space in ipv6, other features are included in this version which enhances better QoS, security, extensibility, mobility, routing capabilities etc.,

II. IPV6 ADDRESSING

A. Hexadecimal Notation

128-bit IPv6 addresses are represented by splitting them up into eight 16-bit segments. Each segment is written in hexadecimal between 0000 and FFFF, separated by colon. Ex: 2001:0000:130F:0000:0000:09C0:876A:130B

B. Address Compaction

Leading zeroes in a segment can be compacted. All zeroes in one or more segments can be represented with a double colon (::). Double colons can be used only once. IPv4 Embedded in IPv6 addresses are represented with dotted decimal.

C. Prefix Representation

CIDR notation can be used to specify prefix length. ex:2001:CB8E:2A::/64 is network.,2001:3F0E:102A::/48.,2001:10C2:43EE:D0C:F::C14/126.,2001:3F03:102A:3010:20::/75

D. Address Allocation

Internet Assigned Numbers Authority(IANA) allots IPv6 address space to Regional Internet Registries (RIRs).ISPs get address space from the RIRs. Enterprises get their IPv6 address space from their ISP. The allocation process is as follows. The IANA has allocated 2001::/16 for initial IPv6 unicast use. Each registry gets /23 prefixes from the IANA. Registry allocates a /32 prefix to an IPv6 ISP. An ISP allocates a /48 prefix to each end customer.

E. Address Scope

IPv6 addresses are denoted with scope value. The packets cannot be sent beyond a specified scope.

1) Interface-local:The scope of this address spans for its own interface. The loopback address of unicast type is an example for Interface-local scope.
2) Link-local:The scope of Link-Local address spans within the link. The destination node must exist within the same link.
3) Subnet-local:The scope of Subnet-Local address spans within the subnet of multiple links.
4) Admin-local:The scope of this address is configured by the admin.
5) Site-local:The scope of the Site-Local address spans across multiple links connected within the same site.
6) Organization-local:The scope of the organization-local address spans across multiple sites within an organization.
7) Global:The scope of this address spans across entire internet.

F. Address Types

The IPv6 addresses are categorized in to three types. They are Unicast, Multicast, Anycast.

1) *Unicast:*The Unicast address is used to send a packet to a single interface in a network. The types of Unicast addresses are as follows.

- Unspecified 00..0 (128 bits) ::/128
- Loopback 00..1 (128 bits) ::1/128
- Link Local Unicast 1111 1110 10 FE80::/10
- Site-Local Unicast fec0::/10
- IPv4-mapped IPv6 address ::FFFF:a.b.c.d
- IPv4-compatible IPv6 address ::a.b.c.d
- Aggregatable global unicast address 2000::/3

2) *Multicast:*The Multicast address is used to send a packet to multiple interfaces in a network. Multicast address is denoted by Multicast 1111 1111 FF00::/8.

3) *Anycast:*The Anycast address is used to send a packet to multiple interfaces in a network and the one nearest will be the destination node.

G. Interface ID

The last 64 bits of the IPv6 address is represented by interface id. The interface id is unique to link and used to identify a particular interface in a link. This ID can be generated by different methods. It can be configured automatically from a 64-bit EUI-64 or by expanding 48-bit MAC address or by automatically generating a pseudo-random number or by manually configured via DHCP.

III. IPV6 HEADER

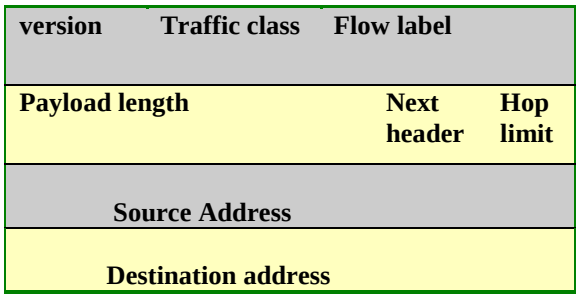

Fig 1: IPv6 Header Format

A. Version (4 bits)

This field indicates the internet protocol version which is 6 and denoted with binary value 0110.

B. Traffic Class (8 bits)

The Traffic class field holds 8 bits that indicates the priority in which a packet must be routed in a network and packet priority value is assigned by the source node.

C. Flow label (20 bits)

This 20-bit is used to indicate packets with same flow and all the ipv6 routers handles all the packets with same flow in a similar way to ensure Quality of Service.

