

Tien Dung Hoang

## **DEPLOYMENT IPV6 OVER IPV4 NETWORK INFRASTRUCTURE**

# **DEPLOYMENT IPV6 OVER IPV4 NETWORK INFRASTRUCTURE**

Tien Dung Hoang

Bachelor's thesis

Term: Spring 2015

Business Information Technology

Oulu University of Applied Sciences

## ABSTRACT

Oulu University of Applied Sciences  
Business Administration - Business Information Technology

---

Author: Tien Dung Hoang

Title of Bachelor's thesis: Research and Deploy IPv6 over IPv4 Network Infrastructure in Medium Organization

Supervisor: Jukka Kaisto

Term and year of completion: Spring, 2015

Number of pages: 52 pages

---

The purpose of this thesis is doing the research about IPv6, concentrate in how to deploy an IPv6 network based on IPv4 network without making any interruption to IPv4 network. This thesis is made for Financing and Promoting Technology Corporation (FPT) in Vietnam.

This thesis is completed in two main parts. The theoretical part is making research about IPv4 and IPv6 to have the point of view about IPv4 and IPv6 basically, and from those one, seeing the advantages of IPv6 comparing with IPv4. One of the most important research in this part is understanding about technologies and solutions to deploy IPv6 over IPv4.

The practical part is doing the simulation of IPv4 to IPv6 conversion based on a part of current network of FPT Company by using GNS3 software. This simulation will simulate a part of real network topology of FPT Company. As a result, FPT Company will evaluate the impact which can be happened when deploying IPv6 network based on current IPv4 network and make a decision should they run the next step of IPv6 deployment in company's current network system.

---

Keywords: IPv4, IPv6, IPv6 technology, GNS3, IPv6 deployment, IPv6 routing

## Contents

1	INTRODUCTION.....	6
2	IPV4 AND IPV6 – OVERVIEW AND COMPARISION .....	8
2.1	IPv4-addressing.....	8
2.1.1	IPv4 address space.....	9
2.1.2	IPv4 limitation.....	10
2.2	IPv6-addressing.....	11
2.2.1	Types and categories of IPv6 addresses .....	13
2.2.2	IPv4 and IPv6 comparison .....	15
3	DEPLOY IPV6 OVER IPV4.....	20
3.1	IPv6 deployment status.....	20
3.2	IPv6 address deployment methods.....	21
3.2.1	EUI-64 in IPv6 .....	21
3.2.2	Stateless address auto-configuration .....	23
3.2.3	DHCPv6 .....	24
3.2.4	Mobile IPv6 .....	27
3.2.5	IPv6 routing table .....	28
3.3	Static routing.....	30
3.4	Dynamic routing protocols .....	31
3.4.1	RIPng .....	32
3.4.2	EIGRP for IPv6.....	32
3.4.3	OSPFv3 .....	33
4	IPV4 TO IPV6 CONVERSION SIMULATION.....	35
4.1	GNS3 introduction.....	35
4.2	Installation and configuration on GNS3.....	35
4.2.1	GNS3 installation .....	35
4.2.2	Router in GNS3.....	36
4.2.3	Switch in GNS3.....	36
4.2.4	Hosts in GNS3 .....	37
4.3	IPv6 migration techniques.....	37
4.4	Simulation network topology and configuration.....	38

5	CONCLUSIONS AND DISCUSSION .....	42
6	REFERENCES .....	43
7	APPENDICES .....	47

# 1 INTRODUCTION

One of the most important issues in computer network industry is studying and trying to solve the growth of global Internet network. This development goes along with integration services, new service deployments, and multiple network connections. The response of IPv4 addressing method will not be enough compared to the development of global networks in the near future. Hence, to research and develop a new addressing method to overcome this limitation is an urgent requirement.

The strong development of information technology, especially in the field of computer networks does not only have to solve the problem of network traffic, but also to solve the requirement of providing addresses for network devices on Internet. There are huge address requirements for computers, mail servers, web servers, printers, Internet protocol television (IPTV), education network, online games and mobile devices connected to Internet. The word “Internet of Things” which was first documented in 1999 opened a new century when a lot of “things” in the future such as coffee machine, refrigerator, washing machine, software, and sensors can be connected and exchange data with manufacturers, operators and owners. This is a problem which needs to be solved.

Currently, the addresses of network devices on Internet are numbered according to the 4<sup>th</sup> version address generation (IPv4), consisting of 32 bits. IPv4 was introduced in RFC 791 in Sep, 1981 (IETF. 1981, cited 21.4.2015). In theory, IPv4 includes 4 billion addresses. However, because of the strong growth in number of network devices, the shortage of IPv4 addresses is inevitable. The limitation of technology and the disadvantages which cannot be reparable of IPv4 has boosted the development of new Internet address generation. IPv6 was designed to overcome the inherent limitations of IPv4 addresses. IPv6 was introduction in RFC 2460 in 1998 (IETF 1998, cited 21.4.2015). Currently, IPv6 has been standardized step by step and put into practical use. However, the conversion from IPv4 to IPv6 is facing many problems due to asynchronous devices, Internet Service Providers (ISPs) with different network infrastructures, knowledge of users and limited amount of network managers.

The target of this thesis is to conduct on the research about IPv6 for Financing and Promoting Technology Corporation (FPT), one of the largest private enterprises in Vietnam, conducting core

businesses in multi fields of ISP, technical solutions, software development, system integration, retails and finance. This thesis is divided in three chapters. Chapter 2 and 3 are theoretical parts of this thesis. The aim of chapter 2 is giving an overview on both IPv4 and IPv6, and concluding by the advantages of IPv6 comparing with IPv4. Chapter 3 concentrates on introduction about technologies and solutions to deploy IPv6, for example IPv6 address deployment methods, IPv6 routing protocol.

Chapter 4 is the practical part of this thesis. By using GNS3 software to demonstrate how to deploy IPv6 technology based on currently IPv4 technology and evaluate the impact which can be happened to current FPT company network, the final result will be used to consider if FPT company should move on to next step in deploy IPv6 to current company network in near future.

There are three main goals I want to reach after completing this thesis. The first goal is understanding the characteristics and structure of IPv6. The second one is understanding new features and technologies of IP6 comparing with IPv4, and the last one is if it can be deployed IPv6 in the simulation network system, especially based on technology platforms of Cisco System.

## 2 IPV4 AND IPV6 – OVERVIEW AND COMPARISION

On 03.02.2011, the supply of IPv4 Internet addresses had officially exhausted after 30 years of use. Internet Assigned Numbers Authority (IANA) organization allocated the last IPv4 address range for Regional Internet Registry (RIR) organizations. That did not mean that everything was terminated, nor did mean that Internet came to doomsday. IPv6 address will be the next generation on Internet. This version is designed to overcome the limitations of IPv4 protocol and add new features which need in operations and services of next network generation. (APNIC 2015, cited 30.4.2015.)

### 2.1 IPv4-addressing

IPv4 addresses use 32 bits, divides into 4 octets (each octet has 8 bits = 1 byte), counts from left to right, from bit 1 to bit 32. Each octet is separated by period. Because of using 32 bits for addressing, so the space of IPv4 is  $2^{32}$  IP addresses. The figure 1 shows the IPv4 structure.

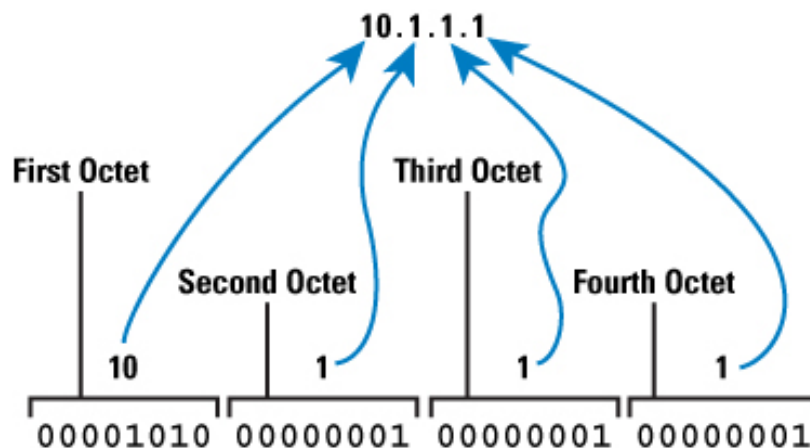


FIGURE 1. IPv4 structure (White, R 2015, cited 13.3.2015)

IP address is formed by two parts: Network-IDs and Host-IDs. On networks, routers use IP address to transfer packets from source network to destination network. Packets have to have IP address of both source and destination. When a router receives a packet, it will define the destination network, find the route from routing table, and transfer that packet through the right router interface to next router.



