

THESIS

Ganesh Sharma

IMPLEMENTATION OF IPv6



**Rovaniemen
ammattikorkeakoulu**
University of Applied Sciences

**DEGREE PROGRAMME IN INFORMATION
TECHNOLOGY**

ROVANIEMI UNIVERSITY OF APPLIED SCIENCES

SCHOOL OF TECHNOLOGY

Degree Programme in Information Technology

Thesis

IMPLEMENTATION OF IPv6

Ganesh Sharma
2014

Supervisor: Kenneth Karlsson

Approved 2014

The thesis can be borrowed.

Author(s)	Ganesh Sharma	Year	2014
Commissioned by			
Thesis title	Implementation of IPv6		
Number of pages	67+6		

On 14 September 2012 last block of IPv4 has been allocated from the Regional Internet Register (RIR) across the Europe, Middle East and Asia. In addition, the demand of further addresses, security and efficient routing across Internet has been increasing every day. Hence, to provide the abundant IP addresses and also to overcome the shortcoming of IPv4, IETF developed a new protocol IPv6. IPv6 overcome the limitations of IPv4 and integrate advance feature. These advanced improvements include larger address space, more efficient addressing and routing, auto-configuration, security, and QOS.

The main objective of this project was to implement IPv6 network in Cisco laboratory of Rovaniemi University of Applied Sciences (RAMK). Cisco 2800 and 1700 Series routers, 3500 series Cisco Catalyst Switches, Microsoft Server 2012, Windows 7, Windows 8 and finally Mac OS X were used during implementation process.

This project covers the implementation of IPv6, DHCPv6, DNS, Routing Protocols EIGRP, and Security. The goal of the project was to implement IPv6 to existing IPv4 network without affecting the running services. Furthermore, this project was implementation in Local Area Network (LAN) only.

Key words: IPv6, IPv4, Protocols, Addresses, RFC, Routing, NAT.

CONTENTS

1 INTRODUCTION	1
1.1 PROJECT BACKGROUND	ERROR! BOOKMARK NOT DEFINED.
2 TECHNOLOGICAL BACKGROUND	3
2.1 IPV4 OVERVIEW	3
2.1.1 Addressing	3
2.1.2 Address Class	4
2.1.3 IPv4 Header	5
2.1.4 Network Address Translation	6
2.2 IPV4 LIMITATIONS	7
2.3 IPV6 OVERVIEW	8
2.3.1 IPv6 Addressing	9
2.3.2 IPv6 Header	10
2.3.3 Unicast	12
2.3.4 Multicast	13
2.3.5 Anycast	14
3 COMPARISON BETWEEN V4 AND V6	15
3.1 ADDRESS SPACE	15
3.2 ADDRESS NOTATION	16
3.3 IP HEADER	17
3.4 HIERARCHICAL ROUTING	18
3.5 MOBILITY	18
3.6 SECURITY	19
3.7 QUALITY OF SERVICES	19
4 NEW FEATURES OF IPV6	20
4.1 INTERNET CONTROL MESSAGE PROTOCOL FOR IPV6 (ICMPv6)	20
4.2 NEIGHBOR DISCOVERY PROTOCOL	21
4.2.1 Neighbor Solicitation and Advertisements	22
4.2.2 Router Solicitation and Advertisements	23
4.2.3 Redirect	25
4.4 ADDRESS AUTOCONFIGURATION	25
4.4.1 Stateful	26
4.4.2 Stateless	26
4.4.3 Autoconfiguration Process	26
4.5 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)	27
4.5.1 Stateful and Stateless DHCPv6	28
4.5.3 Prefix Delegation	30
4.6 DOMAIN NAME SERVER (DNS)	30
4.7 BUILT IN SECURITY	31
5 TRANSCION TECHNOLOGY	33
5.1 DUAL STACK	33
5.2 TUNNELING	34
5.2.1 Generic Routing Encapsulation Tunnel	35
5.2.2 Intrasite Automatic Tunnel Addressing protocol (ISATAP)	36
5.2.3 Teredo Tunneling	36
5.2.4 6to4 Tunneling	37
5.3 TRANSLATION	37
5.3.1 Nat64	38
5.3.2 Nat-PT	39
5.4 TUNNEL BROKER	40
6 UPGRADE PLAN	41
6.1 INTRODUCTION	41
6.2 EVALUATION OF CURRENT NETWORK	41
6.3 ADDRESSING PLAN	43
7 IMPLEMENTATION OF IPV6	44

7.1 INTRODUCTION.....	44
7.2 DHCP AND DNS	46
7.3 ROUTING	48
7.4 TUNNELING	50
7.5 ZONE BASED FIREWALL	51
9 CONCLUSION	54
BIBLIOGRAPHY	55
APPENDIX.....	58

List of Figures and Tables

Figure 1. IPv4 Header (Del Ray 1981).....	5
Figure 2. NAT Mechanism (Odom 2012).....	7
Figure 3. IPv6 Header (Deering and Hinden 1998).....	11
Figure 4. IPv6 Unicast Address Format (Hinden and Deering 2006)	12
Figure 5. IPv6 Multicast Address Format (Hinden and Deering 2006).....	13
Figure 6. Anycast Address Format (Hinden and Deering 2006).....	14
Figure 7. IPv4 and IPv6 Addressing (Davies 2012).....	16
Figure 8. IPv4 and IPv6 Header (Odom 2012)	17
Figure 9. ICMPv6 Message Formats	20
Figure 10. Neighbor Solicitation	23
Figure 11. Neighbor Advertisement.....	23
Figure 12. Router Solicitation	24
Figure 13. Router Advertisement.....	24
Figure 14. Redirect Message Format (Nordmark et al 1998).....	25
Figure 15. Addresses Autoconfiguration (Davies 2012)	27
Figure 16. DHCPv6 Message (Droms et al 2003).....	28
Figure 17. DNS Lookup (Davies 2012).....	31
Figure 18. Dual-Stack Mechanism in OSI References Model (Davies 2012).....	34
Figure 19. Encapsulations IPv6 in IPv4 (Nordmark & Gilligan 2000)	35
Figure 20. Translation of IP Addresses (Bagnulo et al 2011).....	38
Figure 21. IPv6 and IPv4 Network Using NAT64 (Graziani 2012).....	39
Figure 22. NAT-PT (Tsirtsis–Srisuresh 2000)	39
Figure 23. The Tunnel Broker Model (Durand et al 2001).....	40
Figure 24. RAMK Network.....	42
Figure 25. IPv6 Configuration in Server 2012	46
Figure 26. IPv6 DNS A records	47
Figure 27. IPv6 DNS Record	47
Figure 28. IPv6 Stateless Autoconfiguration in Windows 8 PC	48
Figure 29. Test for DNS Name Resolution	48
Figure 30. IPv6 Packet Inside IPv4 packet.....	51
Table 1. IPv4 Address Classes (Del Ray 1981)	4
Table 2. List of Multicast Addresses (Hidden and Deering 1998)	14
Table 3. ICMP Error Message (Conta et al 2006)	21
Table 4. ICMP Information Message (Conta et al 2006)	21
Table 5. Inventory List	42
Table 6. Addressing Plan	43

1 INTRODUCTION

After the emergence of Internet in 1960, it has completely revolutionized the way of communications eternally (Tyson 2013; Banstola 2012). With its capabilities, the Internet has become a worldwide broadcasting mechanism for information sharing widely. Furthermore, it has developed into a medium for collaboration and interaction between individuals regardless of geographic location. (Dye–McDonald–Rufi 2010,1–4.) Besides, the massive structure of the Internet, the TCP/IP has played a significant role in the comprehensive expansion of communications (Graziani 2012). As a result, large numbers of communication devices are combined to the Internet. However, this leads to the problem of address exhaustion, as IP addresses are not unlimited. The Internet community has been witnessing the exhaustion of IPv4 since 2000. (Banstola 2012; Davies 2012, 1–2.)

The current Internetwork uses Internet protocol version 4 (IPv4). IPv4 was developed in the 1980s in order to provide the communication between the researchers, military and academic intuitions. (Sportack 2005, 1-9; Dye et al 2010, 33.) The early networks were in the primitive stage and are limited to few organizations. Hence, during the development of IPv4, scientists did not concern about the future Internet and its expansions. (Dye et al 2010, 1–5; Loukola– Skytta 1998.) However, with the exponential growth of the Internet, IPv4 started to face different obstacles concerning address spacing, security, and Quality of Service. (Hagen 2006, 1–2.)

Though, IPv4 has survived for more than 30 years and become the most important aspect of the today's communications systems, it failed to provide the rapid growth of the Internet (Davies 2012, 5). Today's networking requirement extends beyond the support for data communications to the Unified Communication System, which combines the data voice and video in a same stack of communications (Hagen 2006, 1–2).

Furthermore, this project is influenced by the circumstance of IP address depletion. In addition, this project is implemented at Cisco laboratory of RAMK, Rovaniemi. In addition, the goal of the project is to implement IPv6 to

existing IPv4 network without affecting the running services. Furthermore, this project was implementation in Local Area Network (LAN) only.

The project is carried using the Cisco IOS 15.1 release. Cisco IOS 15.1 is an advanced and newer operating system for Cisco devices. It integrates the advanced features like IPv6 tunneling, IPv6 stack and IPv6-per Interface Neighbor Discovery Cache Limit.

This thesis project cover the implementation client/server IPv6 addressing, DHCP, DNS, Internal routing with EIGRP, Tunneling and finally Zone Based Firewall.

2 TECHNOLOGICAL BACKGROUND

2.1 IPv4 Overview

The Internet Protocol was designed to anticipate the data transmission between hosts on interconnected and packet-switched networks. Prior to IP, it was complicated for hosts on different networks to communicate, for instance, a host on a Token Ring network could not communicate with the host on an Ethernet. (Sportack 2005, 1–9.) Del Ray (1981) quoted that “This incapability of communication endures because of incompatibilities of vendor neutral standard of transmission speeds, signaling methods, and synchronization techniques”. Since the two hosts cannot communicate through their native protocols, they must use IP to carry their data. (Dye et al 2010). IP provides a universal standard means of communications for host computers that reside on different types of networks. Moreover, networks that are separated by a large geographic distances. (Del Ray 1981.)

IPv4 was described in the RFC 760 (January 1980), later modified by RFC 791 (September 1981). The IP works at layer 3 of OSI model, in TCP/IP at Network layer. The basic functionality of IP is addressing and fragmentation. The Internet uses the addresses to carry packets or datagram towards their destinations. (Dye et al 2010, 171–196; Del Ray 1981.)

2.1.1 Addressing

Del Ray (1981, 6) summarizes the IPv4 addressing as follow:

Addresses are fixed length of four octets (32 bits). An address begins with a network number, followed by local address (called the "rest" field). There are three formats or classes of internet addresses: in class a, the high order bit is zero, the next 7 bits are the network, and the last 24 bits are the local address; in class b, the high order two bits are one-zero, the next 14 bits are the network and the last 16 bits are the local address; in class c, the high order three bits are one-one-zero, the next 21 bits are the network and the last 8 bits are the local address.

IPv4 address are 32-bits in length and are binary in nature, but are expressed in a dotted decimal format that can be easily understood by human (Odom 2012). Furthermore, the 32-bits are broken into 4 groups of 8 bits each, also known as octets or bytes. Each of the four bytes is then converted into decimal number range between 0-255. Finally each byte is separated by a dot. (Dye et al 2010, 179; Del Ray 1981.)

An example of IPv4 address would be: -

11000000 10101000 00000001 00000001 in binary form.

192.168.1.1 in dotted decimal form.

2.1.2 Address Class

During the development of IP, no classes were developed, because it was considered that 254 networks would be enough for the existing network (Odom 2012). Furthermore, the number of network starts to grow; likewise IPv4 addresses are classified into different classes to provide the requirements of different size of networks (Rockell – Wenger 2000; Graziani 2012). (Dye et al 2010, 181; Del Ray 1981.)

According to Del Ray (1981, 23) IPv4 addresses are divided into classes for flexibility in addressing as shown below:

Table 1. IPv4 Address Classes (Del Ray 1981)

<i>High Order Bits</i>	<i>Format</i>	<i>Class</i>
0	7 bits of network, 24 bits of host	a
10	14 bits of network, 16 bits of host	b
110	21 bits of network, 8 bits of host	c
111	escape to extended addressing mode	

shows the maximum allowed time that the packet stays in the Internet.

Protocol specifies which next layer protocol will be used after the IP processing is done.

Header Checksum is on the header only. Some of the headers field may change; therefore this is computed each time the header is processed.

Source Address marks the sender and it is 32-bit long in size.

Destination Address indicates the receiver and is also 32-bits long.

Options support some other options i.e. security.

Data includes information of next layer. (Nguyen 2012; Del Ray 1981, 10; Rockell – Wenger 2000.)

2.1.4 Network Address Translation

The Network Address Translator (NAT) is a mechanism implemented to map the private address to public routable address (Odom 2012). In a NAT framework, a single node acts as endpoint between private network and public network. This makes a single unique IP address represents entire group of nodes in a network. (Rockell – Wegner 2000.)

Furthermore NAT device use a single or pool of unique public IP addresses represents the private network to the Internet. Further, inside the network, each node has any RFC 1918 IP address and NAT device translate the private IP to public IP. Whenever, nodes try to communicate outside the internal network. (Khan – Sindi 2012; Davies 2012, 4.) Additionally, NAT devices maintain a table called NAT table, keeping track of the sending packets and incoming packet to the appropriate nodes. (Graziani 2012; Francis – Egevagn 1994.)

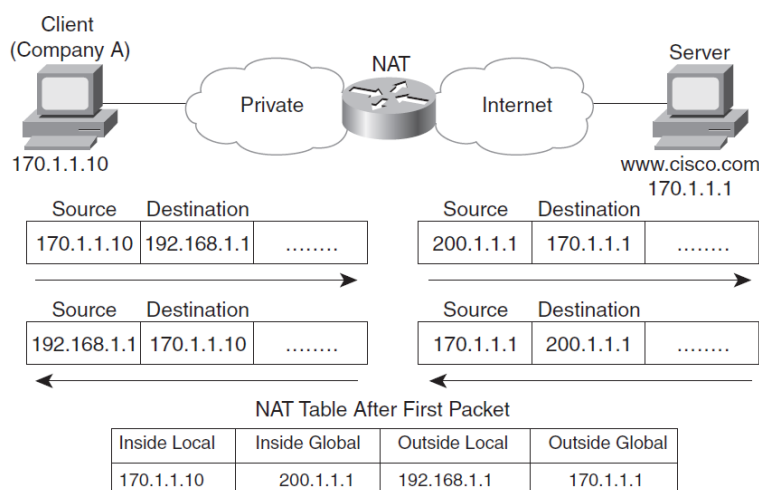


Figure 2. NAT Mechanism (Odom 2012)

2.2 IPv4 Limitations

IPv4 has been around for a long time and has certainly run its course proving its features to be useful both in the implementation and operation. Furthermore, it is an integral part of every network, from a local area network to the worldwide Internet. Nevertheless, everything has worst part and certainly IPv4 is not an exception. (Khan – Sindi 2012.) With the rapid growth of population and tremendous development of technology, the demand for IPv4 addresses becomes higher day after day running out available resources (Graziani 2012). However, one of the obvious reasons is that there hasn't been a substantial improvement made since its development. (Hagen 2006, 1, 35.)