D. Payload length (16 bits)

This field indicates the length of payload. It also includes length of extension header if present.

E. Next Header (8-bits)

This field identifies the transport layer protocol used by the next header and ipv6 provides an extension header for a packet to do specific task and this detail is also added as option in this field.

F. Hop limit (8 bits)

This field is used to denote the number of hops that the packets are limited to travel. When a packet undergone the number of hops denoted, it is dropped. The packets cannot travel not more hops than specified in this filed.

G. Source Address (128 bits)

This is the 128-bit IP address of the node where the packet first originated.

H. Destination Address (128 bits)

This is the 128-bit IP address of the node where the packet finally has to reach.

IV. ICMPV6

Internet Control Message Protocol version 6 (ICMPv6) is the upgraded version of ICMP for Internet Protocol Version6.The ICMPv6 combines the activities of three main protocols ICMP (Internet Control Message Protocol version), IGMP (Internet Group Membership Protocol), and ARP (Address Resolution Protocol).Hence it becomes a multipurpose protocol performs various tasks that includes error diagnostics and error reporting, neighbor discovery, reporting multicast memberships.

A. ICMPV6 HEADER

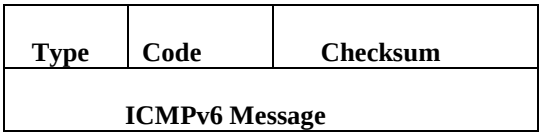

Fig 2: ICMPv6 Header Format

1) Type (8 bits):The Type field indicates the type of message and the value determines which type of error or information message.
2) Code (8 bits):The value of the code depends on the type of message and its value gives additional precise information about the message.
3) Checksum (16 bits):This field is used for the error detection purpose.
4) ICMPv6 Message (32 bits):ICMPv6 messages are categorized in to Error messages and Information messages. Information message includes two of icmpv6 messages, Neighbor discovery messages, and Group membership messages.

Error Message includes Destination-Unreachable Message, Packet-Too-Big Message, Time-Exceeded Message, and Parameter-Problem Message

Type	Meaning
1	Destination Unreachable
2	Time Exceeded
3	Packet Too Big
4	Parameter Problems

Information message includes two of icmpv6 messages. They are Echo-Request Message and Echo-Reply Message. Neighbor Discovery Messages includes Router-Solicitation Message, Router-Advertisement Message, Neighbor-Solicitation Message, Neighbor-Advertisement Message, Redirection Message, Inverse-Neighbor-Solicitation Message, and Inverse-Neighbor-Advertisement Message.Group membership messages includes Group Membership Query, Group Membership Report, Group Membership Reduction

Type	Meaning
128	Echo Request
129	Echo Reply
130	Group Membership Query
131	Group Membership Report
132	Group Membership Reduction
133	Router Solicitation
134	Router Advertisement
135	Neighbor Solicitation
136	Neighbor Advertisement
137	Redirect

V. NEIGHBOR DISCOVERY PROTOCOL

Neighbor Discovery Protocol is introduced in the internet protocol version6. It has following functions. Router discovery, Prefix discovery, Parameter discovery, Address auto configuration, Address resolution, Next-hop determination, Neighborun reachability detection, Duplicate address detection (DAD), Redirection.

It makes use of ICMPv6 neighbor discovery messages such as Router-Solicitation Message, Router-Advertisement Message, Neighbor-Solicitation Message, Neighbor-Advertisement Message, Redirection Message, Inverse-Neighbor-Solicitation Message, and Inverse-Neighbor-Advertisement Message.