### 2.1.1 IPv4 address space

IPv4 is divided in 5 classes A, B, C, D and E. By using first octet (first 8 bits or first byte), an IP address can be determined which class it belongs to, and depending on that class, it can be easily determined which portion of IP address is Network-ID and Host-ID. From table 1, class of an IP address in binary can be recognized by some first bits in first octet, for example with A-class is 0, B-class is 10, C-class is 110, D-class is 1110 and E-class is 1111. For example, IP address “192.168.0.1” has the first octet is 192, so according to table 1, it belongs to C-class with the range from 192 to 223. The Network-ID of this IP address is 192.168.0.0 and Host-ID is 1. Table 1 shows the IPv4 classes.

TABLE1. IPv4 classes (Intense School and InfoSec Institute 2013, cited 13.3.2015)

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

IPv4 private address is used for private purpose such as home, office, company, organization. These addresses will not be used in Internet. Private network includes: A-class: 10.0.0.0–10.255.255.255, B-class: 172.16.0.0–172.31.255.255 and C-class: 192.168.0.0–192.168.255.255.

In every network, there is a network address and a broadcast address. Network address of a network has all bits of Host-ID equal to 0. Broadcast address of a network is using to send a message to all network-attached hosts rather than by a specific host. For example, with subnet 192.168.0.0/24, network IP address of this subnet is: 192.168.0.0; broadcast IP Address of this subnet is: 192.168.0.255

Network mask used to determines which subnet an IP address belongs to. It specifies how many bits are used for Network-ID and Host-ID. The network mask of A-class is 255.0.0.0; B-class is 255.255.0.0 and C-class is 255.255.255.0. Subnetting is a process to divide one network into two

or more than two smaller networks. In a big company or in ISP, each department or customer will have a private subnet to increase security and management.

### 2.1.2 IPv4 limitation

IPv4 only supports 32 bits, so IPv4 cannot respond to address requirements on Internet nowadays. Two major issues IPv4 are facing with are the shortage of addresses, especially B-class IPv4 address space and the dramatically increase of routing tables on the Internet.

In addition, the demand of auto-configuration has become necessary. In the first period of development, IPv4 are classified based on the size of address and divided in three commonly used classes (A, B and C). They are different in bit numbers of Network-ID and Host-ID. This way has a limitation because IPv4 addresses were drained dramatically due to using classes inefficiently.

In 1990, Classless Inter-Domain Routing (CIDR) technique was built based on address mask. CIDR was temporarily overcome the shortage of IPv4 address. The hierarchy of CIDR improved the expansibility of IPv4. This technique helped to allocate IPv4 more flexibly by using subnet mask. The length of Network-ID and Host-ID is depended on number of leading bit (bit 1) in subnet mask, so the space of IPv4 address is more flexible. (Cisco Systems, Inc 2004, cited 30.4.2015.) For example, if using C-class with subnet mask = 24 for an organization, the address range is 8 bits host-ID (= 254 hosts). This is convenient. However, CIDR disadvantage is router only can know Network-ID and Host-ID if know subnet mask.

There are some other short-time solutions such as *Address allocation for Private Internets* which was introduced in RFC 1918 (IETF 1996, cited 21.4.2015). With this solution, a part of address space will be used to be private addresses and Network Address Translation (NAT) is a technique which allows thousands of hosts can go to Internet through a few regular IP addresses. IPv4 protocol is used and maintained by NAT technique and Dynamic IPv4 Address Allocation. However, because of using these technologies, transferring data through network devices will face problems in peer-to-peer transmission, end user devices security and QoS.

## 2.2 IPv6-addressing

IPv6 addresses contains 128 bits, divides into 16 octets in binary number system or 8 groups in hexadecimal number system. Each octet has 4 hexadecimal, equal with 16 binary bits. When writing, each group of 4 octets (16 bits) is represented as unsigned integer which is written in hexadecimal form and separated by colons (:). With 128 bits are used, IPv6 will have  $2^{128} \sim 340,282,366,920,938,463,463,374,607,431,768,211,456 \sim 3.4 * 10^{38}$  IPv6 addresses. It is  $2^{96}$  times more than IPv4 address space. There is an interesting comparison between IPv4 and IPv6 is if IPv4 as big as a golf ball, IPv6 as big as a sun. In 1994, Internet Engineering Task Force (IETF) promoted IPv6 in RFC 1752 (IETF 1995, cited 21.4.2015). IPv6 overcomes some problems such as address shortage, quality of services, auto-configuration, authentication and security. (Microsoft TechNet 2004, cited 30.4.2015.)

With the huge IPv6 address space, NAT and dynamic address allocation will not need to be used. At that time, each device will have a global IP address. This is not only for Internet but also for all computer networks, telecommunication system, control system and smart houses. In future, each air conditioner, refrigerator, washing-machine and rice cooker can have IPv6 address and the owners can connect and give them commands from far distance. At present, the requirement only need 15% address space of IPv6, and 85% for the future.

In IPv6, because having a lot of bits are zero, there are some rules to reduce in writing. For example: with IPv6 address 1099:0000:0000:0000:0009:0900:200C:463A, 0 can be written instead of 0000, 9 instead of 0009, 900 instead on 0900. Consequently, the address in short is 1099:0:0:0:9:900:200C:463A. Another rule can be used is grouping zero numbers by double colons "::", so the IPv6 address in example above can be much shorter: 1099::9:900:200C:463A.

The IPv4-compatible address, 0:0:0:0:0:w.x.y.z (where w.x.y.z is the dotted decimal representation of a public IPv4 address), is used by IPv6/IPv4 nodes that are communicating with IPv6 over IPv4 infrastructure which uses public IPv4 addresses, such as the Internet (Computer Networking Notes 2015, cited 19.3.2015). Figure 2 shows the IPv6-compatible embedded IPv6 address representation.

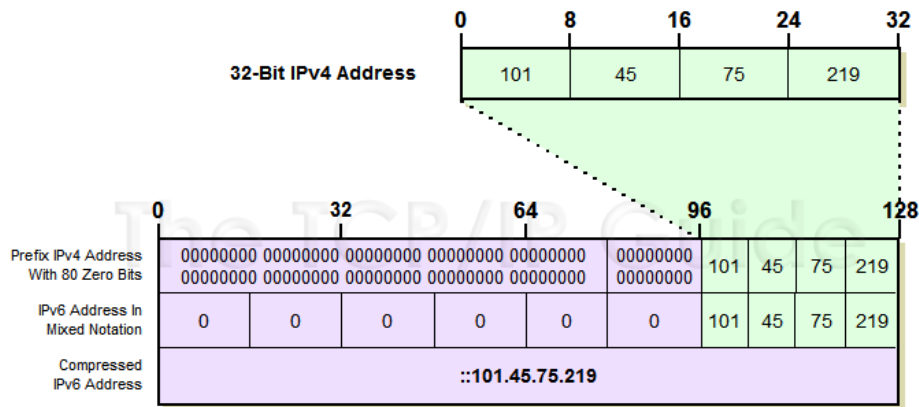


FIGURE 2. IPv4-compatible embedded IPv6 address representation (Kozierok 2005a, cited 18.3.2015)

According to Computer Networking Notes, IPv4-mapped address is used to represent an IPv4 address as a 128-bit IPv6 address (Computer Networking Notes 2015, cited 19.3.2015). They have a set of 16 ones after the initial string of 80 zeroes, and then the IPv4 address. Figure 3 shows the example of IPv4-mapped address.