The compelling problems that IPv4 is facing are IP address depletion and scaling in routing. Long-term as well as short-term solutions to address these problems are being developed. These short-term solutions are CIDR, RFC 1918 addresses and NAT. (Davies 2012, 1–11.) The long-term solutions consist of various proposals for new Internet protocols with larger addresses i.e. IPv6. (Francis – Egevang 1994.)

Until the long-term solutions are ready takeover the demand for IP addresses. These short-term solution have been compensating for this

problem, it is just a temporary solution as long as the IPv4 addresses are exhausted. (Davies 2012,4; Graziani 2012.)

Furthermore, Internet provides only the data communication during its birth. Nonetheless, development of the real-time services for instance, Voice over IP encounter the demands of bandwidth and timely delivery. (Davies 2012, 4.) Thus, the necessity for better support for prioritized and real-time communication become obligatory. Further, The Type of Service field in IPv4 header was designed to manage the packet. However, it was never widely implemented because of limited functionality. (Hagen 2006, 128–129.)

Similarly, early networks were primitive and are limited to certain university and organization. Hence, security was not significance during the development and security framework was not developed. Nevertheless, Internet starts to flourish exponentially and the securities become important concerns of all. (Khan – Sindi 2012.) Although, the Internet protocol Security (IPSec) was developed as an add-on feature, due to innumerable interoperability IPSec was not widely implemented. (Hagen 2006, 101–105; Davies 2012, 5–8.)

2.3 IPv6 Overview

The Internet Engineering Task force (IETF) starts a footstep in developing a successor protocol of IPv4 in the early 90's. There has been a number of proposal to solve the problem of address space limitation and developed the advanced engineering in the field of communications. (Loukola – Skytta 1998.) And, one of them is an Internet Protocol- Next Generation (IPng) purposed in 1993 and later modified and developed into IPv6. (Hagen 2006, 1–10, 17–19.)

IPv6 is defined in RFC 2460, which is a suite of standard protocols (Graziani 2012). It is the next generation of network layer protocols for the Internet, after IPv4. Deering and Hinden (1998) state “Similar to IPv4, IPv6 is an Internet Layer protocol for packet - switched internetworking and provides end-to-end datagram transmission across multiple IP networks”. In order to

anticipate the increasing network security demands, a large address space, real-time communication, IPv6 become inevitable. Likewise, IPv6 is designed to allow multiple levels of subnetting and address allocation within an organization or even in the Internet. (Davies 2012, 1–11; Loukola – Skytta 1998.)

IPv6 addresses are 128-bits long, which is a four times larger than the size of 32-bits IPv4 address. Moreover, with the 32-bits addressing space contribute roughly 4 billion of usable address not enough for the total population of world. (Graziani 2012.) On the other hand, 128-bit addressing grant 2^{128} i.e. 655,570,793,348,866,943,898,599 address, enough to provide a 4 billion addresses for every square meter of the earth surface. (Davies 2012, 1–11.) Similarly, the large addresses spaces are designed to be subdividing into hierarchical routing domains that reflect the Internet. In addition, 128 bits provides multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing. These kinds of hierarchical routing are not available on the IPv4-based Internet. (Hagen 2006, 35–38; Loukola – Skytta 1998.)

The Internet Engineering Task Force (IETF) designed IPv6 in order to overcome the limitations of IPv4, providing advanced improvements on the existing IP infrastructure. These improvements include larger IP address space, more efficient addressing and routing, auto-configuration, built-in IPsec, QOS, redesigned header, and neighbor detection. (Deering – Hinden 1998a.)

2.3.1 IPv6 Addressing

IPv6 uses the hexadecimal notation for representation of IP addresses. Hexadecimal notation makes the larger numeric expression simpler and efficient. (Hagen 2006, 35–58.) Likewise, 128-bits are sub divided into eight fields where each fields contains 4 digits, and fields are separated by colons. (Davies 2012, 57–59.) Further, Each IPv6 address has a specific prefix length commonly called as subnet mask. An IPv6 node gets /64 prefix by default but it can be altered as required. A pair of colon or a full IPv6-address is followed by prefix-length. And can be written as: ipv6-address/prefix-length. (Deering – Hinden 1998a.)

An example of IPv6 would be:

2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A /64

In order to shorten IPv6 addresses, we can omit the leading zeros as

2001:**0**DB8:0000:0000:**0**2AA:**00**FF:FE28:9C5A /64

2001:DB8:0000:0000:2AA: FF: FE28:9C5A /64

If there are single group of four zeros can be narrowed down to a single zero

2001:DB8:**0000:0000**:2AA: FF: FE28:9C5A /64

2001:DB8:**0:0**:2AA: FF: FE28:9C5A /64

Furthermore, group of consecutive zeros are compressed to double colons. However, double colons are used only once in each address.

2001:DB8:**0:0**:2AA: FF: FE28:9C5A /64

2001:DB8::**2AA**: FF: FE28:9C5A /64

In addition, to define the network ID, each IPv6 address uses a prefix instead of a subnet mask (Cisco System 2012). The prefix is a forward slash followed by the number of bits in the network ID. A prefix represents a range of addresses and identifies the separation of the address. There is neither limitation nor boundaries on the prefix length, as in IPv4 with CIDR. (Davies 2012, 57–60.)

An example would be 2001:0DB8::**2AA**: /64 indicating that the right part after 64-bits can be changed. (Cisco System 2012; Deering – Hinden 1998a.)

2.3.2 IPv6 Header

In RFC 2460, Deering and Hinden (1998a, 12) explains the IPv6 header size and its fields associated with header as follow:

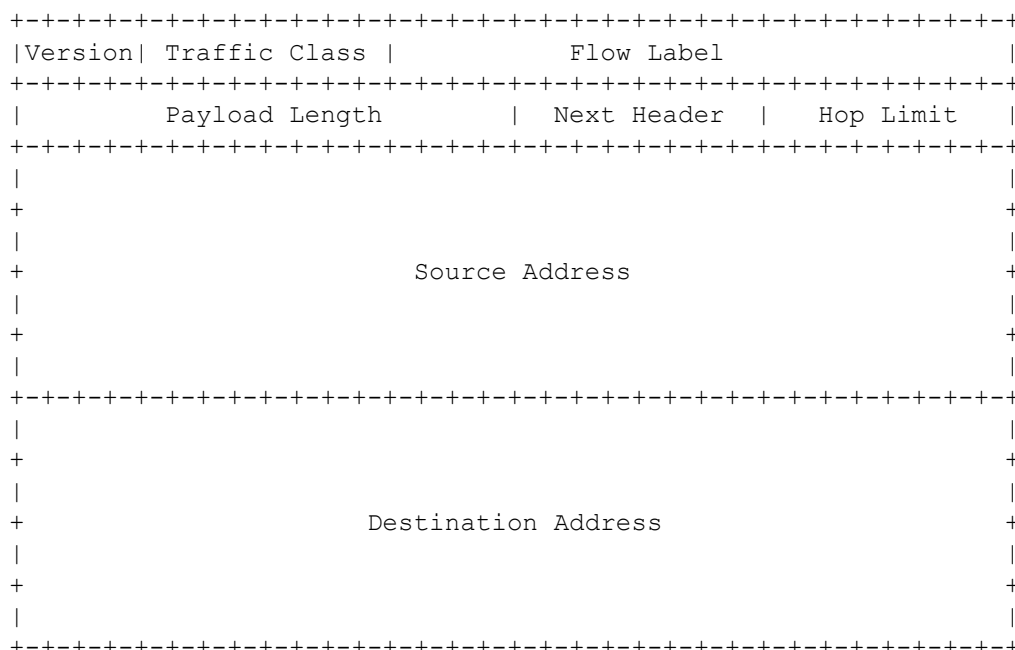


Figure 3. IPv6 Header (Deering and Hinden 1998)

Version: The version field is a 4-bit field that indicates the version of the Internet Protocol. For IPv6 the version field is 6 and for IPv4 it is 4.

Traffic class: An 8 bit traffic class field is used by IPv6 node to indicate the packets so that they can be distinguished and given special priority. It replaces the Type of Service field in IPv4.

Flow Label: It is a 20-bits field is used to label packets from a source belonging to a certain flow that all require the same processing.

Payload length: A 16 bit payload length field specifies the length of the data carried, including any extension headers, in numbers of bytes.

Next header: It is an 8-bit field identifies the type of the header following after the IPv6 header and replaces the protocol field in the IPv4 header.

Hop limit: An 8 bit field indicates that how many hops are left before the packet is discarded. One decreases this value every time it passes through a router. The time to live field in the IPv4 header has the same functionality, but the field was renamed to reflect the actual use of the field.

Source Address: 128-bits field represent the sender of the Packet.

Destination Address: 128-bits field; represent the intended recipient of the packet. (Deering – Hinden 1998a.)

2.3.3 Unicast

Unicast IP addresses are assigned to a single interface and enabling the uniqueness within the scope of the type address (Hinden–Deering 2006). These addresses deliver data packets to a single interface of an IPv6 node (Cisco system 2012). Furthermore, more than one unicast address can be assigned to a single interface. Likewise, multiple interfaces are allowed to use same address as long as appear as a single interface to an IPv6 node (Loukola – Skytta 1998; Davies 2012, 101–110.) Hinden and Deering (2006) emphasizes that Unicast addresses consist of subnet prefix and host ID or interface ID and the format is illustrated as follow:

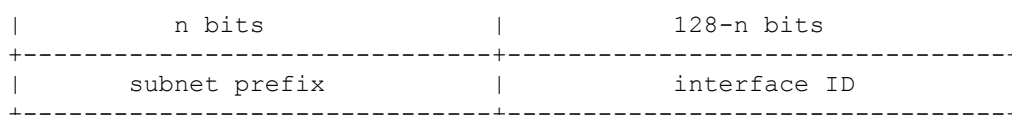


Figure 4. IPv6 Unicast Address Format (Hinden and Deering 2006)

Unicast addresses are further classified different groups they are unique global, link-local, and unique local/site-local addresses, Unspecific and Loopback address.

Global Unicast: These addresses are designed in a hierarchically-structure to develop an efficient routing infrastructure across the Internet (Hagen 2006, 35–40). They are equivalent to the public IPv4 address, such as, 200.200.200.0/24.

Link-local: Link-local addresses are used by nodes, while communicating with other nodes on the same subnet (Hagen 2006, 35–40). Moreover, they are link-local in scope i.e. nodes can communicate with other node without connected to a router. In addition, the router will not forward any packets outside the same link using Link-local address.

Unique local/ Site-Local: These addresses are equivalent to the IPv4 private address spaces, such as 10.0.0.0/8 (Davies 2012, 77–89). These addresses are mainly used by the organizations that are not yet connected to Global Internet and shall not be routed in Internet. Site- local addresses also have their first 10 bits reserved and always start with FEC0::/10 (Hinden–Deering 2006.)

Unspecific Addresses: Those address which have all zeros in address field are regarded as Unspecific addresses i.e. 0:0:0:0:0:0:0:0/128 or :: /128 and used when the IPv6 nodes haven't got any IPv6 address(Hinden–Deering 2006.)

Loopback Addresses: The loopback address i.e. 0:0:0:0:0:0:0:1 or ::1 is used to identify a loopback interface. It is equivalent to the IPv4 loopback address of 127.0.0.1. A node send IP packet to itself by using this address. (Hinden–Deering 2006.)

2.3.4 Multicast

The multicast addresses are used to identify a single or multiple interfaces. In addition, multicasts address functions as in IPv4 network and packets addressed to a multicast address are delivered to all interfaces represented by the address. (Davies 2012, 77–89.) As explained by Hinden and Deering (2006) first eight bits of IPv6 multicast addresses are always reserved to one and always begins with “FF” and multicast address format is shown below:

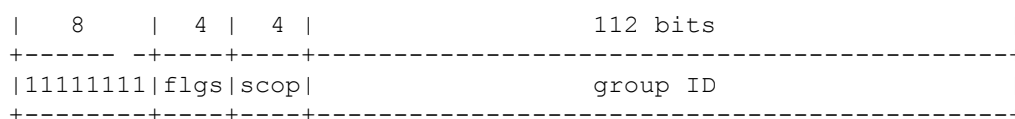


Figure 5. IPv6 Multicast Address Format (Hinden and Deering 2006)

As defined by Hidden and Deering (1998b) in RFC 2375 the following table describes the reserved multicast address:

Table 2. List of Multicast Addresses (Hidden and Deering 1998)

Addresses	Reserved For	Scope
FF01::1	All nodes address	Local node
FF01::2	All routers address	Local node
FF02::1	All nodes address	Link-local
FF02::2	All routers address	Link-local
FF02::5	OSPF	Link-local
FF02::6	OSPF	Link-local
FF02::9	RIP	Link-local
FF02::1:FFXX:XXXX	Solicited-node address	Link-local
FF02::A	EIGRP	Link-local
FF05::2	All routers address	Site-local
FF05::1:3	All DHCP Server	Site-local
FF05::1:4	All DHCP relay agents	Site-local

2.3.5 Anycast

Hinden and Deering (2006) suggest, “Anycast are the unicast addresses assigned to the multiple interfaces. The packets destined to anycast addresses are routed to the interface that is nearest in terms of routing distance”. The anycast addresses are the unicast addresses assigned to interfaces concurrently. Likewise, IPv6 unicast they are assigned to one or more interfaces and packets are delivered to an anycast address. Furthermore, the anycast addresses eliminate the broadcast in the network through identifying multiple interfaces. (Davies 2012, 77–89.)

The anycast addresses are explicitly configured using the unicast addresses and addressing format is shown below:

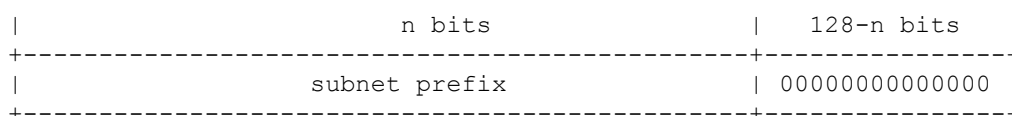


Figure 6. Anycast Address Format (Hinden and Deering 2006)

Meanwhile, Davies (2012) points out the main difference between the multicasts and anycast addresses as “A multicast address is used for one-to-many communication, with delivery to multiple interfaces. An anycast address is used for one-to-one-of-many communication, with delivery to a single interface”.

3 COMPARISON BETWEEN v4 AND v6

Even though IPv4 is a dominant network layer protocol of the Internet; it has its own disadvantages, experienced by Internet users. In order to overcome these disadvantages, the IETF developed IPv6, a suite of protocols and its standards. (Khan – Sindi 2012.) In contrast, IPv6 have many superiority over IPv4 and large address space is one of them. Further, one major difference in IPv6 network is that routers are no longer required to fragment oversized packets. The host itself does fragmentation and the routers can simply route the packet through internetworks depending upon MTU of the link. (Davies 2012, 1–2.) Additionally, multicast addresses substitute the broadcast addresses. Similarly, Neighbor Discovery (ND) replaces ARP. (Hagen 2006, 1–10, 17–21.)

