ICTN 6885: Network Management Technology

Final Term Paper

Professor's Name: Dr. John Pickard

Student's Name: Rahul Ravella

Date: 4/6/2015

Table of Contents

Abstract

IPv6 has almost become a requirement for industries as well as end users. With the exhaustion of all the IPv4 addresses and the growth of number of devices the need has finally come. This paper will talk about the advantages of IPv6, its features compared to IPv4, the different headers it has and how they work. The paper will also talk about DHCPv6 as well as IPv6 auto-configuration, their features and how they are configured and work. These features should provide an idea on the advantages of IPv6 and provide an insight to companies and businesses to make the move towards it.

Introduction

Through the increase in the growth of the internet after it become more commercialized, a need had arisen for the implementation of an addressing method that provided more IP addresses than the then IPv4. While IPv4 could only provide 4.3 billion addresses with a 32 bit address, the IPv6 with its 128 bit addresses would allow for 3.4×10^{38} addresses. With the increase in the quantity of devices that connect with the internet such as smartphones, TVs, watches, the need for IPv6 has grown more now than ever. IPv6 provides a lot of new features that IPv4 couldn't possible have. These features and more will be discussed in the paper. (Knights, 2007)

Features of IPv6

A few of the features that important in IPv6 are:

New Header format:

The new header format in IPv6 was constructed in such a way as to minimize the overhead that is created. This was done by moving the option fields and the nonessential fields in to the extension headers which are located at the end of the header. This allows for a smoother and a more streamlined processing when it comes to routing between the intermediate routers. It helps to provide better support during real-time traffic.

Both the IPv6 and IPv4 headers are not compatible with each other as the protocol of IPv6 is not backward compatible with the protocol of IPv4. To process both the header formats, a router or a host needs to implement both IPv4 and IPv6. The address of IPv6 is four times as big as the addresses of IPv4 but the header of IPv6 is only two times as large as the header of the IPv4. (Microsoft, 2005) (Microsoft, 2005)

Bigger address space:

It has already established that IPv6 has 128 bit source and destination addresses. This allows for 3.4×10^{38} addresses. The larger number of addresses is not the only advantage for having a bigger address space. It also helps by allowing multiple levels of subnetting and the allocation of addresses from the subnets in the organization to the backbone of the internet.

Only a small part of the vast number of addresses have been allocated for the use by hosts while the majority are available for the future use when they are required. Another advantage for such a large number of addresses is that techniques such as address conversion i.e, NAT etc may not be necessary in the future when the world changes completely to IPv6. (Microsoft, 2005)

More efficient Packet Processing:

Through the more simplified packet header, the processing of the packets becomes more efficient. While IPv4 had IP level checksum, the IPv6 doesn't which eliminates the need for the recalculation of the checksum at every hop router. This was achieved through the concept that

technologies involving linked layer already have the control aswell as checksum capabilities built in. (Network Computing, 2011)

Hierarchical addressing routing infrastructure:

The global addresses of IPv6 used on the internet were created in such a way as to provide efficient and hierarchical routing infrastructure which deals with the multiple levels of the ISPs. The routers on the backbone have a smaller routing table in the IPv6 compared to that of the IPv4 internet. (Microsoft, 2005)

Stateful and Stateless address configuration

The process of host configuration has become simpler since the IPv6 provides support for the stateful address configuration which deals with the configuration of addresses when the DHCP server is present, and the stateless address configuration which deals with the configuration of addresses when the DHCP server is not present. In the stateless address configuration, the devices and the hosts can automatically configure themselves for the link through the addresses that are obtained from the local routers. The hosts can configure themselves automatically without a router through the link local addresses and start communication without the need to do any configuration manually. (Microsoft, 2005)

Security:

The best way to provide some kind of security for IPv4 was to implement NAT and NAPT which caused a lot of issues regarding communication between end to end nodes. IPsec provides integrity, authenticity and confidentiality and is integrated into IPv6. While the IPv4 ICMP packets can carry potential malware, firewalls in companies block them. In the case of ICMPv6, these packets are permitted in because of the implementation of the IPsec in the packets of IPv6.The IPsec provides interoperability between the various implementations of the IPv6. (Network Computing, 2011) (Microsoft, 2005)

Better quality of service than IPv4:

With the introduction of a new field in the IPv6 called the Flow Label, the IPv6 was given a boost in the QoS. The field helps in defining how some packets are identified and guided by the routers. Since the movement of the packets from the source to the destination is defined in the header of the IPv6, the QoS support can be obtained even though the packet has an IPSec encryption. The delivery of information without the possibility that the data has been modified or intercepted by systems give IPv6 a high level of QoS which can help in applications such as VOIP and other peer to peer applications. (Das, 2015) (Microsoft, 2005)

Neighboring node interaction:

A new protocol has been made for the IPv6 called the Neighbor Discovery Protocol for the ICMPv6 which manages the relationship between the neighboring nodes. It is a mechanism that looks for packets of NS/NA in the network to check whether changes have been made in the MAC and IP pairings. The protocol is efficient enough that it replaces the Address Resolution Protocol (ARP), ICMPv4 Redirect and Router Discovery through the use of unicast and

multicast messages while providing more functionality. (Microsoft, 2005) (Barbhuiya, Biswas, & Nandi, 2011)

Extensibility:

When there is a need, new features can be added through the extension headers which are located at the end of the IPv6 header. While the IPv4 could only handle 40 bytes for the options, the IPv6 extension header can handle as many bytes as the size of the IPv6 packet. (Microsoft, 2005) (Richard & Malone, 2005)

Better Mobility features:

Mobility support is mandatory in the IPv6 to give seamless handover services to the devices that are mobile. To provide this feature, the IETF had suggested protocols such as the MIPv6 (Mobile IPv6), FMIPv6 (Fast Mobile IPv6) and HMIPv6 (Hierarchical Mobile IPv6). Because of such a large address space of IPv6, every mobile device can potentially have an IP address for itself and with the help of the extension headers of MIPv6, route optimizations between different mobile nodes can be possible when moving between different networks in 3G. (Das, 2015) (Yousaf, Muller, & Wietfeld, 2010)

Three Types of Addresses used in IPv6

IPv6 has three main addressing types. They are unicast, multicast and anycast.

Unicast:

The unicast address type in the IPv6 operates similar to that of IPv4. The unicast addressing mode is also called the aggregatable global unicast address. The unicast address sends data from the any one particular source to any one particular destination. The unicast addressing type is one of the most commonly used as most of the traffic these days come move from one point and end up at one destination. This concept might change in the near future when more people start using video services and VoIP.

There are four types of addresses that work under unicast:

- Global unicast: These addresses are conventional and publically routable similar to that of IPv4 addresses.
- Link-local addresses are meant for the private and addresses that are not routable in IPv4. These addresses have not been designed to perform routing but rather mean to stay in a single network segment.
- Unique local addresses, similar to link local addresses are for private addressing. The main difference is that they are unique and when joining two subnets, they will not cause any collision of addresses.

- Special addresses: These addresses are loopback addresses. (Wilkins, 2011) (Schroder, 2006)

Multicast:

The IPv6 multicast address has the same functionality similar to that of the IPv4 broadcast address type. Here, data is sent from one location to multiple devices with different destinations. If the data had to be sent to these different devices through unicast, a separate session with a new process would need to be created for each device causing large amounts of delays and heavy traffic.