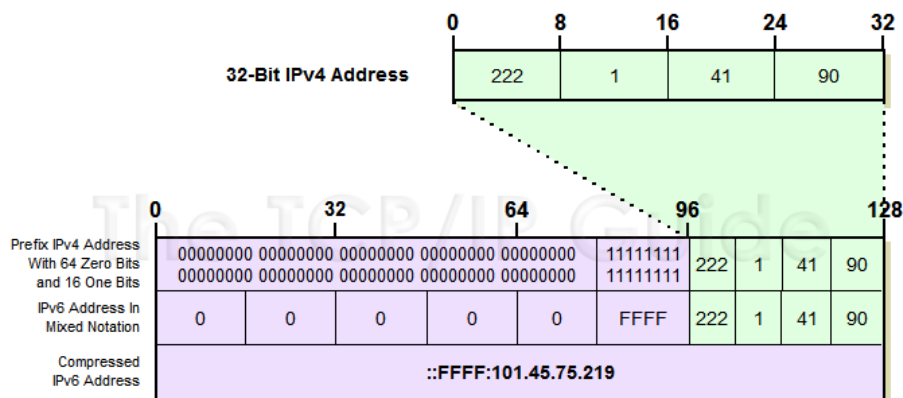


FIGURE 3. IPv4-mapped embedded IPv6 address representation (Kozierok 2005a, cited 18.3.2015)

Unspecified address 0:0:0:0:0:0:0:0 is used by IPv6 node to show that it does not have IP address. It is used to be source address of a packet when an IPv6 node wants to check if any node in same network are using an address it has plan to use. Unspecified address will never be assigned to an interface or becomes destination address. Loopback address 0:0:0:0:0:0:0:1 is used to identify

loopback interface and is used to check if a node can be worked with IPv6 or not. This address will never be sent on a link or forwarded by IPv6 router. The scope of this address is within a node.

### 2.2.1 Types and categories of IPv6 addresses

IPv6 addresses are divided in three main types: unicast address, multicast address and anycast address. Unicast Address is used to identify an interface. If a packet is sent to unicast address, it is only sent to a unique interface. There are three different unicast addresses: unicast global address, unicast link-local address and unicast site-local address. Unicast global addresses, also known as *aggregatable global unicast addresses*, are assigned by ISP to the sites which need to connect to Internet. They are similar with IPv4 public addresses. (Microsoft TechNet. 2003, cited 16.3.2015.) The figure 4 is the three-level structure topology of IPv6 global address. They are public topology (48 bits), site topology (16 bits) and interface of a mode on a specific subnet (64 bits). Table 2 shows the description of each field in unicast global address.

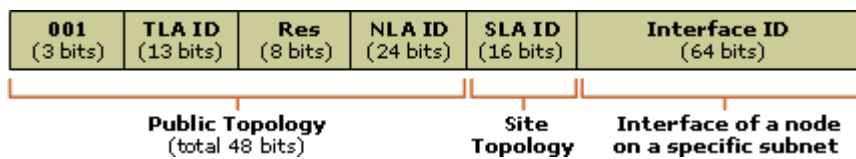


FIGURE 4. IPv6 unicast global address (Microsoft TechNet. 2003, cited 16.3.2015)

TABLE 2. Fields in a unicast global address (Microsoft TechNet. 2003, cited 16.3.2015)

Field	Description
001	Identifies the address as an IPv6 unicast global address.
Top Level Aggregation Identifier (TLA ID)	Identifies the highest level in the routing hierarchy. TLA IDs are administered by IANA, which allocates them to local Internet registries, which then allocate a given TLA ID to a global ISP.
Res	Reserved for future use (to expand either the TLA ID or the NLA ID).
Next Level Aggregation Identifier (NLA ID)	Identifies a specific customer site.
Site Level Aggregation Identifier (SLA ID)	Enables as many as 65,536 (2 <sup>16</sup> ) subnets within an individual organization's site. The SLA ID is assigned within the site; an ISP cannot change this part of the address.
Interface ID	Identifies the interface of a node on a specific subnet.

Unicast link-local addresses (the prefix is FE80::/64) are used by hosts when they want to communicate with other hosts in same local network. They are similar with IPv4 APIPA addresses, used by computers running Microsoft Windows (Microsoft TechNet. 2003, cited 16.3.2015). All IPv6 interfaces have link-local addresses and automatically configure these addresses to communicate with each other. The structure of link-local address is showed in figure 5.

<b>1111 1110 10</b> (10 bits)	<b>000 . . . 000</b> (54 bits)	<b>Interface ID</b> (64 bits)
----------------------------------	-----------------------------------	----------------------------------

FIGURE 5. IPv6 unicast link-local address (Microsoft TechNet. 2003, cited 16.3.2015)

From the figure 5, it can be concluded that: first 10 bits are fixed values: 1111 1110 10; next 54 bits are 0 and last 64 bits are Interface address. A link-local addresses always has prefix is FE80::/64. Because unicast link-local address only be used in the same link, so router cannot transfer any packet with source or destination address is link-local address.

Unicast site-local addresses are not used in Internet. Normally they are used in an organization or a company. They are similar with IPv4 Private Address (10.X.X.X, 172.16.X.X, 192.168.X.X). First 10 bits are fixed: 1111 1110 11; next 38 bits are 0, next 16 bits are subnet ID and last 64 bits are interface ID. A site-local address always has the prefix FEC0::/48. The structure of link-local address is showed in figure 6.

<b>1111 1110 11</b> (10 bits)	<b>000 . . . 000</b> (38 bits)	<b>Subnet ID</b> (16 bits)	<b>Interface ID</b> (64 bits)
----------------------------------	-----------------------------------	-------------------------------	----------------------------------

FIGURE 6. IPv6 Unicast Site-local Address (Microsoft TechNet. 2003, cited 16.3.2015)

Multicast Address is similar with multicast address in IPv4 and is used to identify a group of interfaces. If a packet is sent to multicast address, it will be sent to all interfaces which belong to that multicast address. In IPv6, broadcast address is removed. It is replaced and undertaken by multicast address. According to figure 7, at the first octet, IPv6 multicast address has prefix is FF::/8. IPv6 addresses from FF00:: to FF0F:: are used for multicast purpose, defined by IANA.

<b>1111 1111</b> (8 bits)	<b>Flags</b> (4 bits)	<b>Scope</b> (4 bits)	<b>Group ID</b> (112 bits)
------------------------------	--------------------------	--------------------------	-------------------------------

FIGURE 7. IPv6 Multicast Address (Microsoft TechNet. 2003, cited 16.3.2015)

According to Microsoft TechNet, there are two states of flag field. If this field is set to zero, the address is a permanently assigned multicast address. In contrast, if set to 1, it identifies a transient address. The scope field is used to identify the purpose of the multicast traffic, such as interface-local, link-local, site-local, organization-local, or global scope. The purpose of Group ID field is identifying the multicast group (Microsoft TechNet. 2003, cited 16.3.2015.)

Anycast Address is similar with IPv4 anycast address but more efficient. It is used to identify multiple interfaces and be used primarily by large ISPs. Microsoft TechNet said “IPv6 delivers packets addressed to an anycast address to the nearest interface that the address identifies. In contrast to a multicast address, where delivery is from one to many, an anycast address delivery is from one to one-of-many. Currently, anycast addresses are assigned only to routers and are used only as destination addresses” (Microsoft TechNet. 2003, cited 16.3.2015.)