3.1 Address Space

The most crucial difference between IPv4 and IPv6 is address space. The earlier protocol used 32-bit addressing, resulting to a theoretical limit of 2^{32} i.e. 4,294,967,296 addresses. However, the new protocol is 128-bit long allocating total number of 2^{128} i.e. roughly $3.4 * 10^{38}$ possible addresses. (Cisco System 2007.) Despite that available IPv4 addresses are being rapidly depleted. Consequently, migration to another protocol becomes unavoidable. Unlike IPv4, IPv6 has very large number of addresses space that would be available for a long time (Hagen 2006, 35–38). In addition, these addresses are allocated in a hierarchical nature to minimize the size of the global routing tables. (Davies 2012, 1–5.) As noted by the Davies (2012) following diagram plots the comparison between addressing of IPv4 and IPv6:

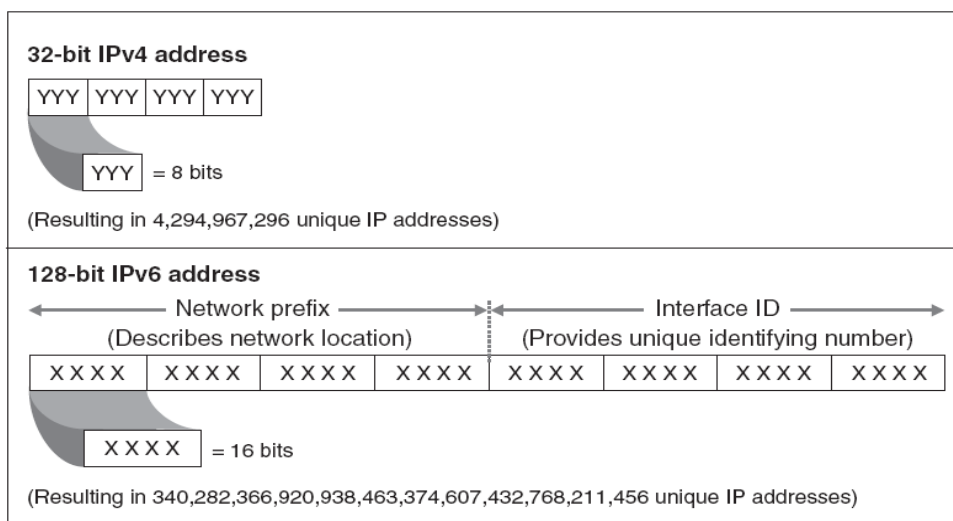


Figure 7. IPv4 and IPv6 Addressing (Davies 2012).

3.2 Address Notation

There is an immense difference in the notation between IPv4 and IPv6 addresses. IPv4 is represented in a dotted-decimal notation grouped of four bytes, each separated by dot “.” On the other hand, IPv6 are represented as hexadecimal number eight fields of four bytes, separated with colons. Additionally, leading zeros are always omitted in both IPv4 and IPv6. Whereas in IPv6, one or several fields of zeroes can be compressed and represent with two colons. However, this can only be done once. (Deering–Hinden 1998a.)

An example of IP addressing is explained as:

IPv4 address: - 192.168.1.1

IPv6 address: - 2001:db8:0000:0102:00ac:0000:0000:00ab

2001:db8:0:102: ac: 0:0: ab

2001:db8:: 102:ac:0:0:ab

2001:db8:0:102: ac:: ab

Nevertheless, a slash and the length in number of bits in both IPv4 and IPv6 represent prefix length. IPv4 prefix: 192.168.10.0/24

IPv6 prefix: 2001:db8:0:102:: /64

(Hagen 2006, 45–58; Cisco System 2007.)

3.3 IP Header

IPv6 header is more simple and fixed size of 40 bytes. Conversely, IPv4 headers range from 20 and 60 bytes depending on the presence of option field (Deering– Hinden 1998a). On contrary to IPv4, unnecessary fields have been removed from the IPv6 header, for example, header length, identification, flags, fragment offset, header checksum, and options field. In addition, these identification fields along with the fragment-offset field have been moved to a fragment header extension header. (Hagen 2006, 1–11, 17–33; Cisco system 2008.)

In IPv4 fragmentation is done when needed by the routers along route to destination, while with IPv6, fragmentation is only allowed at the source. Further, header checksum is removed, since IPv6 depends on upper level protocols, lower layer checksums and error correction schemes for data integrity. (Davies 2012, 5–11; Graziani 2012.) Consequently, eliminating the recalculation of the checksum at every hop, as well as time to live field is changed at every hop. Furthermore, options are no longer defined in the IPv6 header, but rather the extension headers are equivalent to IPv4 options. (Deering – Hinden 1998a). The difference in the header size of IPv4 and IPv6 are described below:

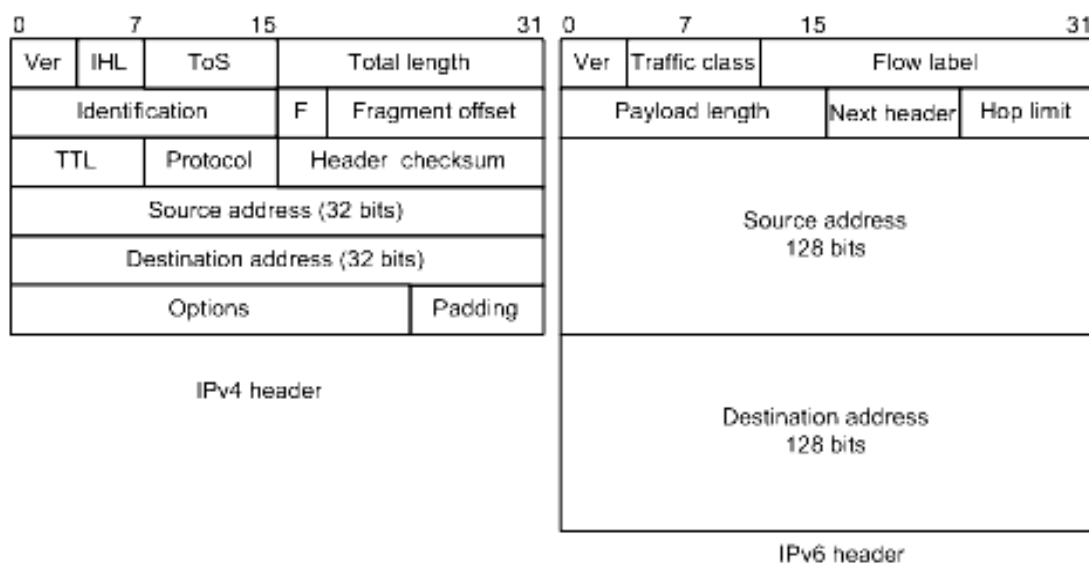


Figure 8. IPv4 and IPv6 Header (Odom 2012)

3.4 Hierarchical Routing

The larger address space, scalable routing is an important factor to maintain the viability of the Internet. While in IPv4, addressing format is designed as hierarchical, whereas routing is not. Consequently, this routing scheme will not be scalable enough to sustain the growth of the Internet. (Graziani 2012.) Furthermore, in IPv4 networks routing are inefficient, for instance, a typical Internet backbone routers contains more than 85,000 routes in their routing tables through which data can be transmitted. (Davies 2012, 5–11.) In contrast, IPv6 is designed to support for a large and scalable routing across the Internet. Additionally, addresses in IPv6 are distributed across the globe in a hierarchical order. (McFarland– Sambhi– Sharma– Hooda 2011, 17–20.)

3.5 Mobility

Mobility in IPv6 ensures the mobile devices roaming potential, regardless of its location in an IPv6 network. RFC 3775, document the mobility support for IPv6, allowing the nodes to be reachable across the IPv6 Internet. Consequently, always identified by their home addresses regardless of its current point of attachment to Internet. (Graziani 2012; Jonson – Perkins – Arkko 2004.) In order to bring about the mobility, mobile nodes had to use a specific address that is always assigned to the mobile node within the subnet prefix of its home network and always reachable. (Davies 2012, 549–555.) Whenever a mobile device is in foreign network, it sends the network information to the home agent about its current link using the IP address of the foreign link also known as care of address. (Graziani 2012.) As a result, the home agent route the packet using tables, tunnels and encapsulation. Therefore, mobility simplifies the movement of node from one Ethernet segment to another as well as it from an Ethernet to a wireless LAN, without having to change its IPv6 addresses (Jonson et al 2004; Hagen 2006, 315–318).

3.6 Security

On the important aspect of security, IPv6 was developed with native support for IPSec. Unlike IPv4, IPSec was not built into the design, but later developed as an add-on feature. (Kent – Atkinson 1998.) IPSec is mandatorily embedded in all kinds of networking devices and IPv6 advanced security can be deployed immediately. (Hagen 2006, 101–105; Graziani 2012.) Furthermore, importance of IPSec has grown recently as all the organizations have dictated to enable IPv6-capable systems and to transition to IPv6-capable networks. And finally, IPSec has the security practice of maintaining simplicity in order to provide greater assurance that security is maintained. (Vyncke– Hogg 2008, 4–10; Loukola– Skytta 1998.)

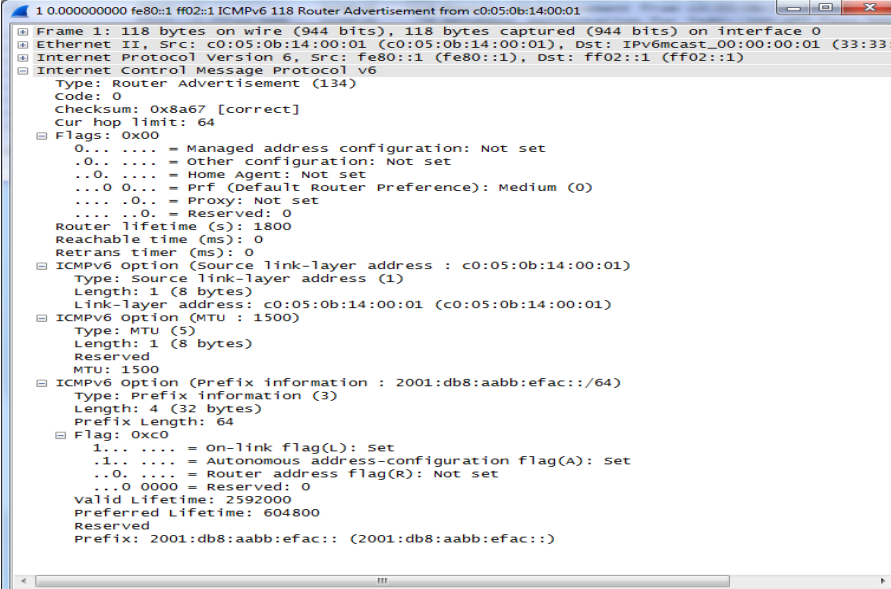
3.7 Quality of Services

An 8-bit field in the IPv6 header is used by nodes to guarantee the IP packets for timely delivery and management of traffic flow (Davies 2012, 91–100). This new field in the IPv6 header substitutes the Type of Service field in IPv4 and defines how traffic is managed. Traffic class allows nodes to identify and provide special supervision for packets belonging to certain data flow. (Deering – Hinden 1998a.) Because the traffic is identified in the IPv6 header, support for prioritized delivery can provide better communication, for instance, VOIP and real time application. (Graziani 2012; Hagen 2012, 128–130.)

4 NEW FEATURES OF IPv6

4.1 Internet Control Message Protocol for IPv6 (ICMPv6)

The Internet Control Message Protocol defined in RFC 4443 is a widely used protocol for gathering information and troubleshooting about devices connected in the network (Davies 2012, 117–129). Moreover, ICMPv6 is more advanced than ICMPv4 and includes wide varieties of new functionality for the efficient communication in the Network. As defined by Conta, Deering, and Gupta (2006) the ICMP is divided into two types of message: error and information. Furthermore, a packet has been capture-using wireshark and the ICMPv6 message and the typical format of message type in ICMP is as follow:



```

1 0.000000000 fe80::1 ff02::1 ICMPv6 118 Router Advertisement from c0:05:0b:14:00:01
  Frame 1: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
  Ethernet II, Src: c0:05:0b:14:00:01 (c0:05:0b:14:00:01), Dst: IPv6mcast_00:00:00:01 (33:33:
  Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
  Internet Control Message Protocol v6
    Type: Router Advertisement (134)
    Code: 0
    Checksum: 0x8a67 [correct]
    Cur hop limit: 64
    Flags: 0x00
    0. .... = Managed address configuration: Not set
    .0. .... = Other configuration: Not set
    ..0. .... = Home Agent: NOT set
    ...0 0... = Prf (Default Router Preference): Medium (0)
    .... .0.. = Proxy: Not set
    .... ..0. = Reserved: 0
    Router lifetime (s): 1800
    Reachable time (ms): 0
    Retrans timer (ms): 0
    ICMPv6 option (Source link-layer address : c0:05:0b:14:00:01)
      Type: Source link-layer address (1)
      Length: 1 (8 bytes)
      Link-layer address: c0:05:0b:14:00:01 (c0:05:0b:14:00:01)
    ICMPv6 option (MTU : 1500)
      Type: MTU (5)
      Length: 1 (8 bytes)
      Reserved
      MTU: 1500
    ICMPv6 option (Prefix information : 2001:db8:aabb:efac::/64)
      Type: Prefix information (3)
      Length: 4 (32 bytes)
      Prefix Length: 64
      Flag: 0xc0
      1... .... = On-link flag(L): Set
      .1. .... = Autonomous address-configuration flag(A): Set
      ..0. .... = Router address flag(R): Not set
      ...0 0000 = Reserved: 0
      Valid Lifetime: 2592000
      Preferred Lifetime: 604800
      Reserved
      Prefix: 2001:db8:aabb:efac:: (2001:db8:aabb:efac::)
  
```

Figure 9. ICMPv6 Message Formats

Each field in the message body performs the different functions, for instance, the type fields represent the type of the message, and code field always depends on the type of the message. And finally, checksum performs the error detections in the data packets during transmission. (Hagen 2006, 60–68.) The different categories of ICMPv6 message according to Conta et al (2006) are shown in following table:

Table 3. ICMP Error Message (Conta et al 2006)

ICMPv6 error messages:

Code	Message
1	Destination Unreachable
2	Packet Too Big
3	Time Exceeded
4	Parameter Problem
100	Private experimentation
101	Private experimentation
127	Reserved for expansion of ICMPv6 error messages

Table 4. ICMP Information Message (Conta et al 2006)

Code	Message
128	Echo Request
129	Echo Reply
200	Private experimentation
201	Private experimentation
255	Reserved for expansion of ICMPv6 informational messages

4.2 Neighbor Discovery Protocol

Neighbor Discovery is the family of protocols at the core of IPv6, which is specified in the RFC 2461 (Graziani 2012). The specification described in the RFC intergrades different protocols from the IPv4 and adds the new features; address autoconfiguration, parameter discovery, next-hop destination, Neighbor Unreachable Detection (NUD) and Duplicate Address Detection (DAD). (Nordmark–Narten–Simpson 1998.)