One main difference between them is that the multicast in the IPv6 would send the packets only to those devices that are in the multicast group instead of sending the packets to all the devices on the segment causing a lot of network overhead in a large network causing broadcast storms. The packets will not be forwarded if the device is not in a multicast group. (Wilkins, 2011) (Schroder, 2006)

Anycast:

The main difference between IPv6 and IPv4 come under the anycast address type. The concept of anycast was proposed to be implemented in IPv4 but it never took off. In this type of addressing type, the packet is sent to the closest device that is available. When implementing this address type, the devices are provided with the same anycast address and the protocol will automatically calculate the closest path to the source and route the traffic to that particular device. The advantages of this addressing type is that it can provide automatic failover and load balancing capabilities. Since the IPv6 protocol will take care of the packet reaching its final destination, it becomes very simple to administer compared to that of the unicast addressing type. (Wilkins, 2011) (Schroder, 2006)

Extension Headers of IPv6

One of the advantages of the IPv6 is that it has a better and more improved options mechanism than the IPv4. The options header is located between the upper-layer protocol header and the fixed header between the IPv6 header and the transport layer header in the packet. Majority of the headers of the IPv6 are not looked at or undergo processing till the packet arrives at the final location. They are not processed by any of the routers that are located in the path of the packet. This provides a very big performance improvement over IPv4 as all the options are checked in IPv4 causing delays and situations leading to bottle necks.

The options field in IPv6 can be of any length compared to the fixed length of the IPv4. The options that can be carried by a packet is not confined to the 40 byte limit. The way these options are used can provide better functionality that were not possible in IPv4. (Oracle, 2010)

Following are the extension headers that are present in IPv6:

- Authentication Header
- Fragmentation Header
- Encapsulation Header
- Routing Header
- Destination Options
- Hop by Hop options
- Mobility header
- Basic IPv6 Header

Authentication header:

The header of the IPv6 is related to the arrangement that is being used in the IPv4 authentication header. It is placed in the datagram as an extension header. The header is linked to previous header and puts the values of the assigned value for the authentication header into the Next Header field. The authentication header is located in the IP header and comes before the Destination Options header when the header is in the transport mode. (Kozierok, 2005). The header provides data integrity, data authentication and anti replay protection for the packets of IPv6. The header doesn't have the capability to provide data confidentiality services but it can be achieved by pairing it with the Encapsulation Security Payload header. (Microsoft, 2005)

Fragmentation header:

The main feature of the fragment header is that it provides the information that is required to allow the fragments to be reassembled (Kozierok, 2005). The Next header field is included along with the Fragment offset field, a more fragments flag and an identification field. Payloads from the only the source nodes can be fragmented. On the chance that the payload is larger, the payload is fragmented and the fragment header is used to rejoin the fragments. (Microsoft, 2005)

Encapsulation header:

Unlike the authentication header which provides data integrity and authentication services for the whole packet of the IPv6, the Encapsulation header provides data authentication, confidentiality and integrity the payload that is encapsulated. The header has in it the Security Parameters Index that identifies the sequence number field and the IPSec which provides protection from anti replay. (Microsoft, 2005)

Routing header:

The routing header works similar to the loose source routing that is present in IPv4, the header provides a list of the destinations that are close to the host so that the packets can find a path to reach the final destination. The routing header consists of the Next header, Header extension length, Routing type and Segments left fields. (Microsoft, 2005)

Hop by Hop Options header:

The hop by hop extension header provides support for Jumbo-grams and when combined with the Router Alert option, it becomes the main part of the functioning of Multicast Listener Discovery. It also plays an important part in the functioning of the IPv6 multicast through MLD and RSVP. (Cisco Systems, 2006)

Destination Options:

The Destination options header provides the parameters that are required for delivering packets to destinations that are intermediately located or the end destination. The fields in the header are similar to that are present in the Hop-by-Hop header. The header is used in the following ways:

- In the presence of the routing header, the destination header gives the processing or the delivery option at each of the nearby destinations.
- The destination header provides the processing or the delivery options at the end destination. (Microsoft, 2005) (Shiyao, Wang, & Xu, 2010)

Mobility header:

The mobility provides services for mobile IPv6. The header is dedicated to moving mobility messages. The extension header contains the payload protocol field and by default is set to 59 to show that the header is the last one in any packet. The MH type field provides the information on the type of mobility message that is being sent. The mobility message is stored in the Message Data field. (Microsoft, 2005)

DHCPv6

The dynamic host control protocol is the protocol that allows computers, servers and other devices with network capabilities to get an IP address as well as the IP address of the DNS server and the gateway address. The DHCP provides more reliable IP address configuration as well as a reduced network administration.