A. *Neighbor Discovery Functions*

1) Router discovery:The host automatically locates the router with the help of icmpv6 information messages such as Router Solicitation and Router Advertisement. During Router solicitation, the host after allotted to a certain network multicast router solicitation message to all routers in that network. The router in turn responds by advertising with its address.
2) Prefix discovery:The host can get all reachable prefix information during router advertisements so that all the traffic can directly be sent to destination without forwarding to router.
3) Parameter discovery:The router advertisement also includes the maximum transmission unit (MTU) and the default hop limit values for the host to send packets accordingly.
4) Address auto configuration:The host can automatically generate a stateless address by combining the EUI-64 of the interface with the prefix learned from prefix discovery method.
5) Address resolution: The host makes use Neighbor-Solicitation and Neighbor-Advertisement Messages to discover neighbor's link layer address. The host multicasts a neighbor solicitation and the neighbor respond with link layer address during neighbor advertisement.
6) Next-hop determination: When the destination does not come under local link, the host determines which router it must take to reach destination. Once the next hop is found it is stored in destination cache. This destination cache maintains information about recent device's next hop, destination address and interface identifier.
7) Neighborunreachability detection: Here the neighbor node is checked for its reachability using neighbor solicitation message. When a neighbor advertisement is got from the desired node, the node is reachable else unreachable. Its entry is then removed from neighbor cache.
8) Duplicate Address Detection (DAD): The host ensures that the address assigned by it does not exist to other node in the same link. So it sends a neighbor solicitation and gets back neighbor advertisement. When the same address is found, the host changes its own assumed address.
9) Redirection: In this process, the router sends a redirection message to the host to take up the most preferable hop.

VI. MULTICAST LISTENER DISCOVERY MLD

The Multicast Listener Discovery protocol is introduced for the multicast transmission in IPV6 network. MLD protocol uses ICMPv6 information messages such as Group Membership Query, Group Membership Report, and Group Membership Reduction for managing multicast function.

Multicast router can send either general query to all multicast listener's addresses with Maximum Response Delay unit or a specific query for a particular group of multicast listeners.

The router uses general query message to discover multicast listeners in the network. The multicast nodes respond by sending report message to the multicast router. When the multicast node decides not to receive multicast packets, acknowledge the multicast router by MLD done message and can leave the group.

VII. IPV6 ROUTING

The Routing types in IPv6 are similar to that of the IPv4 but with slight upgradation in the protocols used for routing. The protocols used in IPv6 routing are RIPv6, OSPFv6, IDRPv2, EIGRP and Dual IS-IS.

These protocols are upgraded for the purpose of supporting the 128-bit address of IPv6 with slight modifications done in their functionalities. For instance, RIPv6 is similar to the previous version of RIP but it is modified to support 128-bit address and provide integrated routing that supports simultaneously both ipv4 and ipv6 routing. It is used to get information about the route or any changes in route.

OSPFv6 or OSPFv3 are same and modified to support 128-bit address type as well as removed authentication function, since it is carried out by security features of IPv6. It is used to determine the cost of each route. Whereas IDRPv2 and EIGRP are modified to allow multiprotocol routing.

VIII. IPV6 SECURITY

The IPsec feature is widely adopted in IPv4 as an optional thing. Whereas in IPv6, IPsec feature is inbuilt in it. The IPsec features includes authentication to ensure the data got from an original node using shared keys and digital certificates. The data sent is encrypted and hence they are decrypted only in the destination node with the help of shared keys. Hence confidentiality is maintained. Further Data integrity is maintained by comparing checksums.

IX. TRANSITION METHODS

Internet Protocol version 4 and Internet Protocol version 6 are not compatible with each other which means they cannot communicate with each other. It takes some time to convert all the nodes and devices related to a network from internet protocol version 4 to version 6. In order not to disturb the data transmission in the ipv6 deployment process, both the protocols ipv4 and ipv6 must co-exist in the same node. Several transition mechanisms are proposed to act with both versions of protocols simultaneously. The transition mechanisms come under three categories. They are Dual Stack, Tunnelling, and Translation.

There are two mechanisms in which packets can be sent they are IPv4 over IPv6 and IPv6 over IPv4. Dual Stack technique comes under IPv4 over IPv6 mechanism and Tunnelling techniques comes under IPv6 over IPv4 mechanism.

A. Dual Stack

It is the simple and flexible transition technique in which all the nodes, routers, switches are made compatible with both IPv4 and IPv6 protocols. The IPv4 and IPv6 functionalities co-exist in same node as dual IP layer. When IPv4 packet approaches the host it is accessed by the IPv4 part of the stack and when IPv6 packet is to be accessed, it is dealt by the IPv6 part of the stack. Dual stack method is widely used by IPv6 network to access the IPv4 hosts. Dual stack method requires all the network devices to support both the versions of internet protocols 4 and 6. Hence the resource requirements doubles and when some devices not compatible with both versions ipv4 and ipv6 some other techniques can be used. But Dual stack technique is widely preferred for immediate and easy transition in big enterprises.