IPv6 ND Protocol is a series of five ICMPs messages responsible for node-to-node communication on a same link (Davies 2012, 131–139). Further, ND is one of the enhanced features of IPv6 that completely eliminates the broadcast, unlike in IPv4 (Graziani 2012). The most important function of this protocol is used to determine the link-layer address of the nodes in a same link. Additionally, hosts to keep track of any changes in its default gateway and routes for routing the packets, and discover the best routes that are

willing to route the packets on their behalf use ND. (Hagen 2006, 60–68; Nordmark, et al 1998.)

ND messages consist of a ND message header that is composed of an ICMPv6 header and ND message specific data. A ND message might contain additional ND options. ND message option provide an additional information usually indicating media access control (MAC) addresses on-link network prefixes, on-link maximum transmission unit (MTU) information and redirection data. (Davies 2012, 131–135; Nordmark et al 1998.)

4.2.1 Neighbor Solicitation and Advertisements

Neighbor solicitation is send by a PC to the entire PC in the same segment or group of the computers depending on the type of request. In order to verify the uniqueness of the link-local address, the IPv6 node uses the duplicate address detection technique called Duplicate Address Detection (Graziani 2012). DAD is a mandatory function performed for verifying that the address that the Node are about to use is available and unique in the network, performed for all kind of address whether it is Link-Local addresses or Global Unicast Address (Hagen 2006, 60-68). Furthermore, nodes perform the neighbor solicitations for requesting the information about neighbor devices and neighbor devices sends the information through neighbor Advertisements. (Davies 2012, 131–139; Hagen 2006, 60–68.)

A datagram has been capture when the IPv6 host in the network using the Wire shark and the packet look like as follow:

```

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: c0:09:08:9c:00:00 (c0:09:08:9c:00:00), Dst: IPv6mcast_ff9c:00:00 (33:33:ff:9c:00:00)
Internet Protocol Version 6, Src: :: (:), Dst: ff02::1:ff9c:0 (ff02::1:ff9c:0)
  0110 .... = Version: 6
  .... 1110 0000 .... .. = Traffic class: 0x000000e0
  .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 24
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: :: (:)
  Destination: ff02::1:ff9c:0 (ff02::1:ff9c:0)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Internet Control Message Protocol v6
  Type: Neighbor Solicitation (135)
  Code: 0
  Checksum: 0xb1e5 [correct]
  Reserved: 00000000
  Target Address: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0)

```

Figure 10. Neighbor Solicitation

And as well Neighbor Advertisement packet has been capture using the same tool and it look like as shown in given image.

```

Frame 9: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
Ethernet II, Src: c0:09:08:9c:00:00 (c0:09:08:9c:00:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
Internet Protocol Version 6, Src: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0), Dst: ff02::1 (ff02::1)
  0110 .... = Version: 6
  .... 1110 0000 .... .. = Traffic class: 0x000000e0
  .... .. 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 32
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0)
  [Source SA MAC: c0:09:08:9c:00:00 (c0:09:08:9c:00:00)]
  Destination: ff02::1 (ff02::1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Internet Control Message Protocol v6
  Type: Neighbor Advertisement (136)
  Code: 0
  Checksum: 0xfdac [correct]
  Flags: 0x20000000
  Target Address: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0)
  ICMPv6 option (Target link-layer address : c0:09:08:9c:00:00)

```

Figure 11. Neighbor Advertisement

4.2.2 Router Solicitation and Advertisements

When the hosts in the network get its link-local address, it is wondering, what's the global address network space that it's attached to? The host sends another type of message called as router solicitation; requesting for network information about the network it attach to. (Graziani 2012.) Additionally, this message is sent to well-known multicast group *FF02::2*. It is the group that all the routers supporting IPv6 routing have already joined and able to hears the Router Advertisement request. (Davies 2012, 131–139;

Hagen 2006, 60–68.) Consequently, the router answers by sending Router Advertisement, if one present. Furthermore, the Router Advertisements contains the valuable information like autoconfiguration, Stateful autoconfiguration, DHCP, IPv6 global network prefix and other option. These messages are sent periodically or in response of Router Solicitation. (Nordmark et al 1998.)

A datagram has been capture using the Wire shark, which shows the different fields in the trace data.

```

+ Frame 34: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 0
+ Ethernet II, Src: c0:09:08:9c:00:00 (c0:09:08:9c:00:00), Dst: IPv6mcast_00:00:00:02 (33:33:00:00:00:02)
+ Internet Protocol Version 6, Src: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0), Dst: ff02::2 (ff02::2)
  0110 .... = Version: 6
  .... 1110 0000 .... .... .... = Traffic class: 0x000000e0
  .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 16
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: fe80::c209:8ff:fe9c:0 (fe80::c209:8ff:fe9c:0)
  [Source SA MAC: c0:09:08:9c:00:00 (c0:09:08:9c:00:00)]
  Destination: ff02::2 (ff02::2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
+ Internet Control Message Protocol v6
  Type: Router Solicitation (133)
  Code: 0
  Checksum: 0xe9e2 [correct]
  Reserved: 00000000
  + ICMPv6 option (Source link-layer address : c0:09:08:9c:00:00)

```

Figure 12. Router Solicitation

A datagram has been capture using the Wire shark, which shows the different fields in the trace data.

```

+ Frame 35: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
+ Ethernet II, Src: c0:00:17:68:00:00 (c0:00:17:68:00:00), Dst: IPv6mcast_00:00:00:01 (33:33:00:00:00:01)
+ Internet Protocol Version 6, Src: fe80::1 (fe80::1), Dst: ff02::1 (ff02::1)
  0110 .... = Version: 6
  .... 1110 0000 .... .... .... = Traffic class: 0x000000e0
  .... .... 0000 0000 0000 0000 0000 = Flowlabel: 0x00000000
  Payload length: 64
  Next header: ICMPv6 (58)
  Hop limit: 255
  Source: fe80::1 (fe80::1)
  Destination: ff02::1 (ff02::1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
+ Internet Control Message Protocol v6
  Type: Router Advertisement (134)
  Code: 0
  Checksum: 0x3201 [correct]
  Cur hop limit: 64
  + Flags: 0x00
  Router lifetime (s): 1800
  Reachable time (ms): 0
  Retrans timer (ms): 0
  + ICMPv6 option (Source link-layer address : c0:00:17:68:00:00)
  + ICMPv6 option (MTU : 1500)
  + ICMPv6 option (Prefix information : 2001:ac11:3578:12af::/64)

```

Figure 13. Router Advertisement

4.4.1 Stateful

A host uses stateful address configuration when it receives Router Advertisement messages with no prefix options. In these Router Advertisement messages, the Managed Address Configuration flag is set to 1. The Flag set to 1 means that the nodes should receive all the information from the DHCP server. (Thomson – Narten – Jinmei 2007.)

4.4.2 Stateless

Stateless Autoconfiguration of addresses is based on the message of Router Advertisement that has the Managed Address Configuration and Other Stateful Configuration flags set to 0. In addition, these messages contain one or more Prefix Information options. Stateless autoconfiguration generates a temporary address until it can determine the full configuration of the network it is on, and then it generates a permanent address that it can use. (Davies 2012, 205–210.)

4.4.3 Autoconfiguration Process

During the autoconfiguration, firstly, a link-local address is derived, based on the link-local prefix and the 64-bit interface identifier. Secondly, the IPv6 host generated the link-local address node perform the Duplicate Address Detection. If another node on the local link has the same link-local address, the IPv6 node that sends the Neighbor Solicitation message receives a Neighbor Advertisement message. As a result of Neighbor Advertisement message, the address autoconfiguration stops. In this case, IPv6 address must be manually configure. However, if no one sends Neighbor Advertisement message, this indicates the link-local address is unique and valid. Finally, the link-local address is initialized for the physical interface of an IPv6 node. (Davies 2012, 205–210.)

Conversely, if the Autonomous flag in the Prefix Information option is set to 1, the network prefix and the 64-bit interface identifier are used to generate

address. Again to verify the uniqueness of the address, the IPv6 host uses duplicate address detection. Based on the final outcome of DAD, the address is initialized. The initialization of address includes setting the valid and preferred lifetimes, based on the Valid Lifetime and Preferred Lifetime fields in the Prefix Information option. Davies (2012) draws attention to the autoconfiguration process elaborated in following diagram:

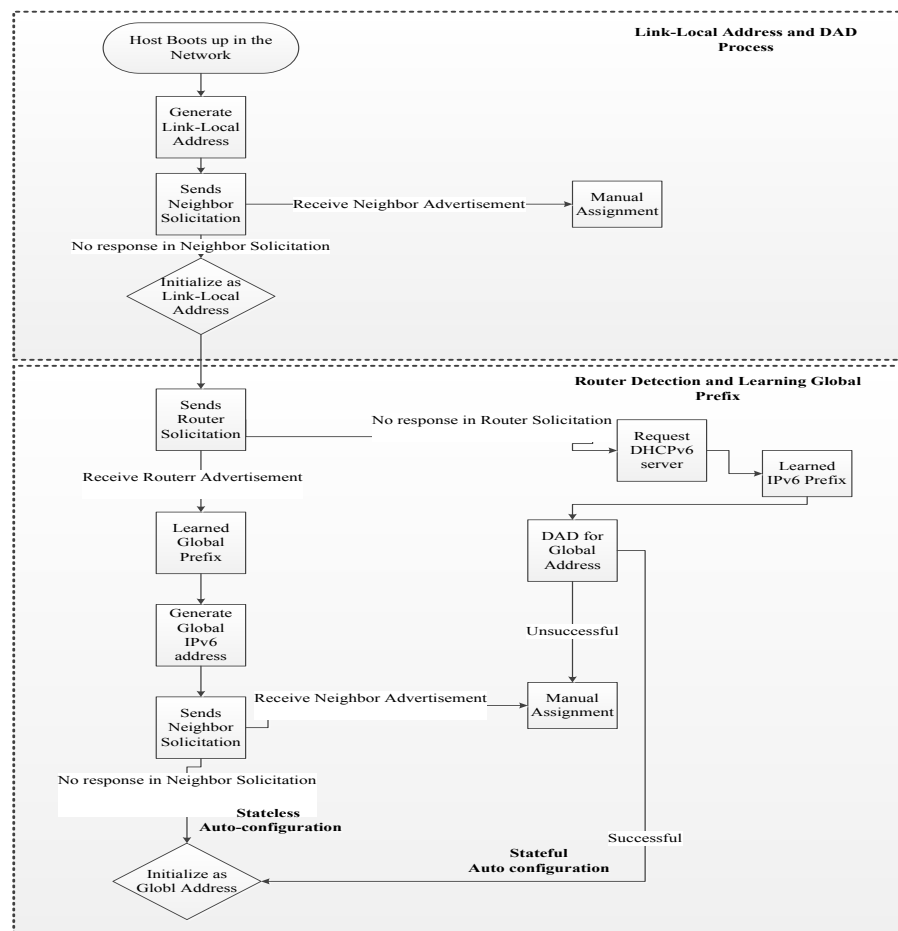


Figure 15. Addresses Autoconfiguration (Davies 2012)

4.5 Dynamic Host Configuration Protocol (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a client/server protocols originally defined in the year 1993, in RFC, 1531 and later in 1997 modified into RFC, 2131 (Odom 2012; Dye 2010, 87–90). The basic functionality of a DHCP is to provide automatic managed configuration of a particular network to the IP clients. In IPv6 world new and extended DHCPv6 has been

introduced, as described in RFC, 3315. In addition, DHCP is an unreliable protocol and use the UDP port for receiving the message. The IPv6 client uses UDP port 546 for listening, while in IPv6 server as well as relay agents' uses UDP port 547 for listening. (Davies 2012, 210–215; Droms–Bound–Volz–Lemon –Perkins–Carney 2003.)

As defined by Droms et al (2003) the message format between the DHCP server/client messages is shown below:

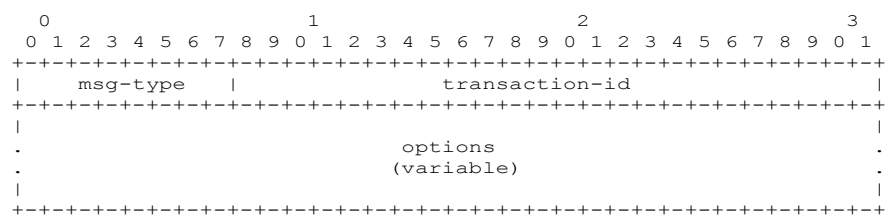


Figure 16. DHCPv6 Message (Droms et al 2003)

The brief description of each field is given below:

Msg-type: It indicate the type of DHCP message

Transaction-id: Used by client to group the message.

Options: Contains the identification of client/server, IPv6 prefixes, and other important configurations.

According to Droms et al (2003) DHCP is the "stateful address autoconfiguration protocol" and the "stateful autoconfiguration protocol" referred to in "IPv6 Stateless Address Autoconfiguration".

4.5.1 Stateful and Stateless DHCPv6

The IPv6 client machines configure their IP addresses from the DHCPv6 server on the basics of the Router Advertisements received from the router. According to Droms et al (2003) the Router Advertisements contains Flags field, which have one of the following information.

Managed Configuration Flag: - This field is commonly known as ***M flag***, contains a value either 0 or 1.

Other Configuration Flag: - It known as ***O Flag***; also contains value ether 0 or 1.

These field values can be interchanged according to the need of a network. According to Davies (2012) the client receives Router Advertisements the combinations of values in **M** and **O** flags are following.

Both **M** and **O** are set to 0: - It indicates that hosts in the network autoconfiguring their address using Router Advertisements and other option like DNS are manually configured.

Both **M** and **O** are set to 1: - This is referring the client to use the DHCPv6 server for configuring both addresses and other configuration and this process is known as Stateful DHCP.

M flag set to 0 and **O** flag to 1: - In this combination client autoconfiguring their addresses but use the DHCPv6 for other configuration and this process is known as Stateless DHCP.

M flag set to 1 and **O** flag to 0: - This is an unlike combination and not used because it indicate that client use DHCPv6 for only configuring addresses, but not for other configuration.

Stateful DHCPv6 is used for address configuration of IPv6 client in the network when they receives the Router Advertisement message with *M* flag or bit set to 1 or if no routers are present in the link (Hagen 2006, 226–234; Davies 2012, 210–215). Conversely, DHCPv6 server is used to provide other information then the process is called as stateless DHCPv6. Node on the IPv6 network use Router Advertisement Message to obtain the other information for instance DNS. (Droms et al 2003; Banstola 2012.)