With the introduction of the IPv6, there was a need to make a new protocol which would update the current DHCP as IPv4 DHCP could not provide the auto configuration of IPv6 addresses on the devices. That's when the DHCPv6 was released. Following are some of the differences between DHCPv6 and the DHCP in IPv4:

- No baggage: The previous DHCP used to run on a protocol called BOOTP. The layout of the packet had a lot of waste where many of the options were not as useful as they could be. A lot of implementations needed to be done which would help tweak the DHCP to be compatible with clients that were buggy. The DHCPv6 doesn't have this issue.
- DHCPv6 Multicast: The DHCPv6 servers that are registered in the multicast can send the DHCP configuration to only those devices that need it unlike the IPv4 DHCP which

sends a broadcast of the DHCP to all the devices on the network, not knowing when to stop.

- Network Administration: The DHCPv6 provides better and easier network administration compared to DHCP on IPv4.
- A single exchange is enough to provide the configuration to all the interface on any client. This allows the servers to send one exchange that will provide addresses for all the interfaces.
- The DHCPv6 has the capability of providing temporary addresses. While all the addresses are infact temporary, the temporary addresses deals with IPv6 privacy addresses. (Kerr, 2006)

IPv6 Address Auto-Configuration

DHCPv6 and DHCP are both termed as stateful protocols since they both create tables within the DHCP servers. The IPv6 auto-configuration is a stateless auto-configuration protocol which can configure a link local address to all the interfaces. The ability of IPv6 that allows it to configure all the devices without the need for the stateful configuration is an useful feature which is provided by the auto configuration of IPv6. The feature is available on interfaces that are capable of multicast. (Microsoft, 2005)

The autoconfiguration is possible in more than one of the states. These states are as follows:

Tentative:

The tentative address is an address which is in the process of verification on a particular link before it is assigned to an interface. The address is not considered to be assigned. Whatever packets arrive at the interface that has this address are discarded while only the Neighbor Discovery packets which have a connection to the Duplicate Address Detection are accepted. (Thomson & T.Narten, 1998)

Preferred:

The preferred addresses are those addresses that have been verified as being unique and can be assigned to any interface where the usage by the upper layer protocols is not restricted. The preferred addresses can be used as either the destination or the source address where the packet is being sent to or from a particular interface. (Thomson & T.Narten, 1998)

Deprecated:

A deprecated address is an address whose assignment is not forbidden but is discouraged. New communications should not be using the deprecate address as a source address, none the less the packets that that are sent to and from these addresses are received without any issues. The source address can still be used as a depreciated address if changing to a preferred address will cause issues to a protocol at the upper layer. (Thomson & T.Narten, 1998)

Valid:

A valid address is an address which consists of either a preferred address or a deprecated address. These addresses can be assigned to either the destination or the source addresses while the internet protocols should deliver the packets to these sources or destinations. (Thomson & T.Narten, 1998)

Invalid:

Invalid addresses are those that addresses that have not been assigned to any of the interfaces. An invalid address occurs when a valid addresses reaches its lifetime. The invalid addresses should not be assigned to either the source or the destination. In either case, a packet cannot be sent and the receiver cannot respond and the packet cannot be received. (Thomson & T.Narten, 1998)

Other than the address states, the autoconfiguration has three types. These types of addresses are:

Stateless:

The addresses are configured through the use of the receipt of the Router Advertisement messages. This process requires that hosts should not be using a stateful address configuration protocol and the messages must have the address prefixes. (Microsoft, 2005)

Stateful:

The addresses are configured through use of stateful address protocols. Protocols such as DHCPv6 come under the stateful address configuration protocols. The host can use this type of configuration when the messages it receives does not include the address prefixes. The configuration protocol is also used when there are no routers in the network. (Microsoft, 2005)