## 2.2.2 IPv4 and IPv6 comparison

There is a big difference between fixed header of IPv4 and fixed header of IPv6. IPv6 header has 40 octets (or 40 bytes), different with 20 octets in IPv4. However, numbers of field in IPv6 is less than IPv4, so less time needed to spend to process headers, and because of that, it is faster and more flexible. Address field of IPv6 fixed header is 4 times bigger than address field of IPv4 fixed header. Checksum field in IPv4 disappeared in IPv6 Internet because connections nowadays are much faster and more stable, so only hosts need to count checksum, and routers do not need to do that anymore. The purpose of checksum field is to check error in header. However, the value in time to live (TTL) field is changed every time when a packet is transmitted through a router. Consequently, re-calculating checksum field each time when transmitting through a router will make delay time. It can be reduced the delay time if take down this field. There is also no packet segmentation in IPv6. In IPv4, when a packet is too big, router can segment it, however, this can make overhead for packet. In IPv6, only source host can segment a packet following by suitable value depend on Maximum Transmission Unit (MTU) it can find. So, to supporting for source host, IPv6 have a field to help finding MTU from source to destination. Figure 8 shows IPv4 and IPv6 fixed headers.

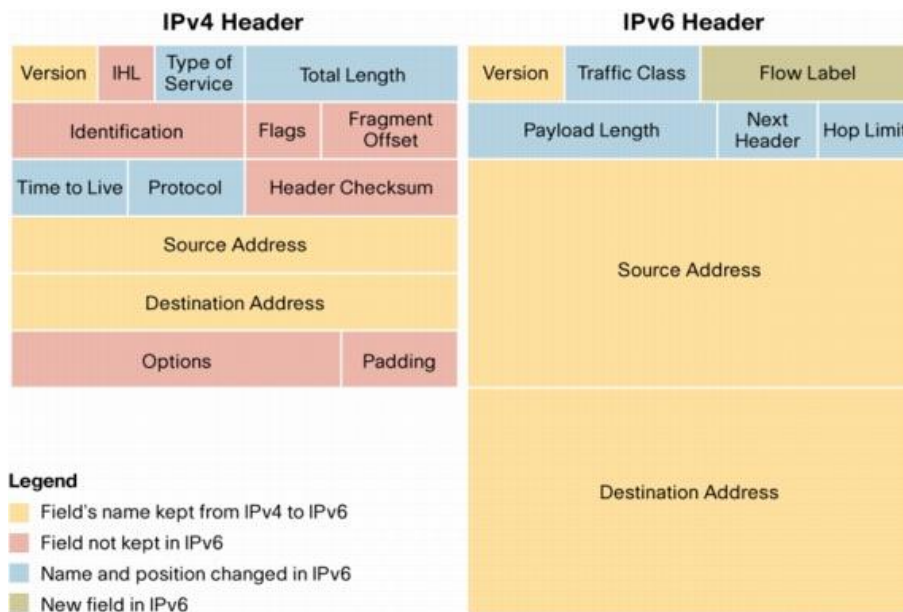


FIGURE 8. IPv4 and IPv6 fixed headers (Paper. W. 2006, cited 19.3.2015)

In addition to fixed header, IPv6 has extension headers. These headers stand between fixed header and upper-layer protocol header, and they carry the information of optional Internet layer and are classified by their functions. This way can reduce the workload for routers and add functions flexibly. Figure 9 shows the chaining extension headers in IPv6 packets.

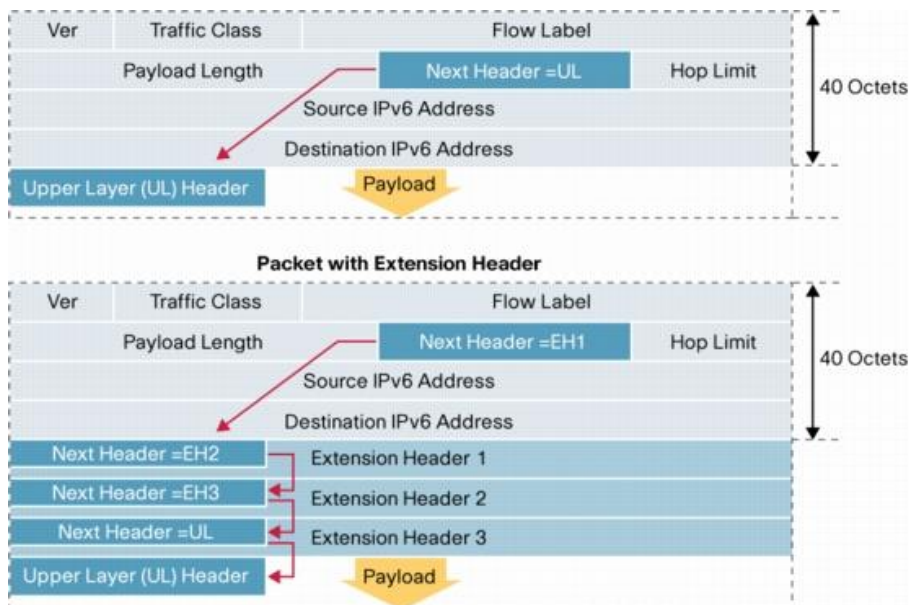


FIGURE 9. Chaining extension headers in IPv6 packets (Paper. W. 2006, cited 19.3.2015)



There are many types of extension headers, and following by RFC 2460, they should be chained in IPv6 packet by this order: IPv6 main header, hop-by-hop options header (if present), destination options header, routing header, fragment header, authentication header, encapsulating security payload header, destination options header, upper-layer header. According to Paper. W, common used of extension headers (EHs) are showed in table 3.

TABLE 3. IPv6 Extension Headers (Paper. W. 2006, cited 19.3.2015.)

Extension headers	Purposes
Hop-by-Hop EH	Is used for the support of Jumbo-grams or, with the Router Alert option, it is an integral part in the operation of Multicast Listener Discovery (MLD). Router Alert [3] is an integral part in the operations of IPv6 Multicast through MLD and RSVP for IPv6.
Destination EH	Is used in IPv6 Mobility as well as support of certain applications.
Routing EH	Is used in IPv6 Mobility and in Source Routing. It may be necessary to disable "IPv6 source routing" on routers to protect against DDoS.
Fragmentation EH	Is critical in support of communication using fragmented packets (in IPv6, the traffic source must do fragmentation-routers do not perform fragmentation of the packets they forward)
Mobility EH	Is used in support of Mobile IPv6 service
Authentication EH	Is similar in format and use to the IPv4 authentication header defined in RFC2402
Encapsulating Security Payload EH	Is similar in format and use to the IPv4 ESP header defined in RFC2406 [5]. All information following the Encapsulating Security Header (ESH) is encrypted and for that reason, it is inaccessible to intermediary network devices. The ESH can be followed by an additional Destination Options EH and the upper layer datagram

IPv6 uses 64 bits for Host-ID. A technique called EUI-64 is used to simply assign an address for a host comparing to IPv4. There are seven main advantages of IPv6 comparing with IPv4. They are: auto-configuration, high performance, mobility support, high security, simple header, route aggregation and renumbering IPv6 devices.

Auto-configuration is used to simplify setting up host devices. IPv6 supports both stateful and stateless auto-configuration. Stateful auto-configuration requires manual configuration from administrators for IPv6 range on DHCPv6. With stateful auto-configuration, DHCPv6 takes charge of assign and administrate IP address for nodes over a network. DHCPv6 server will have a list of nodes and information about their state to know the availability of each IP address. In contrast to stateful auto-configuration, the hosts in network which uses stateless auto-configuration will connect with router and get the Network-ID. Even if there is no router, hosts in same network can determine their address from contents of received user advertisements. Stateless auto-configuration is normally suitable for individuals, small companies and organizations. (Das 2008a, cited 20.3.2015.)

The transmission is in higher performance because IPv6 has enough IP addresses, so no need for private addresses, NAT or some other techniques. From that point of view, it can reduce the time to process packet's header, reduce overhead because of address transformation. Using IPv6 can also reduce the routing time. Because many IPv4 ranges are allocated for users but cannot be summarized, it will increase amount of entries in routing table and overhead when routing. Different from that, IPv6 addresses are allocated through ISP, so reduce overhead and entry in routing table. IPv4 uses a lot of broadcast such as ARP request, when IPv6 uses Neighbor Discovery Protocol (NDP) to do auto-configuration function without using broadcast. Moreover, multicast limitation scope addresses such as global, organization-local, site-local, link-local or node-local are used to limit the multicast packets.