4.5.3 Prefix Delegation

Prefix Delegation is a mechanism to assign the prefix addresses to the networking devices that are unaware of the networking topology. For instance, Internet Services Provider (ISP) may use prefix delegation to assign the prefix addresses to the Customer Premise Equipment (CPE). The requesting router communicates with ISPs delegating router, which then selects the prefix(s) to be assigned and used by customer. In this method it is not mandatory to advertise prefix(s) information on Router Advertisement message but the default gateway must be informed to the IPv6 client. (Troan – Droms 2003.)

4.6 Domain Name Server (DNS)

Domain Name Server was originally specified in RFC 882 and 883, but in November 1987 it was rewritten and specified in RFC 1034 and 1035. The main functionality of DNS is to map domain name into IP address and vice-versa. (Thomson– Huitema– Ksinant –Souissi 2003; Liu 2010, 1–8.)

The current DNS system for IP lookup doesn't support the IPv6 address resolutions. Further, the application server assumes that queries are returned to IPv4 addresses only (Banstola 2012; Liu 2010, 1–8). In order for the support for IPv6 name resolution some extension has to be made and Thomson et al (2003) have explained then as

A resource record type is defined to map a domain name to an IPv6 address.

A domain is defined to support lookups based on address.

Existing queries that perform additional section processing to locate IPv4 addresses are redefined to perform additional section processing on both IPv4 and IPv6 addresses.

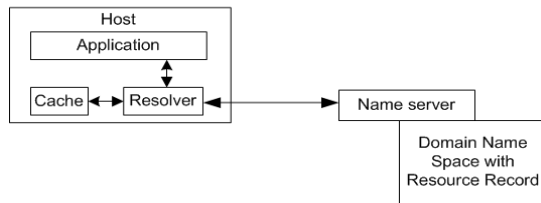


Figure 17. DNS Lookup (Davies 2012)

Figure 17 illustrates DNS lookup process and components of DNS for example, Domain Name Space, Name server and Resolver. Domain Name Space contains the record for domain names defined with specific type like A, AAAA, and A6. Name server stores the information about where those zones reside and, resolver carryout the queries from client machine to name server. Name server and resolver have cache so that information from cache can be used if a client requests the same information frequently, instead of repeating the entire process. (Banstola 2012; Liu 2010, 1–8.)

4.7 Built in Security

IPv6 have built in security as IPSec and have solved security problems opposed by IPv4. IP Security, originally defined in RFC 2410 and later modified in RFC 4301, is a collection of open standards protocols developed by the IETF providing advance security for transmission of datagram over unprotected networks such as the Internet. Furthermore, IPSec operates at Layer 3 of OSI model, encrypting and authenticating packets during the data communication. (Das 2008; Hagen 2006, 101–105.) Using the IPSec as a security in a production environment following network security services can be achieved.

Data confidentiality: - Datagrams are encrypted before sending them across a network.

Data integrity: - Packets are authenticated in order to ensure that the data has not been corrupted during transmission.

IPSec operates in a two different: transport mode where only the payloads of IP packet are encrypted and communication occurred between two end

nodes. While, another is Tunnel mode where the communication happened between two sites like VPN and the entire packet is encrypted. (Blanchet 2006, 223–240.)

In IPv6 only tunnel mode encryption is supported using authentication header (AH) and the ESP extension header. The authentication header provides integrity and authentication for all IP Packets using signature-based algorithm in end-to-end data communication. The Encapsulating security payload header provides integrity, confidentiality, and data origin authentication, connectionless integrity of the inner packet, antireplay, and limited traffic flow confidentiality. (Hagen 2006, 101–105.)

5 TRANSITION TECHNOLOGY

IPv4 dominates today's Internet; hence the migration needs to happen. However, transition to IPv6 must be increment and over time as these protocols will coexist for many years from now. (Blanchet 2006, 278–290.) Transition to IPv6 involves the upgrading of applications, hosts, routers, and DNS to support IPv6. Because this migration might take years, IPv6/IPv4 nodes must be able to coexist over IPv4 infrastructures such as the Internet and Intranets. (Davies 2012, 283–289.)

Implementation should be carried out within isolated networks, and then these networks have to be interconnected with other networks over existing IPv4 Infrastructures. In order to connect these isolated networks different transition technologies are needed. (Davies 2012, 283–298.) The Internet Engineering Task forces (IETF) has defined the different protocols, mechanism, tools and procedure in order to transition to IPv6. According to Graziani (2012) these techniques are divided into three groups: Dual Stack, Tunneling and Translation.

According to Nordmark and Gilligan (2000) specify different mechanisms for transition from IPv4 to IPv6 in host and routers for instance, Dual Stack and tunneling.

5.1 Dual Stack

The adoption of new technology depends on its easy integration with the existing infrastructure without significant disruption of service. Dual stack is a most common technique for integration of IPv6. It contains both IPv4 and IPv6 Internet layers with separate protocol stacks. Further, these protocol stacks contain separate implementations of transport layer protocols, such as TCP and UDP. As a result, dual stacked device simultaneously communicates with IPv4 and IPv6 devices, agreeing on which IP version to use. However, the transition from IPv4 to IPv6 does not require upgrades on all nodes at the same time; IPv4 and IPv6 will coexist for long time from now. (Hagen 2006, 255-260; Davies 2012, 283–288.)

Even though a node may be equipped to support both protocols, one or the other stack may be disabled for operational reasons. A stack being enabled has IP addresses assigned, but whether or not any particular application is available on the stacks is explicitly not defined. Thus, According to Nordmark and Gilligan (2000) IPv6/IPv4 nodes may be operated in one of three modes:

With their IPv4 stack enabled and their IPv6 stack disabled.

With their IPv6 stack enabled and their IPv4 stack disabled.

With both stacks enabled.

IPv6/IPv4 nodes with their IPv6 stack disabled will operate like IPv4-only nodes. Similarly, IPv6/IPv4 nodes with their IPv4 stacks disabled will operate like IPv6-only nodes. IPv6/IPv4 nodes MAY provide a configuration switch to disable either their IPv4 or IPv6 stack.

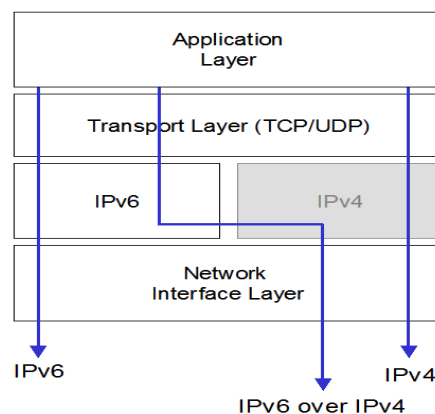


Figure 18. Dual-Stack Mechanism in OSI References Model (Davies 2012)

5.2 Tunneling

Tunneling is one of method for migration to IPv6 network infrastructure to transfer data. In this method, IPv6 clients communicate with each other over an IPv4 infrastructure through a tunnel. IPv6 tunneling enables IPv6 nodes to communicate with other IPv6 nodes over the existing IPv4 Internet.

Additionally, tunneling comfort for the IPv6 deployment by maintaining compatibility with the large existing IPv4 network. (Hagen 2006, 255–259; Davies 2012, 283–298.)

Tunneling is a mechanism of encapsulating the IPv6 packets within an IPv4 header. In the IPv4 header, protocol field is set to 41 indicating IPv6 has been encapsulated. Furthermore, the encapsulated packet consist source and destination IPv4 address of tunnel endpoints. (Blanchet 2006, 278–287.) IPv6 tunneling facilitates the IPv6 nodes to bridge with other IPv6 nodes over the existing IPv4 Internet. As a result, encapsulated packet travels across the IPv4 Internet till they reached the destination nodes, and then the packet is de-encapsulate and forwarded to the final destination. (Nordmark–Gilligan 2000.)

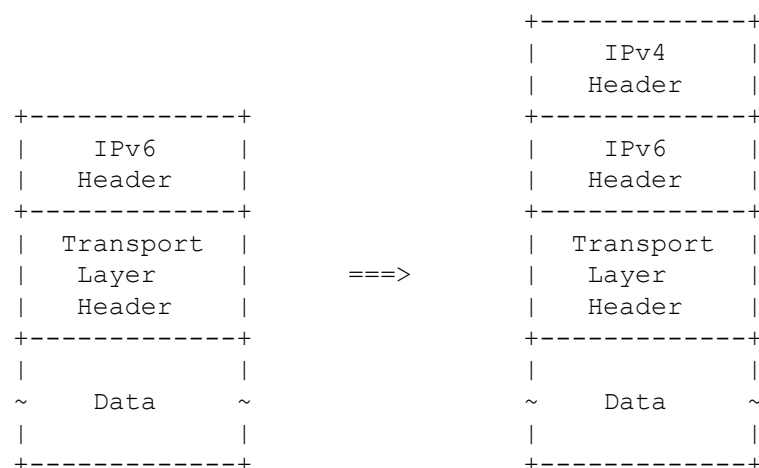


Figure 19. Encapsulations IPv6 in IPv4 (Nordmark & Gilligan 2000)

5.2.1 Generic Routing Encapsulation Tunnel

GRE is a manual tunneling also known as configured tunnel. Whenever implementing GRE, the tunnel endpoint addresses are determined from configuration in the encapsulating mode. For each tunnel, the encapsulating mode must be store in the tunnel endpoints addresses. GRE tunnel can carry other than IP protocols for instance IPX/SPX. (Graziani 2012; Nordmark & Gilligan 2000.)

5.2.2 Intrasite Automatic Tunnel Addressing protocol (ISATAP)

ISATAP automatic tunneling technology mainly used to provide IPv6 connectivity between IPv6/IPv4 hosts across an IPv4 network. Further, this technology is used within private organization, as these addresses are not routable in the Internet. (Hagen 2012, 290–299.)

Host using the standard addresses autoconfiguration mechanism automatically configures ISATAP tunneling. The ISATAP router is responsible for resolving IPv6 to an IPv4 address. And, the host communicates with ISATAP router by using IPv4. The router provides the host with information about the IPv6 ISATAP network prefixes, and default gateway. (Hagen 2012, 293–298.) Tunnel endpoints for automatic tunnels are determined by the use of routes, next-hop addresses based on destination IPv6 addresses, and logical tunnel interfaces. Automatic tunneling allows both IPv4 and IPv6 nodes to communicate over the IPv4 routing infrastructure without pre-configuring tunnels. (Davies 2012, 290–298.)

5.2.3 Teredo Tunneling

As defined by Nordmark and Gilligan (2000) in RFC 2893 an automatic tunneling manual configuration is not required, rather tunnel are created dynamically. Teredo is one of the automatic IPv6 transition technologies that allow IPv6/IPv4 nodes to communicate using global IPv6 addresses, distant by NAT devices. IPv6 traffic travel through NAT devices without having to configure the NAT in a Teredo based technology. Teredo use special IPv6 addresses are global addresses, unique to the Internet.

5.2.4 6to4 Tunneling

According to Carpenter and Moore (2001) as defined in RFC 3056 6to4 is an automatic tunneling that provide unicast IPv6 connectivity between IPv6 sites and the hosts across the IPv4 Internet. Nodes on individual network configured their addresses automatically with both a 64-bit prefix. And the 6to4 router is configured with a 6to4 pseudo-interface. The 6to4 router is always the edge router connected to public IPv4 Internet.

The IPv6 traffic that does not match any of the network prefixes on routing table is forwarded to a 6to4 router. The 6to4 router has a static default route that forwards traffic to other 6to4 sites. The 6to4 router on the site border also has a default route `::/0` that forwards traffic to a 6to4 relay.

5.3 Translation

Even though, IPv6 is developed to completely replace IPv4 and discipline of Network Address Translation (NAT). Implementation of IPv6 will happen in increments during the foreseeable future. The IETF defined Translation to accumulate the various network scenarios in order to implement IPv6. (Bagnulo–Matthews–Beijnum 2011.) According to Graziani (2012) translation is the process of translating IP header and address between the communicating networks. Although, translation is a shorter solution, and offer some advantages over the other technologies such as tunneling they are:

- Translation provides a means for gradual and seamless migration to Ipv6.

- Content providers can provide services transparently to IPv6 Internet Users.

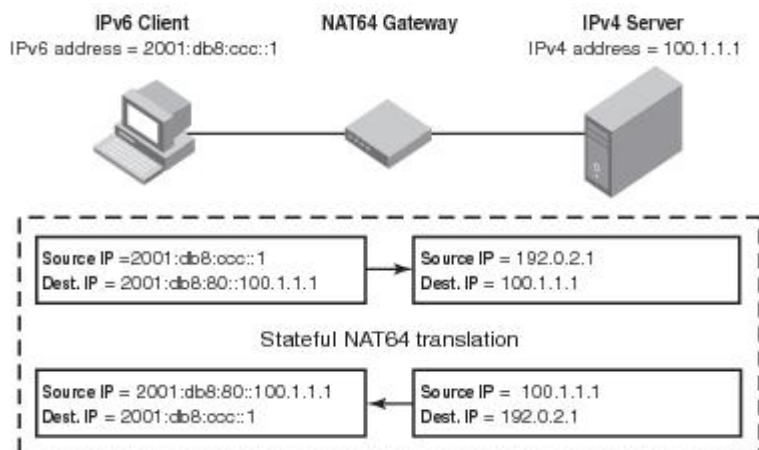


Figure 21. IPv6 and IPv4 Network Using NAT64 (Graziani 2012)

5.3.2 Nat-PT

NAT-PT works similar to NAT mechanism as in IPv4 environment, translating RFC 1918 private addresses to global public addresses and vice-versa. NAT-PT is a mechanism used to translate IPv4 addresses to IPv6 addresses and also IPv6 addresses to IPv4 using 96-bit IPv6 prefix. (Graziani 2012.) NAT-PT is a short-term solution only used if there is no other mechanism to communicate IPv6 nodes to IPv4 nodes (Tsirtsis–Srisuresh 2000).

NAT-PT uses a pool of unique globally routable IPv4 address to be translated for IPv6 nodes. NAT-PT offers a straightforward solution based on transparent routing and address/protocol translation, allowing a large number of applications in IPv6 and IPv4 realms to inter-operate without requiring any changes to these applications.