Both:

Here, the configuration depends on the receipts of the messages of Router Advertisement. The messages have stateless address prefixes while it demands that the hosts should use the stateful address configuration protocol. (Microsoft, 2005)

Conclusion

There a lot of features and advantages that are present in IPv6 that IPv4 couldn't have. While the features listed in this paper are only a few that IPv6 has, there are a lot more that have not been mentioned. With these features, IPv6 will provide a faster and a more secure method of communication while giving a lot of support for device configuration to the network as well as a lot of support for mobile devices through the use of MIPv6. Because of all these advantages, more companies should start moving towards turning their networks to IPv6 to better manage their network.

Works Cited

Barbhuiya, F. A., Biswas, S., & Nandi, S. (2011). Detection of Neighbor Solicitation and Advertisement Spoofing in IPv6 Neighbor Discovery Protocol. *ACM*, 111.

Cisco Systems. (2006, October). *IPv6 Extension Headers Review and Considerations .* Retrieved from http://www.cisco.com/: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.pdf

Das, K. (2015). *Top 10 Features that make IPv6 'greater' than IPv4*. Retrieved from http://ipv6.com/: http://ipv6.com/articles/general/Top-10-Features-that-make-IPv6-greater-than-IPv4.htm

Kerr, S. (2006, October). *DHCPv6.* Retrieved from http://meetings.ripe.net/: http://meetings.ripe.net/ripe-53/presentations/dhcpv6.pdf

Knights, M. (2007). IPv6. *IEEE*, 18.

Kozierok, C. M. (2005). *The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference.* No Starch Press.

Microsoft. (2005). *IPv6*. Retrieved from HTTP://WWW.MICROSOFT.COM/WINDOWS2000/DOCS/IPV6.DOC

Microsoft. (2005, January 21). *IPv6 address autoconfiguration.* Retrieved from https://technet.microsoft.com: https://technet.microsoft.com/en-us/library/cc778502%28v=ws.10%29.aspx

Microsoft. (2005, January 21). *IPv6 features*. Retrieved from https://technet.microsoft.com: https://technet.microsoft.com/en-us/library/cc780593%28v=ws.10%29.aspx

Microsoft. (2005, November). *Understanding Mobile IPv6.* Retrieved from http://www.cu.ipv6tf.org/: http://www.cu.ipv6tf.org/pdf/MobileIPv6.pdf

Network Computing. (2011, August 6). *Six Benefits of IPv6*. Retrieved from http://www.networkcomputing.com/: http://www.networkcomputing.com/networking/six-benefits-of-ipv6/d/d-id/1232791?

Oracle. (2010). *IPv6 Administration Guide.* Retrieved from https://docs.oracle.com: https://docs.oracle.com/cd/E19683-01/817-0573/6mgc65bb3/index.html

Richard, N., & Malone, D. (2005). *IPv6 Network Administration.* O'Reilly Media.

Schroder, C. (2006, September 20). *Understand IPv6 Addresses*. Retrieved from http://www.enterprisenetworkingplanet.com/: http://www.enterprisenetworkingplanet.com/netsp/article.php/3633211/Understand-IPv6-Addresses.htm

Shiyao, Wang, Y., & Xu, K. (2010). Utilizing Destination Options Header to Resolve IPv6 Alias Resolution. *IEEE*.

Thomson, S., & T.Narten. (1998, December). *IPv6 Stateless Address Autoconfiguration.* Retrieved from https://tools.ietf.org: https://tools.ietf.org/html/rfc2462

Wilkins, S. (2011, December 28). *IPv6 Address Types*. Retrieved from http://www.petri.com/: http://www.petri.com/ipv6-address-types.htm

Yousaf, F. Z., Muller, C., & Wietfeld, C. (2010). A Comprehensive MIPv6 Based Mobility Management Simulation Engine for the Next Generation Network. *ACM*.