Mobility is really important protocol in network system nowadays. Mobile IP (MIP) is an IETF standard communications protocol for both IPv4 and IPv6. With MIP, mobile device users can move from one network to another with the same IP address, stay connected and maintain ongoing applications. If MIP need to be add if want to use on IPv4, it is already integrated in IPv6. In addition, header what are used in IPv6 routing make mobile IPv6 works more effectively than mobile IPv4. In future, mobile devices such as laptop, tablet, and smartphone will use same IPv6 address for each device on any telecommunication system.

IP Security (IPsec) is an IETF standard protocol using for IP network security on both IPv4 and IPv6. Although basically, the functions of IPsec are the same on IPv4 and IPv6 environments, in IPv6, IPsec is compulsory and ready to be used. It makes IPv6 network safer.

Header of IPv6 is simpler and reasonable than IPv4. IPv6 only has 6 fields if comparing with 10 fields in IPv4. So IPv6 packets will transfer faster, from that, increase network speed.

Route aggregation is a technique which is the same with route summarize in IPv4. ISP will summarize IP addresses with the same prefix and send that prefix to other routers for advertising purposes. By this way, routers can make routing tables smaller and increase routing scalability, leads to the network functions expansion such as optimizing bandwidth and increasing throughput used to connect more devices and service on Internet such as VoIP, TV on demand, high resolution video, real-time applications, game online, study or meeting online.

Renumbering IPv4 devices is a stressful issue for IT administrator. It affects network operation and consumes much manpower to re-configure IPv4 address for all devices in network. IPv6 is designed to renumber address easier. An IPv6 address which was assigned to nodes in two states: preferred and deprecated, depend on lifetime of that address. Lifetime can be configured manually on interface when configuring IP address or add to values used for auto-configuration on routers. Because of that, all nodes on IPv6 network can be renumbered by changing lifetime for a prefix on routers which provide this value. After that, routers can notice a new prefix and all nodes can renumber IP Address. In fact, node can maintain using old address for a period of time before deleting it totally.

### **3 DEPLOY IPV6 OVER IPV4**

Implementation, conversion and replacement a protocol on the Internet is not easy. On Internet, IPv6 address cannot immediately replace IPv4 in a short time. It is a long process. IPv6 address generation was developed when IPv4 address system was completed and is now operating worldwide. During the development period, IPv6 needs to be implemented on IPv4 network infrastructure. IPv4 and IPv6 will co-exist for a long time, an unlimited period of time.

Chapter 3 will present the status of current IPv6 deployment, technologies to deploy IPv6 and convert between IPv4 and IPv6. This chapter will also introduce the routing protocols which operate on IPv6 such as static routing protocol, RIPng, EIGRP for IPv6, OSPFv3.

#### **3.1 IPv6 deployment status**

In Asian countries, the limitation of IPv4 address space has put a certain obstacle to the development of the Internet in important economic regions, such as China, Taiwan, Japan, and Korea. These countries define that IPv6 technology is next network generation and very potential. Developing IPv6 and ranking to the forefront of the next network generation technology are clear direction of Asian governments. China aims to build the world's largest IPv6 network. (Das 2008b, cited 20.3.2015.)

In Europe, applying IPv6 did not have the orientation from governments, but IPv6 still strongly grows by many large projects, develops IPv6 networks to connect many European countries, and also connects Europe with other continents. Internet was begun in the US, and this country holds almost IPv4 address space, therefore, the requirement for IPv6 is not an urgent issue. However, due to the primacies of IPv6 security, in 2008, US Department of Defense has decided to deploy IPv6 for whole defense network system. (Das 2008b, cited 20.3.2015.)

In Vietnam, National Promoting IPv6 Department was established on 01.06.2009. After nearly 4 years of researching and constructing, based on the discussions, opinions and comments of experts, relevant ministries and the experience of deploying IPv6 from other countries, National Promoting IPv6 Department has completed and submitted the national action plan about IPv6 converting to Vietnam Ministry of Information and Communication.

With goal-oriented and specific road, the plan is the base for all IT businesses to make IPv6 transformation plan and apply it depending on actual situation of their own network. At the same time, the training providers in IT industry also have specific plans to integrate the IPv6 content in curriculum. With the promulgation of the national action plan, the minister also asked the ISP to quickly build and deploy their specific IPv6 action plan, consistent with overall national action plan. National Promoting IPv6 Department need to prepare IPv6 trained manpower to ensure for transition in Vietnam. IPv6 migration path in Vietnam is divided into three phases: Phase 1-preparation phase lasted from 2011 to 2012. Phase 2-inception phase launched from 2013 to 2015. Phase 3-transition phase will launch from 2016 to 2019. The general objective is to ensure that before 2020, entire network and internet services of Vietnam will be converted to operate safely and truthfully based on IPv6. (VNNIC 2015, cited 21.3.2015.)

### **3.2 IPv6 address deployment methods**

It is very important to understand how to assign an address in IPv6. There are many methods to address IPv6 such as EUI-64 in IPv6, stateless address auto-configuration, DHCPv6. Furthermore, mobile IPv6 and IPv6 routing table are also necessary to understand.

#### **3.2.1 EUI-64 in IPv6**

One advantage of IPv6 compared with IPv4 is address capability. Host can automatically configure a unique 64-bits IPv6 interface identifier (a unique IPv6 interface ID) without the need of manual configuration or DHCP by using IEEE's 64-bit Extended Unique Identifier (EUI-64) format. To assign itself a unique 64-bit IPv6 interface ID, host will convert its 48-bit MAC address to IPv6 modified EUI-64 form to create an IPv6 interface ID by two steps as below. (Stretch 2008, cited 21.3.2015.)

The first step is breaking down 48-bit MAC address into two 24-bit halves: first 24-bit Organizationally Unique Identifier (OUI) portion and NIC specific portion. Between two halves, adding 16-bit hexadecimal value FFFE (11111111 11111110 in binary) to form a 64-bits address. The address now is in EUI-64 form. (Stretch 2008, cited 21.3.2015.) The example is showed in figure 10.

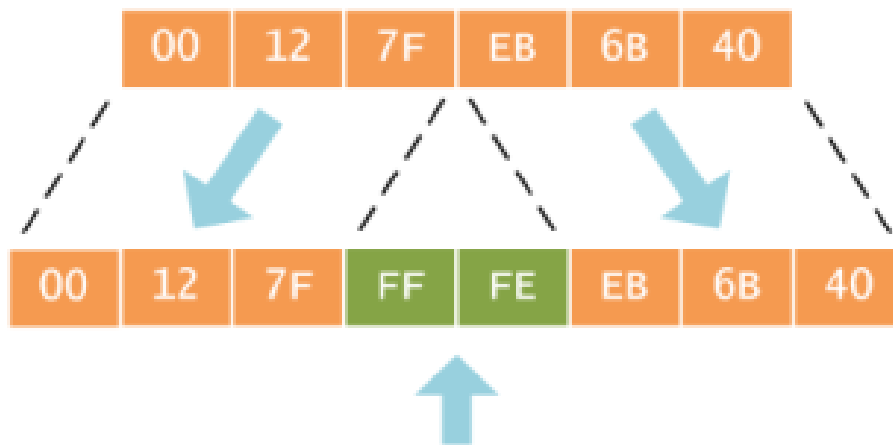


FIGURE 10. Adding 16-bit hex value between two halves of 48-bit MAC address (Stretch 2008, cited 21.3.2015)

In second step, changing the “universal/local” bit (bit 7) in OUI portion of address. Bit 7 in OUI portion will be set to zero if this is the globally unique address which is assigned by IEEE organization. Against with globally unique address, if creating address locally, such as is used for virtual interface or administrators manually configure, this bit will be set to one. In this case, changing the “universal/local” bit from zero to one, so it will be formed to modified EUI-64 interface ID. (Stretch 2008, cited 21.3.2015.) Figure 11 shows the example of second step.