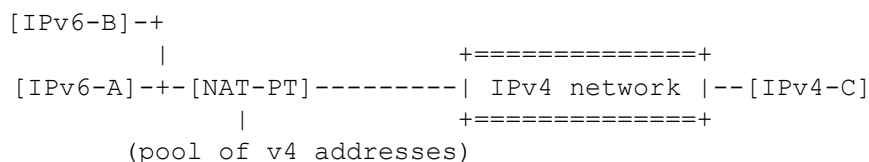


Figure 22. NAT-PT (Tsirtsis–Srisuresh 2000)

5.4 Tunnel Broker

According to Durand, Fasano, Guardini and Lento (2001), Tunnel Broker is a service provides by virtual IPv6 ISP providing communication across IPv4 network to IPv6 clients. The tunnel brokers administer the establishment, maintenance and end the session of tunnel on behalf of the Internet users. The Tunnel brokers transfer the data packets across the tunnel using IPv4 addresses. Durand et al (2001) defines the basic operation of Tunnel broker using a model knows as tunnel Broker Model, illustrated in following diagram:

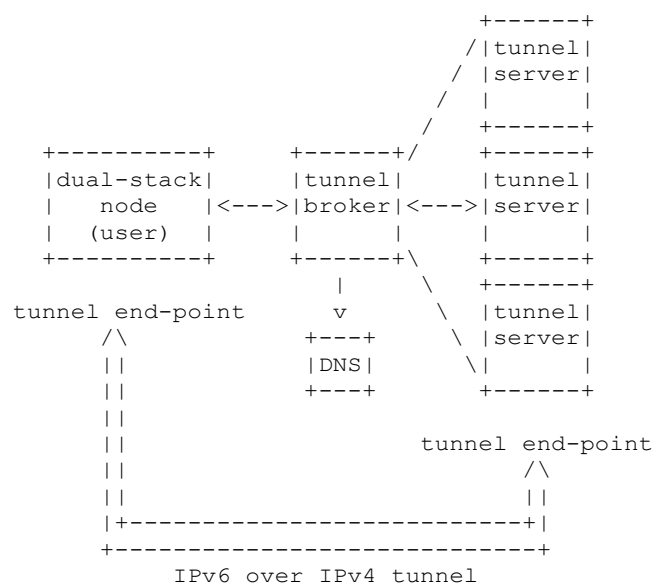


Figure 23. The Tunnel Broker Model (Durand et al 2001)

The Tunnel server is a dual-stack router connected to the global Internet. Furthermore, when the tunnel has been configured between tunnel server and user the Tunnel Broker establish, maintain, and end the session the server part of the tunnel. (Durand et al 2001.) Moreover, tunnel client is a dual-stack node connected to the Internet over IPv4. These clients have to authenticate in order to create tunnel through tunnel broker. Then the tunnel broker provides their IPv4 address, a name for the registration of its IPv6 address in DNS and also, additional information for instance, IPv6 prefix. (Durand et al 2001.)

6 UPGRADE PLAN

6.1 Introduction

Today organizations are aware of customer requirements to support IPv6. This is because of the consequence that World approaching the exhaustion and to enhance the IPv6 infrastructure across global Internet and imminent availability of IPv6 to their customers. However, the organization must have sustainable and legitimate ambition to initiate the IPv6 deployment strategies. They need to understand the business requirements, consideration and imprint IPv6 to production environment.

The limited infrastructures of global Internet have already started the deployment of IPv6. Further, the most acceptable deployments of IPv6 today are being observed in limited scale, contained in the core areas of their networks. These deployments are implemented precisely by the means of deploying dual stack schemes, encapsulating or translating one IP technology into another.

6.2 Evaluation of Current Network

In order for deploying IPv6 to an already existing network it is essential to have basic understanding of the organization network. This section mainly concerns with current layout RAMK network. Furthermore, this network may resemble with other organization network and for other network a different IPv6 plan is carried out. The following figure illustrates the network design of RAMK:

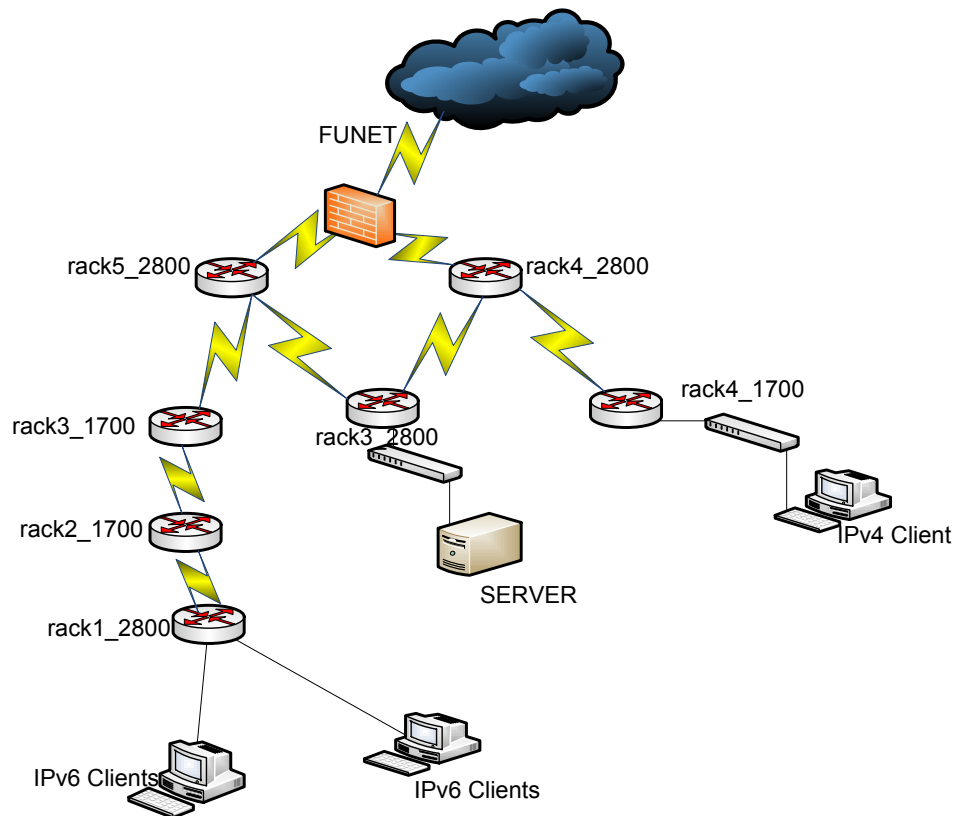


Figure 24. RAMK Network

Interoperability with IPv6 is mainly concern with software or firmware. The older devices that could not be upgraded are likely to be replaced instead. However, RAMK most networking devices have recent operating system and software or firmware need to be update.

The inventories list of RAMK infrastructure and operating system (OS) currently deployed at RAMK network are summarized following table.

Table 5. Inventory List

Device Type	Operating system
PC and Workstation	Windows 7 Windows 8 Mac OS X
Server	Windows Server 2012
Routers	Cisco 2800 & 1700 series
Switches	Cisco Catalyst 2900 Series

All the operating systems and the network devices that were deployed found to be IPv6 compatible but the ones that were not compatible would be upgraded

6.3 Addressing Plan

RAMK has been assigned *2001:db8:aabb:ef::/56* IPv6 provider independent prefix. Further, subnetting has been done according to the size of network needed for the departments. The details addressing used in the RAMK network is explained in following table.

Table 6. Addressing Plan

<i>NETWORK</i>	<i>ADDRESS</i>
FUNET	2001:DB8:AABB:EF11::/64
SERVER	2001:DB8:AABB:EFAB::/64
TUNNELING	2001:DB8:AABB:EFAA::/64
CLASSROOM	2001:DB8:AABB:EFAC::/64
DMZ	2001:DB8:AABB:EF01::/64

7 IMPLEMENTATION OF IPv6

7.1 Introduction

This project is carried using the Cisco equipment's and Windows devices. The IPv6 has been configured mainly on Cisco routers 2800, Windows Server 2012, Windows 8, Windows 7 and finally on MAC OS X.

Cisco devices running the IOS 12.2(2) and later version support IPv6. However, in Cisco routers IPv6 services are not enable by default. Hence the IPv6 services have to be manually enables by using *ipv6 unicast-routing* from global configuration mode as shown below:

```
rack5_ROUTER_2800 (config)#ipv6 unicast-routing
```

After enabling the IPv6 services on the routers, IPv6 addresses have been configured to each interface. Both the global as well as link local addresses have been assigned as static addresses. The following commands have been issued at the interface mode:

```
rack5_ROUTER_2800(config)# interface FastEthernet0/0  
rack5_ROUTER_2800(config-if)# ipv6 enable  
rack5_ROUTER_2800(config-if)# ipv6 address FE80::1 link-local  
rack5_ROUTER_2800(config-if)#ipv6 address  
2001:DB8:AABB:EF06::1/64  
rack5_ROUTER_2800(config-if)#no ip address  
rack5_ROUTER_2800(config-if)# duplex auto  
rack5_ROUTER_2800(config-if)# speed auto
```

Followed by the interface configuration, *show ipv6 interface brief* command has been issued to verify the configuration. Furthermore, to check the basic connectivity between the routers interfaces *ping* commands have been issued.

```
rack5_ROUTER_2800#show ipv6 interface brief
FastEthernet0/0      [up/up]
    FE80::1
    2001:DB8:AABB:EF06::1
FastEthernet0/1      [administratively down/down]
    unassigned
Serial0/0/0          [up/up]
    FE80::1
Serial0/0/1          [up/up]
    FE80::1
    2001:DB8:AABB:EF02::1
Tunnel0              [up/up]
    FE80::C0A8:101
    2001:DB8:AABB:EFAA::2
```

```
rack5_ROUTER_2800#ping 2001:DB8:AABB:EF06::1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:DB8:AABB:EF06::1, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/6/8 ms

The ping test has proved that there is connectivity using IPv6 addresses.

The Microsoft has release the IPv6 stack in 1998 and almost all operating system of Microsoft support IPv6. In the Windows Server 2012, the IPv6 services are enable by default and only IPv6 address are configures as shown in following figure:

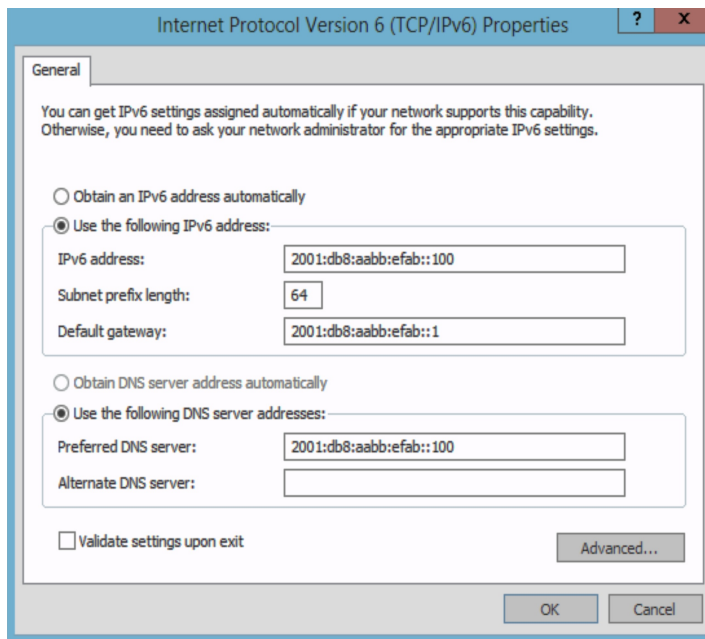


Figure 25. IPv6 Configuration in Server 2012

7.2 DHCP and DNS

DHCP is used to assign IP addresses for end devices, such as laptops, and desktops in the network automatically. RAMK networks have one DHCPv6 server providing services to the client. Previously, RAMK network has been configured DHCPv4 server for providing IPv4 address through stateful autoconfiguration. Although IPv6 addresses are very large, IPv6 to client devices are going to configure its IPv6 address through stateless autoconfiguring. However, client devices will receive the DNS and other information stateful DHCP autoconfiguration. The following figure illustrates the configuration of DNS A records in Windows server 2012.

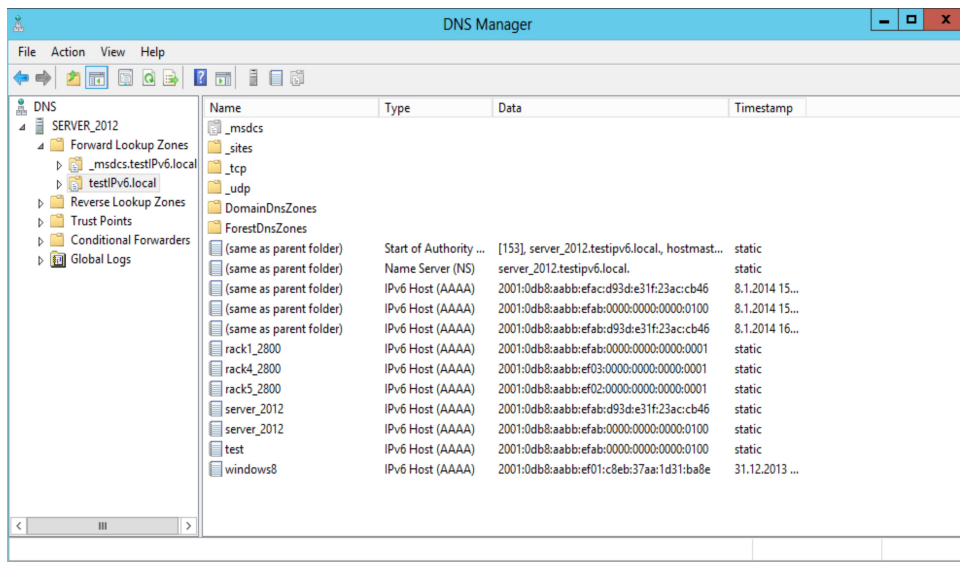


Figure 26. IPv6 DNS A records

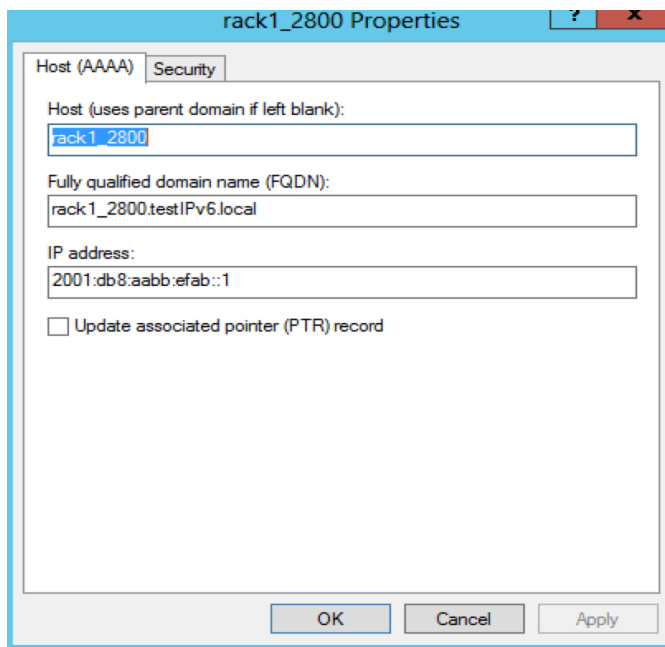
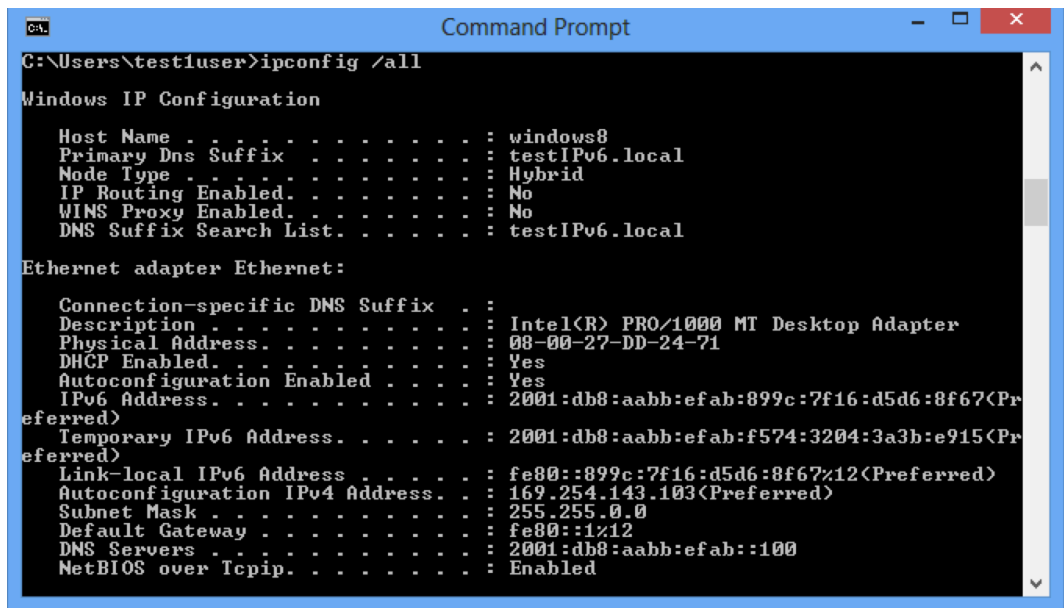


Figure 27. IPv6 DNS Record.

The routers have been configured as a DHCP relay agent, propagating the client DHCP message to server and gets a reply with the DHCP replay message. The following command has been configured on the routers:

The Windows 8 workstation followed the DHCPv6 stateless autoconfiguration process and was able to acquire the IPv6 address from stateless autoconfiguration and other network parameters e.g. DNS from state full auto configuration (DHCPv6)