B. Tunnelling

Tunnelling is the process of sending an ipv6 packet by encapsulating it in to an ipv4 packet. When an IPv4 host does not support dual stack architecture and when such host needs to communicate with the IPv6 network, tunnelling method can be used. Then IPv6 packets are encapsulated in IPv4 packets and sent to the desired IPv4 nodes. Tunnelling can be limited up to certain distances such as router-to-router, host-to-router, host-to-host, and router-to-host.

Tunnelling can be implemented either as automatic tunnelling or configured tunnelling. In automatic tunnelling, connection is automatically established between an IPv6 and IPv4 network. The embedded IPv6 address gives all the necessary information about destination IPv4 network for which packets are to be sent. Whereas in configured tunnels the destination address is manually assigned. They are also called automated tunnels.

The tunnelling types includes 6 to 4, IPv6 Tunnel brokers, Teredo, ISATAP

1) 6 to 4:In this technique, the two IPv6 hosts can communicate with each other through an IPv4 network. This is possible by embedding ipv4 destination address in the ipv6 address. This comes under automatic tunnelling technique.
2) Tunnel brokers:In this technique, the two IPv6 hosts can communicate with each other through an IPv4 network by a service called tunnel broker. An encapsulated path established in existing network that carries ipv6 packets within the ipv4 packets over ipv4 network to an ipv6 destination.
3) Teredo:This technique is mainly used to send ipv6 packets to a host behind an ipv4 NAT. The host that sends ipv6 packets is considered as teredo client and the packets are sent as ipv4 UDP message to NAT ipv4 to reach ipv6 host. The NAT must support UDP port translation.
4) ISATAP:Intra-Site Automatic Tunnel Addressing Protocol which is used to automatically configure a tunnel and to send ipv6 packets encapsulated within ipv4 packet over an ipv4 network trough an ISATAP router to another ipv6 node. The ISATAP router must have a dual stack.

C. Translation

When there exists a network that support only IPv4 transmission and a network that support only IPv6 transmission, a packet from IPv4 only network can be sent to ipv6 only network by a technique called Translation. In this technique IPv4 address can be translated to IPv6 address and IPv6 address in to IPv4 address. There are two kinds of translations possible they are NAT-PT (Network Address Translation- Protocol Translation) and NAT64. Since NAT-PT technique makes use of Application level Gateways for the protocol translation, there occur a delay in inspecting each packets and translating them. So, other method NAT64 is widely used. In this method, IPv6 embeds the ipv4 address of a destination node and in NAT64, address mapping is done. Then the packets are sent to the desired node.

X. CONCLUSIONS

The next generation Internet Protocol version 6 has come up with a huge address space that never come to extinction. Many upgraded features will give added benefitsin terms of reliability security and management etc. There are so many ongoing researches in the area of transition and deployment of IPv6. This paper gives an overview of all the features modified in the IPv6.

ACKNOWLEDGMENT

A sincere gratitude expressed to the anonymous reviewers for providing some useful suggestions.

REFERENCES

[1]. [RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X.Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.
[2]. [RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.
[3]. [RFC6146] Bagnulo, M., Matthews, P., and I. Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.
[4]. [RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. Beijnum,"DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.
[5]. [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
[6]. [RFC1466] Gerich, E., "Guidelines for Management of IP Address Space", RFC 1466, Merit Network, Inc., May 1993.
[7]. [RFC1518] Rekhter, Y., and T. Li, "An Architecture for IP Address Allocation with CIDR", RFC 1518, September 1993.
[8]. [RFC1519] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy", RFC 1519, September 1993.
[9]. [RFC2765] Nordmark, E., "Stateless IP/ICMP Translation Algorithm (SIIT)", RFC 2765, February 2000.
[10]. [RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
[11]. [RFC3056] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.
[12]. [RFC3089] Kitamura, H., "A SOCKS-based IPv6/IPv4 Gateway Mechanism", RFC 3089, April 2001.
[13]. [RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005.
[14]. [RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.
[15]. [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
[16]. [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.
[17]. [RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.
[18]. [RFC4966] Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.
[19]. [RFC5211] Curran, J., "An Internet Transition Plan", RFC 5211, July 2008.
[20]. [RFC5214] Templin, F., Gleeson, T., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, March 2008.
[21]. http://tools.ietf.org/html/rfc
a. http://tools.ietf.org/html/rfc614