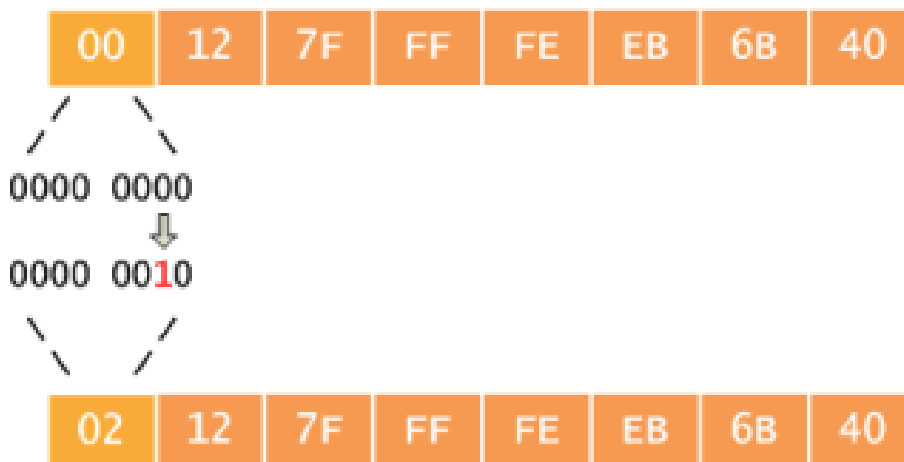


FIGURE 11. Changing the “universal/local” bit (bit 7) / OUI portion of address (Stretch 2008, cited 21.3.2015)

### 3.2.2 Stateless address auto-configuration

There are many advantages of stateless auto-configuration such as no need for DHCP server, allow “hot plugged” of network devices, cost effective, suitable for wireless network, suitable for requiring secure connect applications without additional intermediaries in the form of proxy or DHCP server.

IPv6 is designed as “plug and play” style by using stateless address auto-configuration. It means in a local network, the hosts using stateless auto-configuration will connect to router and get the Network-ID portion of the address. Even if there is no router, hosts in same network can determine their address from contents of received user advertisements. Stateless auto-configuration is normally suitable for individuals, small companies and organizations.

In a local network without router, a host can automatically configure itself IPv6 address and check if that is unique IPv6 address in the scope where it will be used. The IPv6 address is divided in two parts: first left 64-bit subnet prefix (Network-ID portion) and next 64-bit is the host interface ID, and it is just the Modified EUI-64 which is created from MAC address. According to Kozierok, there are six steps of stateless auto-configuration process: link-local address generation, link-local address uniqueness test, link-local address assignment, router contact, router direction and global address configuration.

Link-local address generation is used to form the link-local address from MAC address of host and link-local prefix FE80::/10, is first put as a prefix in the leftmost bits. This prefix FE80::/10 will be 10 bits “1111 1110 10”. The last 64 bits will be the Modified EUI-64 which is created from MAC address. Between link-local prefix and 64 bit interface ID, add 54 zeroes and have 128 bits IPv6 address. After link-local address generation, link-local address uniqueness test will be run on networked device to ensure that the link-local address it generated is unique in local network by using an algorithm called Duplicate Address Detection (DAD). To do this test, the node will send a *neighbor solicitation* message using the *neighbor discovery* (ND) protocol and then listen a Neighbor Advertisement in response to know if that address is using by other node or free to use. If that address is being used by another device, the networked device which is having plan to use it will stop auto configure process and other methods such as manual configuration can be used. However, this case can happen rarely because MAC addresses are designed to be unique in each

network card, so the reason is only because the network is poorly set up or has an error in conversion of address.

Link-local address assignment will be the third step. If the test is passed, that device will use the link-local address it generated. This address will be used in local network but not on Internet because link-local address is not routed. After getting the link-local address, router contact is used to get global address by contacting with a local router using neighbor discovery protocol via internet control message protocol version 6 (ICMPv6) router discovery messages. To do this, the host can listen the router advertisement message sent periodically by routers that contains internet layer configuration or send a link-local router solicitation multicast request and wait the response from routers. The fifth step is giving the host directions by router. It can be stateless configuration with information of internet layer configuration, stateful configuration with information of DHCP server's address, or host will need to be manually configured using static methods. Assume that stateless auto-configuration are using in this case, the host will configure itself with globally unique Internet address by combining the network prefix which was provided by router and device's identifier. (Kozierok 2005b, cited 21.3.2015.)

### **3.2.3 DHCPv6**

Before having DHCP, there was a protocol named BOOTP, using to list MAC addresses and give each of them an IP address. However, there are many other requirements besides only giving a host an IP address, such as time limitation for a host can lease an IP address or information distribution about network services such as DNS and SIP servers. So, DHCP was created to perform these tasks. (Johansson, A., Edvina 2015, cited 21.3.2015.)

DHCP is used in IPv4, and in IPv6, even still keep the name DHCP but it is quite different if compared with DHCP for IPv4. There are three operation modes of DHCPv6: stateful mode, stateless mode and DHCPv6-PD. Stateful mode acts the same function with DHCP on IPv4, it will give a host an IP address and other information. Stateless mode is a combination. Firstly, the host will configure itself an IP address with prefix from router advertisements by using stateless address auto-configuration, and DHCPv6 will give other information such as DNS servers, SIP phones and other services. The last one is DHCPv6-PD. In this mode, network prefix can be provided to home router by a service provider such as ISP. (Johansson, A., Edvina 2015, cited 21.3.2015.)



A host can listen router advertisements which send out frequently by local routers or send out router solicitation and routers will response a router advertisement with flags in its information. There are two flags in router advertisement message are Managed Address Configuration Flag (M flag) and Other Stateful Configuration Flag (O flag). Both flags can be set with value 0 or 1. Table 4 shows four cases with combination of values of M and O flags.

*TABLE 4. Router advertisement message's flag's status (Paper, W 2011, cited 21.3.2015)*

Flag status	Description
M flag is 0 and O flag is 0	Network without DHCPv6 infrastructure. A host can setup a non-link-local address and other setting by using router advertisements or other methods such as manual configuration
M flag is 0 and O flag is 1	Host will obtain an IP address by Stateless Auto-Configuration from the information in router advertisements and DHCPv6 will give other configuration settings. This can be known as Stateless mode of DHCPv6.
M flag is 1 and O flag is 0	DHCPv6 will give a host the information for address configuration but not for other settings. Because other settings such as DNS servers are necessary in IPv6 hosts, so this is unlikely way
M flag is 1 and O flag is 1	DHCPv6 will be used to setup both address and other configuration settings. This can be known as Stateful mode of DHCPv6

To get configuration information from DHCPv6 server, a host can listen a DHCP advertisement or send a DHCP solicit message. If DHCPv6 server is not in the same subnet work that host, a DHCP relay agent which is connected in same segment with that host will forward that request to DHCPv6 server and reply message between DHCPv6 and host. This DHCP relay agent is transparent with hosts. (Paper, W 2011, cited 21.3.2015.)

To send and receive DHCPv6 messages, hosts will use link-local address. DHCPv6 server will use the reserved link-local address "ff02::1:2 (All DHCPv6 relay agents and servers)" or site-local "ff05::1:3 (All DHCPv6 servers)" multicast addresses. Because using reserved link-local "ff02::1:2" multicast address for transmitting, host does not need to be configured with address of DHCPv6 servers. When knowing the DHCPv6 server, host can start using unicast instead of multicast to

send messages. The exchange between IPv6 host and DHCPv6 server can be finished by either 2 or 4 message exchange. (Paper, W 2011, cited 21.3.2015.)