```

C:\Users\testluser>ipconfig /all

Windows IP Configuration

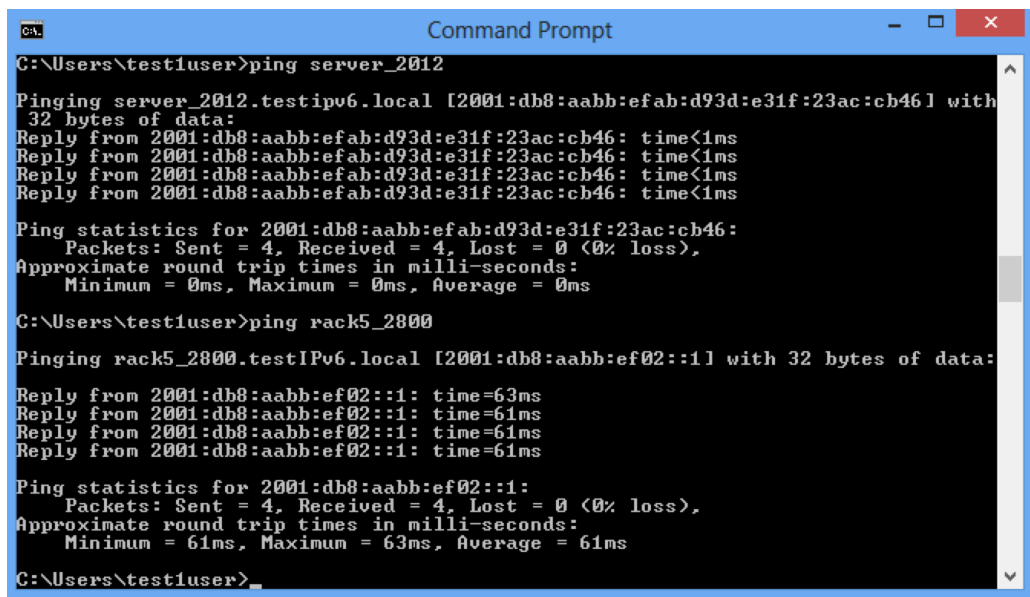
    Host Name . . . . . : windows8
    Primary Dns Suffix . . . . . : testIPv6.local
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : testIPv6.local

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix . . . :
    Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Physical Address. . . . . : 08-00-27-DD-24-71
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
    IPv6 Address. . . . . : 2001:db8:aabb:efab:899c:7f16:d5d6:8f67(Preferred)
    Temporary IPv6 Address. . . . . : 2001:db8:aabb:efab:f574:3204:3a3b:e915(Preferred)
    Link-local IPv6 Address . . . . . : fe80::899c:7f16:d5d6:8f67%12(Preferred)
    Autoconfiguration IPv4 Address. . . : 169.254.143.103(Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . : fe80::1:12
    DNS Servers . . . . . : 2001:db8:aabb:efab::100
    NetBIOS over Tcpip. . . . . : Enabled
  
```

Figure 28. IPv6 Stateless Autoconfiguration in Windows 8 PC

Following the IPv6 autoconfiguration in Windows 8 PC, ping command has been issued to test the DNS resolution and the output is shown in following figure.



```

C:\Users\testluser>ping server_2012

Pinging server_2012.testipv6.local [2001:db8:aabb:efab:d93d:e31f:23ac:cb46] with 32 bytes of data:
Reply from 2001:db8:aabb:efab:d93d:e31f:23ac:cb46: time<1ms
Reply from 2001:db8:aabb:efab:d93d:e31f:23ac:cb46: time<1ms
Reply from 2001:db8:aabb:efab:d93d:e31f:23ac:cb46: time<1ms
Reply from 2001:db8:aabb:efab:d93d:e31f:23ac:cb46: time<1ms

Ping statistics for 2001:db8:aabb:efab:d93d:e31f:23ac:cb46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\testluser>ping rack5_2800

Pinging rack5_2800.testIPv6.local [2001:db8:aabb:ef02::1] with 32 bytes of data:

Reply from 2001:db8:aabb:ef02::1: time=63ms
Reply from 2001:db8:aabb:ef02::1: time=61ms
Reply from 2001:db8:aabb:ef02::1: time=61ms
Reply from 2001:db8:aabb:ef02::1: time=61ms

Ping statistics for 2001:db8:aabb:ef02::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 61ms, Maximum = 63ms, Average = 61ms

C:\Users\testluser>_
  
```

Figure 29. Test for DNS Name Resolutions

7.3 Routing

Enhance Interior Gateway Routing Protocols (EIGRP) originally Cisco proprietary protocols, however in 2013 it was made open standard. RAMK is currently using Cisco EIGRP as the internal routing protocol because of the fact that EIGRP allowing faster network convergence.

EIGRP use the DUAL algorithm in order to calculate the best path across the network. Furthermore, it guarantees loop-free network at every instant throughout a route calculation and allows fast convergence.

In order to enable the EIGRP, *EIGRP* process have to be enable from global configuration mode, along with the *router id*. The EIGRP process will use the IPv4 address, as router id, if one configured, if not manually router id have to be configured and finally *no shutdown* has to be issued. However, router 5 have already configured with IPv4 address. The configuration of EIGRP has been shown as follow:

```
rack5_ROUTER_2800(config)#ipv6 router eigrp 1
rack5_ROUTER_2800(config-rtr)#no shutdown
```

EIGRP was directly configured on each interface for instances Fast Ethernet 0/1. The following command has been issued to configure EIGRP for IPv6:

```
rack5_ROUTER_2800(config)# interface FastEthernet0/0
rack5_ROUTER_2800(config-if)# ipv6 eigrp 1
```

After the configuration of EIGRP in each interface, the *show ipv6 route eigrp* command has been issued to show all the EIGRP learned routes.

```
rack5_ROUTER_2800#show ipv6 route eigrp
IPv6 Routing Table - default - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static
route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS
summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 -
OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
D 2001:AB8:AABB:EF05::/64 [90/2172416]
  via FE80::2, Serial0/0/1
D 2001:DB8:AABB:EF03::/64 [90/2681856]
```

```

via FE80::2, Serial0/0/1
D 2001:DB8:AABB:EF04::/64 [90/2172416]
via FE80::2, Serial0/0/1
D 2001:DB8:AABB:EFAB::/64 [90/26882560]
via FE80::C0A8:401, Tunnel0

```

7.4 Tunneling

RAMK network consists of fewer IPv4 infrastructures that were not able to support IPv6. Hence tunneling has been configured to communicate with isolated IPv6 networks. The tunnels allowed stable secure connections between two dual-stack edge routers.

Manual tunnel has been configured with an IPv6 address on a tunnel interface. Furthermore, IPv4 addresses have been assigned to tunnel source and destination that are reachable in the network. This method was used to interconnect the different IPv6 test devices in the network when the RAMK network was not IPv6 ready.

```

rack5_ROUTER_2800(config)# interface Tunnel0
rack5_ROUTER_2800(config-if)# no ip address
rack5_ROUTER_2800(config-if)#          ipv6          address
2001:DB8:AABB:EFAA::2/64
rack5_ROUTER_2800(config-if)# tunnel source Serial0/0/0
rack5_ROUTER_2800(config-if)# tunnel mode ipv6ip
rack5_ROUTER_2800(config-if)# tunnel destination 192.168.4.1
rack5_ROUTER_2800(config-if)# ipv6 eigrp 1

```

Followed by the tunnel interface configuration, show ipv6 interface tunnel 0 has been issued. This command verifies the configuration and provides useful information as shown below:

```

rack5_ROUTER_2800#show ipv6 interface tunnel 0
Tunnel0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::C0A8:101
No Virtual link-local address(es):

```


Global unicast address(es):
 2001:DB8:AABB:EFAA::2, subnet is
 2001:DB8:AABB:EFAA::/64

Joined group address(es):
 FF02::1
 FF02::2
 FF02::A
 FF02::1:FF00:2
 FF02::1:FFA8:101

MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ICMP unreachable are sent
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds (using 30000)
Hosts use stateless autoconfig for addresses.

Furthermore, using wireshark tool a live IP packet has been capture, carrying IPv6 data inside IPv4 packet as shown following figure:

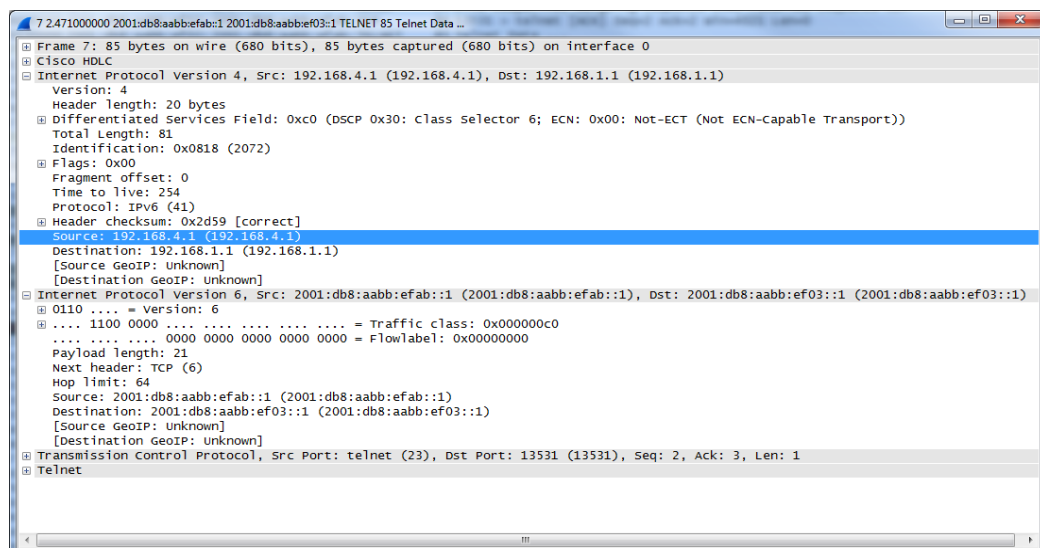


Figure 30. IPv6 Packet Inside IPv4 packet

7.5 Zone Based Firewall

The zone-based firewall is one of the advanced IOS based feature available in Cisco routers. This feature provides advanced traffic filtering or inspection

of IPv6 packets. Furthermore, the zone-based policy firewall supports the inspection of IPv6 packets for instance, ICMP, TCP, and UDP.

In zone-based firewall, a traffic class identifies a set of packets based on its contents. These contents are manually configured as required by a particular network. Additionally, policy has to be configured to take action that is associated with a traffic class for instance to drop, and pass actions for a class. And finally, these actions pass the traffic from one zone to another.

In order to implement security firstly different zones have to be configured and corresponding interfaces as shown below:

```
rack5_ROUTER_2800#show zone security
zone self
  Description: System defined zone
zone INSIDE
  Member Interfaces:
    FastEthernet0/1
zone OUTSIDE
  Member Interfaces:
    FastEthernet0/0
zone DMZ
  Member Interfaces:
    Serial0/0/1
```

After configuring the zones different policy has been configured to inspect the IPv6 packets.

```
rack5_ROUTER_2800#show policy-map type inspect
Policy Map type inspect PMAP
  Class CMAP
    Inspect
  Class class-default
    Drop

rack5_ROUTER_2800# show class-map type inspect
```

Class Map type inspect match-any CMAP (id 1)

Match protocol http

Match protocol https

Match protocol ssh

Match protocol telnet

Match access-group name in-2-out

Finally, the policy has been linked to the different zones as shown below:

```
rack5_ROUTER_2800#show zone-pair security
```

```
Zone-pair name in-2-out
```

```
Source-Zone INSIDE Destination-Zone OUTSIDE
```

```
service-policy PMAP
```

9 CONCLUSION

In today's internetworks the deployment of IPv6 is yet to be accomplished on many front lines. Not only business need but also administrative procedures for transition to IPv6 have to be developed.

IPv6 is a next generation technology and have overcome many of the limitations of IPv4, while introducing new features and functionality. In addition, IPv6 has introduced mobile IP providing roaming potential to mobile nodes, regardless of its location in network. Furthermore, advance security has been embedded to IP stack. Finally, IPv6 provides plentiful of addresses space and is designed to expand the Internet services.

IPv6 supports multiple addresses assignment in an interface that makes it possible for a node to assemble in more than one network and utilize the resources available at the same time. Since the two protocols IPv6 and IPv4 can work together but independently, they might co-exist for longer time than expected so it is sensible to be dual stack than IPv6-only at current situation.

The goal of this project was to create a gradual procedure and mechanism to deploy IPv6 to production network. Firstly, RAMK has deployed IPv6 on all the existing IPv4 network links, enabling both unicast and multicast IPv6 traffic. Secondly, RAMK has enabled many network and application services dual stack including our external facing web server and DNS services. And finally, the overall IPv6 deployment experience has been very positive for RAMK.

BIBLIOGRAPHY

- Bagnulo, M. – Matthews, P. – Beijnum, I. 2011. Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers. Address: <http://www.ietf.org/rfc/rfc6146>. Accessed 20 November 2013.
- Banstola, B. 2012. IPv6 Implementation, Firewall and Redundancy. Licentiate thesis. Vaasa University of Applied Sciences: Faculty of Information Technology.
- Blanchet, M. 2006. Migration to IPv6. England: John Wiley & Sons Ltd.
- Carpenter, B. – Moore, K. 2001. Connections to IPv6 domains via IPv4 Clouds. Address: <http://www.ietf.org/rfc/rfc3056>. Accessed 3 January 2014.
- Cisco System Inc. 2005. IPv6 Header At a Glance. Address: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80260042.pdf. Accessed 24 November 2013.
- Cisco System Inc. 2007. IPv6 Addressing. Address: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8026003d.pdf. Accessed 23 November 2013.
- Cisco System Inc. 2008. IPv6 Extension Headers Review and Consideration. Address: http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html. Accessed 23 November 2013.
- Cisco System Inc. 2012. IPv6 Addressing Guide. Address: http://www.cisco.com/en/US/docs/solutions/SBA/August2012/Cisco_SBA_BN_IPv6AddressingGuide-Aug2012.pdf. Accessed 22 November 2013.
- Conta, A. – Deering, S. – Gupta, M. 2006. Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification. Address: <http://tools.ietf.org/html/rfc3775>. Accessed 10 November 2013.
- Das, K. 2008. IPsec and IPv6- Securing the NextGen Internet. Address: <http://ipv6.com/articles/security/IPsec.htm>. Accessed 10 November 2013.
- Davies, J. 2012. Understanding IPv6. 3rd edition. California: O'really media, Inc.
- Deering, S. – Hinden, R. 1998a. Internet Protocol, Version 6 (IPv6) Specification. Address: <http://www.ietf.org/rfc/rfc2460>. Accessed 23 October 2013.
- 1998b. IPv6 Multicast Address Assignments. Address: <http://www.ietf.org/rfc/rfc2375>. Accessed 27 December 2013.

- Deering, S. – Hinden, R. 2006. Internet Protocol, Version 6 (IPv6) Addressing Architecture. Address: <http://www.ietf.org/rfc/rfc4291>. Accessed 15 October 2013.
- Del Ray, M. 1981. Internet Protocol. Address: <http://tools.ietf.org/html/rfc791>. Accessed 4 October 2013.
- Droms, R. – Bound, J. – Lemon, T. – Perkins, C. – Carney, M. 2003. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). Address: <http://www.ietf.org/rfc/rfc3315>. Accessed 17 October 2013.
- Droms, R. 2004. Dynamic Host Configuration Protocol (DHCP) Services for IPv6. Address: <http://www.ietf.org/rfc/rfc3736>. Accessed 18 October 2013.
- Durand, A.– Fasano,P.– Guardini, I. – Lento, D. 2001. IPv6 Tunnel Broker. Address: <http://www.ietf.org/rfc/rfc3053>. Accessed 20 November 2013.
- Dye, M. A.– McDonald, R.– Ruff, A. W. 2010. Network fundamentals: CCNA Exploration Companion Guide. 9th edition. Indianapolis: Cisco Press.
- Francis, P. – Egevang, K. 1994. The IP Network Address Translator (NAT). Address: <http://tools.ietf.org/html/rfc1631>. Accessed 25 October 2013.
- Graziani, R. 2012. IPv6 Fundamentals. Indianapolis: Cisco Press.
- Hagen, S. 2006. IPv6 Essentials. California: O'really Media, Inc.
- Jonson, D. – Perkins, C. – Arkko, J. 2004. The Internet Society. Mobility Support in IPv6. Address: <http://tools.ietf.org/html/rfc3775>. Accessed 18 November 2013.
- Kent, S. – Atkinson, R. 2006. Security Architecture for the Internet Protocol. Address: <http://www.ietf.org/rfc/rfc2401>. Accessed 25 October 2013.
- Khan, R. – Sindi, F.U. 2012. Necessity to Migrate to IPv6. IEEE: International Conference on Information Society.210-214.
- Liu, C. 2011. DNS and BIND on IPv6: DNS and IPv6. 1st edition. California: O'really Media, Inc.
- Loukola, M.V. – Skytta, J.O. 1998. New Possibilities Offered by IPv6. IEEE. 548-552.
- Mcfarland, S.– Sambhi, M. – Sharma, N. – Hooda, S. 2011. IPv6 for Enterprise Networks.Hierarcial Network Design. Indianapolis: Cisco Press.

- Nguyen, P.M.N. 2012. Transition from IPv4 to IPv6 Best Method for Large Enterprise Networks. Licentiate thesis. Lahti University of Applied Sciences: Faculty of Business Information Technology.
- Nordmark, E. – Gilligan, R. 2000. Transition Mechanisms for IPv6 Hosts and Routers. Address: <http://www.ietf.org/rfc/rfc4213>. Accessed 12 November 2013.
- Nordmark, E. – Narten, T.– Simpson, W.1998. Neighbor Discovery for IP version 6 (IPv6). Address: <http://www.ietf.org/rfc/rfc2461>. Accessed 12 October 2013.
- Odom, W. 2012. CCENT/CCNA ICND1: 640-822 Official Certification Guide. 3rd editions. Indianapolis: Cisco Press.
- Rockell, R. – Wegner, J.D. 2000. IP Addressing and Subnetting, Including IPv6. Rockland, Mass: Syngress Media.
- Sportack, M.A. 2005. TCP/IP First Step. Indianapolis: Cisco Press.
- Thomson, S. – Huitema, C. – Ksinant, V.– Souissi, M. 2003. DNS Extension to Support IP version 6 Address: <http://www.ietf.org/rfc/rfc3596>. Accessed 07 October 2013.
- Thomson, S. – Narten, T. – Jinmei, T. 2007. IPv6 Stateless Address Autoconfiguration. Address: <http://www.ietf.org/rfc/rfc4864>. Accessed 15 October 2013.
- Troan, O. – Droms, R. 2003. IPv6 Prefix Option for Dynamic Host Configuration Protocol (DHCP) version 6. Address: <http://www.ietf.org/rfc/rfc3633>. Accessed 22 October 2013.
- Tsirsis, G. – Srisuresh, P. 2000. Network Address Translation - Protocol Translation (NAT-PT). Address: <http://www.ietf.org/rfc/rfc2766>. Accessed 20 November 2013.
- Tyson, J. 2013. How Internet Infrastructure Work. How Stuff Works. Address: http://computer.howstuffworks.com/internet/basics/internet_infrastructure.htm. Accessed 23 November 2013.
- Vyncke, E.– Hogg, S. 2008. IPv6 Security. Indianapolis: Cisco Press.

```
rack3_ROUTER_1700#sh run
Building configuration...
Current configuration : 941 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname rack3_ROUTER_1700
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$7Ms.$zBTduLOj5t5QY9HDTItyn0
!
no aaa new-model
ip cef
!
no ip domain lookup
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
interface FastEthernet0/0
 no ip address
 speed auto
!
interface Serial0/0
 ip address 192.168.1.2 255.255.255.0
 no fair-queue
 clock rate 56000
!
interface Serial0/1
 ip address 192.168.3.1 255.255.255.0
 clock rate 64000
!
interface Ethernet1/0
 no ip address
 shutdown
 half-duplex
!
router rip
 version 2
 network 192.168.1.0
 network 192.168.3.0
!
ip forward-protocol nd
```



```
!  
no ip http server  
!  
control-plane  
!  
line con 0  
password 7 045802150C2E  
login  
line aux 0  
line vty 0 4  
password 7 00071A150754  
login  
line vty 5 15  
password 7 110A1016141D  
login  
!  
end
```

```
rack2_ROUTER_1700_TOP#show running-config  
Building configuration...
```

```
Current configuration : 873 bytes
```

```
!  
version 12.4  
service timestamps debug datetime msec  
service timestamps log datetime msec  
service password-encryption  
!  
hostname rack2_ROUTER_1700_TOP  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$LK1m$R9XtJbYw5Y1p4tB75sHkq.  
!  
no aaa new-model  
ip cef  
!  
no ip domain lookup  
multilink bundle-name authenticated  
!  
archive  
log config  
hidekeys  
!  
interface FastEthernet0/0  
no ip address  
speed 100  
full-duplex  
!  
interface Serial0/0  
ip address 192.168.3.2 255.255.255.0  
no fair-queue
```

```
!  
interface Serial0/1  
 ip address 192.168.4.2 255.255.255.0  
!  
interface Ethernet1/0  
 ip address 192.168.5.2 255.255.255.0  
 half-duplex  
!  
router rip  
 version 2  
 network 192.168.3.0  
 network 192.168.4.0  
!  
ip forward-protocol nd  
!  
no ip http server  
!  
control-plane  
!  
line con 0  
 password 045802150C2E  
 login  
line aux 0  
line vty 0 4  
 password 110A1016141D  
 login  
!  
end  
  
rack5_ROUTER_2800#sh run  
Building configuration...  
Current configuration : 2273 bytes  
!  
! Last configuration change at 12:51:54 UTC Fri Jan 10 2014  
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname rack5_ROUTER_2800  
!  
boot-start-marker  
boot-end-marker  
!  
enable secret 5 $1$/MdS$OL9B5kIEj2glst.eZMmJW0  
!  
no aaa new-model  
!  
dot11 syslog  
ip source-route  
!
```

```
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
license udi pid CISCO2811 sn FCZ132271ED
!
redundancy
!
class-map type inspect match-any CMAP
  match protocol http
  match protocol https
  match protocol ssh
  match protocol telnet
  match access-group name in-2-out
!
policy-map type inspect PMAP
  class type inspect CMAP
  inspect
  class class-default
  drop
!
zone security INSIDE
zone security OUTSIDE
zone security DMZ
zone-pair security in-2-out source INSIDE destination OUTSIDE
  service-policy type inspect PMAP
!
interface Tunnel0
  no ip address
  ipv6 address 2001:DB8:AABB:EFAA::2/64
  ipv6 eigrp 1
  tunnel source Serial0/0/0
  tunnel mode ipv6ip
  tunnel destination 192.168.4.1
!
interface FastEthernet0/0
  no ip address
  zone-member security OUTSIDE
  duplex auto
  speed auto
  ipv6 address FE80::1 link-local
  ipv6 address 2001:DB8:AABB:EF06::1/64
  ipv6 enable
  ipv6 eigrp 1
!
interface FastEthernet0/1
```

```
no ip address
zone-member security INSIDE
duplex auto
speed auto
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:AABB:EF07::1/64
ipv6 enable
ipv6 eigrp 1
!
interface Serial0/0/0
ip address 192.168.1.1 255.255.255.0
ipv6 address FE80::1 link-local
ipv6 eigrp 1
no fair-queue
!
interface Serial0/0/1
no ip address
zone-member security DMZ
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:AABB:EF02::1/64
ipv6 eigrp 1
!
router rip
version 2
network 192.168.1.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
redistribute static
!
ipv6 access-list in-2-out
permit icmp any any
!
control-plane
!
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
transport input all
line vty 5 988
password cisco
login
transport input all
!
scheduler allocate 20000 1000
```

end

```
rack3_ROUTER_2800#sh run
Building configuration...
Current configuration : 2682 bytes
!  
! Last configuration change at 15:35:51 PCTime Wed Jan 8 2014
!  
version 15.1
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!  
hostname rack3_ROUTER_2800
!  
boot-start-marker
boot-end-marker
!  
security authentication failure rate 3 log
logging buffered 51200
logging console critical
enable secret 5 $1$UOUW$JAIs0XaPAptVrajo4fM2B/
!  
no aaa new-model
!  
clock timezone PCTime 2
clock summer-time PCTime date Mar 30 2003 3:00 Oct 26 2003 4:00
!  
dot11 syslog
no ip source-route
!  
ip cef
!  
no ip bootp server
ip domain name yourdomain.com
ipv6 unicast-routing
ipv6 cef
!  
multilink bundle-name authenticated
!  
voice-card 0
!  
license udi pid CISCO2811 sn FCZ132271E9
archive
  log config
  hidekeys
username admin privilege 15 secret 5 $1$swYP$inZHutIAAEJc0JPLgxkMS.
!
```

```
redundancy
!  
ip tcp synwait-time 10  
!  
interface FastEthernet0/0  
no ip address  
no ip redirects  
no ip unreachablees  
no ip proxy-arp  
ip flow ingress  
duplex auto  
speed auto  
ipv6 address FE80::1 link-local  
ipv6 address 2001:DB8:AABB:EF04::1/64  
ipv6 enable  
ipv6 eigrp 1  
no mop enabled  
!  
interface FastEthernet0/1  
no ip address  
no ip redirects  
no ip unreachablees  
no ip proxy-arp  
ip flow ingress  
duplex auto  
speed auto  
ipv6 address FE80::1 link-local  
ipv6 address 2001:AB8:AABB:EF05::1/64  
ipv6 eigrp 1  
no mop enabled  
!  
interface Serial0/0/0  
no ip address  
no ip redirects  
no ip unreachablees  
no ip proxy-arp  
ip flow ingress  
ipv6 address FE80::2 link-local  
ipv6 address 2001:DB8:AABB:EF03::2/64  
ipv6 eigrp 1  
clock rate 56000  
!  
interface Serial0/0/1  
no ip address  
no ip redirects  
no ip unreachablees  
no ip proxy-arp  
ip flow ingress  
ipv6 address FE80::2 link-local  
ipv6 address 2001:DB8:AABB:EF02::2/64  
ipv6 eigrp 1  
clock rate 56000
```

```
!  
ip forward-protocol nd  
ip http server  
ip http access-class 23  
ip http authentication local  
no ip http secure-server  
ip http timeout-policy idle 60 life 86400 requests 10000  
!  
logging trap debugging  
no cdp run  
  
ipv6 router eigrp 1  
 eigrp router-id 10.10.10.10  
!  
control-plane  
!  
mgcp fax t38 ecm  
!  
line con 0  
 password 7 14141B180F0B  
 login  
 transport output telnet  
line aux 0  
 login local  
 transport output telnet  
line vty 0 4  
 privilege level 15  
 password 7 0822455D0A16  
 login  
 transport input telnet  
line vty 5 15  
 privilege level 15  
 login local  
 transport input telnet  
!  
scheduler allocate 20000 1000  
end  
  
rack4_ROUTER_2800#sh run  
Building configuration...  
Current configuration : 1252 bytes  
!  
! Last configuration change at 12:46:14 UTC Tue Dec 10 2013  
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname rack4_ROUTER_2800  
!  
boot-start-marker
```

```
boot-end-marker
!
enable secret 5 $1$94Zp$tL27AOJxTXmfJjLp7Fas..
!
no aaa new-model
!
dot11 syslog
ip source-route
!
ip cef
!
no ip domain lookup
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
voice-card 0
!
license udi pid CISCO2811 sn FCZ132271E8
!
redundancy
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
duplex half
speed 10
!
interface Serial0/0/0
no ip address
ipv6 address FE80::1 link-local
ipv6 address 2001:DB8:AABB:EF03::1/64
ipv6 eigrp 1
no fair-queue
!
interface Serial0/0/1
ip address 192.168.2.1 255.255.255.0
!
router rip
version 2
network 192.168.2.0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ipv6 router eigrp 1
```



```
no shutdown
!  
control-plane
!  
line con 0
password cisco
login
line aux 0
line vty 0 4
password cisco
login
transport input all
!  
scheduler allocate 20000 1000
end
```