To request one or more IPv6 addresses in four message exchange, firstly, host need to locate the DHCP server by sending Solicit message to reserved link-local “ff02::1:2” multicast address to find available DHCP servers. DHCPv6 servers which meet the host’s requirements will respond with an advertise message. After that, host chooses one DHCPv6 server if have more than one to send request message to request address and configuration information. The chosen DHCPv6 server will response with reply message containing address or addresses and configuration information. At the end, host will send a renew message to DHCPv6 server to extend the lifetimes of its address, allow to continue using that address without interruption. (Paper, W 2011, cited 21.3.2015.) Figure 12 shows HDCPv6-PD request message flows for four message exchange.

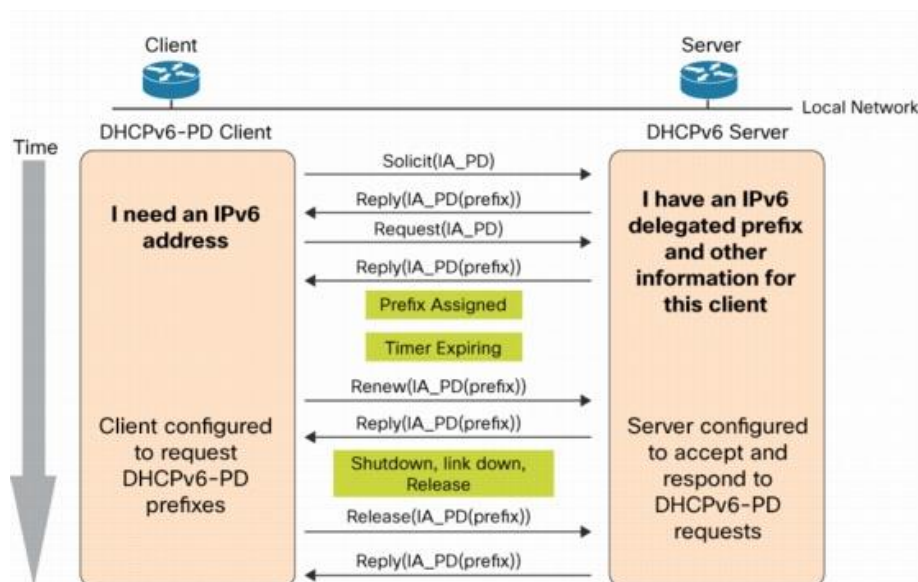


FIGURE 12. HDCPv6-PD request message flows for four message exchange (Paper, W 2011, cited 21.3.2015)

The shorter variation of four message exchange is two message exchange. If a host already has an IPv6 address, either by manually or other way, a simpler way - two message exchange will be used to request configuration information (require rapid-commit is supported). Firstly, host needs to locate the DHCP server by sending solicit message to reserved link-local “ff02::1:2” multicast address to request the assignment of prefix and other configuration information. It includes rapid commit option to indicate that the host will accept an immediate reply message from DHCPv6

server. A DHCPv6 server will immediately response with reply message containing address or addresses and configuration information, which immediately available for host to use. At the end, host will send a renew message to DHCPv6 server to extend the lifetimes of its address, allow to continue using that address without interruption. (Paper, W 2011, cited 21.3.2015.) Figure 13 shows the DHCPv6-PD request message flows for two message exchange.

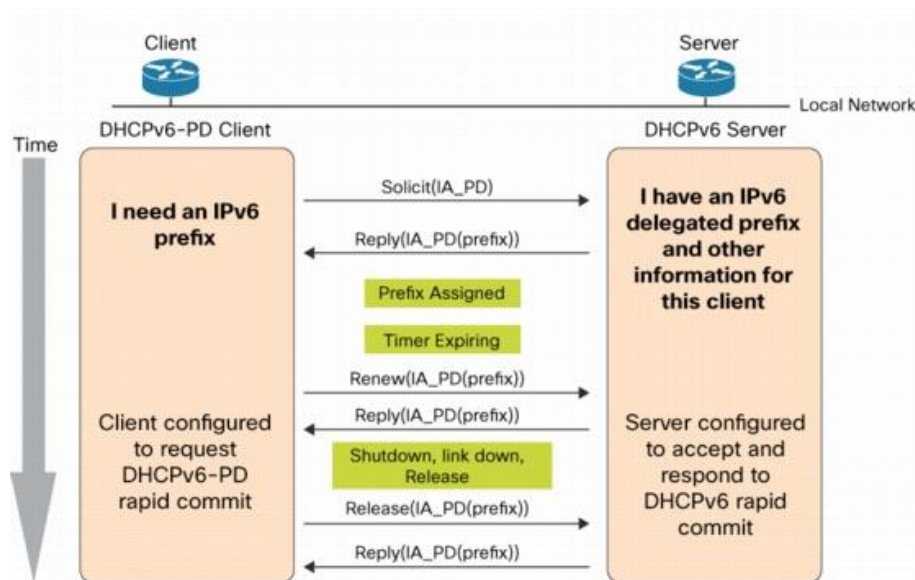


FIGURE 13. DHCPv6-PD request message flows for two message exchange (Paper, W 2011, cited 21.3.2015)

### 3.2.4 Mobile IPv6

Mobile IPv6 is a standard that allows an IPv6 node moves from one network to other networks while still maintaining ongoing connections and its IP address. This is quite useful for many applications such as VPN, VoIP, which need to keep connectivity and IP address continuously. The main reason why mobile IPv6 was designed to support seamless and continuous Internet connectivity because of mobile users. Mobile users frequently move from one place to another with many different wireless systems such as WLAN, WiMAX, BWA, and by using mobile IPv6, mobile devices in IPv6 network can maintain its previously connected link with the same address which was assigned from previously connected link. (Das 2008c, cited 21.3.2015.) Table 5 shows some terms which are necessary to understand in mobile IPv6.

TABLE 5. Mobile IPv6 terms' definition (Kozierok 2005b, cited 21.3.2015)

Term	Definition
Home network	Is the network which mobile device got its home address
Foreign network	Is the network in location which mobile device is operating
Home address	Is the IP address which was assigned by home network and be maintained in foreign network to use in different locations than home network's location
Care-of address	Is the network-native IP address of mobile device when operating in foreign network
Home agent	Is the router on the home network which store the information such as IP address of mobile node, which permanent home address is home agent's network, and have a mission to deliver data what send to that mobile network to the right location it is staying
Foreign agent	Is the router in foreign network with having information of mobile nodes which are visiting in its network and advertising care-of addresses for mobile devices what need. If in foreign network does not have foreign agent, mobile device will have to get an address and advertise that address by itself.
Binding	Is association of address and care-of address

Mobile IPv6 uses some IPv6 features for operation such as stateful/stateless auto-configuration, neighbor discovery and extension header. When a mobile device is in foreign network's location than home network's location and a node want to communicate with this mobile device, it will send data to home address. In the home network, home agent will get that data and transfer that to right location of mobile device by using mobile device's care-of address it had in routing table as source address. (Das 2008c, cited 21.3.2015.)

### 3.2.5 IPv6 routing table

All nodes running IPv6 will have routing table, which is used to determine how to forward packets. Routing table will have information about subnets of networks and next hops to reach those subnets. Routing table entries can be created by adding entries manually, communicating with routers, adding them automatically or when IPv6 initializing. According to Microsoft TechNet, before routing table is used, the destination cache is used to check if there is any entry in destination cache matching with destination address of packet. If the destination cache does not contain an

entry for the destination address, the routing table is used to determine the next-hop address and the next-hop interface. The next-hop address is destination address of packet for a direct delivery (the destination is on local link). For an indirect delivery (destination is not on local link), the next-hop address is the address of router. The next-hop interface can be physical or logical interface which is used to forward packet, either destination or next router. (Microsoft TechNet 2009, cited 21.3.2015.)

After defining the next-hop address and interface, the first packet will be sent and the destination cache will be updated. Next packets which are sent to same destination will use destination cache entry instead of routing table. (Microsoft TechNet 2009, cited 21.3.2015.) There are 4 types of entry in IPv6 routing table, which are showed in table 6.

*TABLE 6. Entry types in IPv6 routing table (Microsoft TechNet 2009, cited 21.3.2015)*

Entry type	Description
Directly connected routes	The routes for networks which are directly connected with current router and have 64 bit prefixes
Remote network routes	The routes for networks which need to reach across other routers and have various prefixes
Host routes	Have 128 bits prefixes and is used to identify specific IPv6 addresses
Default routes	Is used when a specific network cannot found. Default route prefix is ::/0

To determine which route in routing table is used, IPv6 will follow the following steps: First of all, it compares the network prefix bits and chooses the longest prefix length that matches the destination. If there is more than one route with the same longest prefix length, route will choose following by lowest metric to define the best route. If both longest prefix length and lowest metric are satisfactory, the route will be randomly chosen. If a route cannot be found in routing table, packet will be forwarded to default route (network prefix ::/0) if having default routing in routing table or IPv6 will send ICMPv6 destination Unreachable – No Route Found message to sending host and discards packet.

### 3.3 Static routing

IPv6 static routing is not much different from IPv4 static routing, it is configured manually to define a route between two networks. Different with dynamic routing protocols, static routing does not update automatically, instead of that, network administrator will need to re-configure if there is any change related to this static route.

The advantage of static routing is more secure and uses router's resource effectively. Static routing uses less bandwidth and CPU's resource of router to calculate the best route. However, the disadvantage is that it cannot re-configure automatically if it has any change in network topology. Moreover, it also does not have any algorithm to prevent loop in network. Because of that, static routing is normally used in a small network which needs only one route to Internet or to help securing a network if really need to control the traffic transmitting to other networks, or be used for a special purpose.

On Cisco router devices, to configure IPv6 static routing, we go to "configuration mode" and use this command:

```
IPv6 route IPv6-prefix/prefix-length {IPv6-address | interface-type interface-number [IPv6-address]} [administrative-distance] [administrative-multicast-distance | unicast | multicast] [tag tag]
```

There are 4 types of IPv6 static routing which are showed in table 7

TABLE 7. Static routing types (Cisco Systems, Inc. 2015a, cited 22.3.2015)

Static routing types	Description
Directly attached static routes	The destination is assumed to be directly attached with this interface, so only interface is specified. For example: R(config)#IPv6 route 2002:0DB7::/32 serial 0/0 All packets which are sent to address with prefix 2002:DB7::/32 will be forwarded through serial 0/0 interface
Recursive static routes	In this static route, only next-hop is specified. For example: R(config)#IPv6 route 2002:DB7::/32 2002:BD7:3000::1 All packets which are sent to address with prefix 2002:DB7::/32 will be forward through next-hop 2002:BD7:3000::1
Fully specified static routes	With this static routing, both output interface and next-hop address are specified. For example: R(config)#IPv6 route 2002:DB7::/32 serial 0/1 2002:BD7:3000::1
Floating static routes	Is used as a back-up plan for dynamic routing protocols. The Administrative distance (AD) of a floating static route will be higher than the AD of dynamic route protocol it is used to back-up for, so in normally, dynamic route protocols always prefer. In the case, if because of a reason, learning process of dynamic routing protocols is fail, floating static routes will be used. For example: R(config)#IPv6 route 2002:DB7::/32 serial 0/1 2002:BD7:3000::1 210 All three types of static routes above also can be used as floating static routes, only note that AD of that route need to be higher than AD of dynamic routing protocols it is used to back-up for

### 3.4 Dynamic routing protocols

Dynamic routing protocols are used for routing purpose between routers. Routers belonging to a network can be configured in same routing protocol or different routing protocol. For example, network A has three routers R1, R2 and R3. All three routers can be configured with same protocols, such as RIPng, or R1 and R2 can be routed by RIPng protocol while R2 and R3 can be routed by OSPFv3, however, a suggestion is all routers in same network should be configured in same routing protocol. It helps network be more stable and consistent.

Dynamic routing protocols are divided in two forms: distance vector routing protocol and link-state routing protocol. Distance vector routing protocol is run on routers to advertise its connected routes and learn new routes from its neighbors. In distance vector routing protocol, the number of hops is used to calculate the routing cost to reach from source to destination. A router will choose the best path to reach the destination from routing table. Link-state routing protocol is run on routers and identify the state of a link and advertise to its neighbors. Different with distance vector routing protocol, link-state routing protocol only advertises to other routers when it has change in routing table such as new links is learnt from peer routers. After all the routing information has been converged, the link-state routing protocol uses Dijkstra's shortest path first algorithm to calculate the best path to all available links. (Tutorials Point 2015, cited 22.3.2015.)

#### **3.4.1 RIPng**

RIPng protocol is the next generation of RIPv2, is used in IPv6, and is based on distance vector algorithm, or also known as Bellman-Ford algorithm. According to H3C Technologies, there are some working mechanism of RIPng such as: using port 521 and UDP packets to exchange routing information; using hop count to measure the distance between source and destination. As same as RIP and RIPv2, if the hop count is equal or more than 16, the destination network or host is unreachable. (H3C Technologies 2015, cited 17.3.2015.)

RIPng default update time is 30 seconds. If after 30 seconds, no update information is received from a neighbor, that route will be marked as unreachable, and after another 240 seconds with no updating, it will be deleted from routing table. Split horizon and poison reverse methods are used to prevent routing loops and route redistribution in RIPng. (H3C Technologies Co 2015, cited 17.3.2015.)

#### **3.4.2 EIGRP for IPv6**

EIGRP is an enhanced version of the IGRP developed by Cisco. EIGRP uses the same distance vector algorithm and distance information as IGRP. However, the convergence properties and the operating efficiency of EIGRP have improved substantially over IGRP. (Cisco Systems, Inc. 2015c, cited 22.3.2015.)



According to Cisco Systems, “the convergence technology is based on research conducted at SRI International and employs an algorithm called the diffusing update algorithm (DUAL). This algorithm guarantees loop-free operation at every instant throughout a route computation and allows all devices involved in a topology change to synchronize at the same time. Devices that are not affected by topology changes are not involved in recomputations. The convergence time with DUAL rivals that of any other existing routing protocol.” (Cisco Systems, Inc. 2015c, cited 22.3.2015.)

These following features are provided on EIGRP. First of all, network width is increased, from 15 hops for RIP to 224 hops when EIGRP is enabled. Although EIGRP metric can support for thousands of hops, there is a limitation in transport layer hop counter to expand network. To solve this limitation, the transport control field is only increased if an IPv4 or IPv6 packet reaches 15 devices and EIGRP routing protocol is used to learn about destination. When RIP routing protocol is used, the transport control field operates normally. The second feature is fast convergence. By using the DUAL algorithm, the convergence on EIGRP is as quick as current available routing protocol. The third feature is partial updates. This feature can minimize bandwidth which EIGRP packet uses because EIGRP only sends the necessary updates when state of a destination changes instead of sending the entire contents of the routing table. The next one is neighbor discovery mechanism. This is a simple hello mechanism used to learn about neighboring devices. It is protocol-independent. The last feature are arbitrary route summarization, scaling, which helps EIGRP scales to large networks and route filtering. EIGRP for IPv6 provides route filtering using the distribute-list prefix-list command. Use of the route-map command is not supported for route filtering with a distribute list. (Cisco Systems, Inc. 2015c, cited 22.3.2015.)

### **3.4.3 OSPFv3**

“Open Shortest Path First version 3 (OSPFv3) is an interior routing protocol which is modified to support IPv6. This is a link-state protocol and uses Dijkstra’s shortest path first algorithm to calculate best path to all destinations”. (Tutorials Point 2015, cited 22.3.2015.). OSPFv3 is very similar to OSPFv2, and is developed to support both IPv4 and IPv6 while OSPFv2 only supports IPv4. According to Cisco, there are some significant changes in OSPFv3. In OSPFv2, a routing process is necessary and needs to be configured in “configuration” privilege mode of router. However, on OSPFv3, this is unnecessary and OSPFv3 will be enabled on each interface of router. When using a non-broadcast multi-access (NBMA) interface in OSPFv3, the device must be manually configured with the list of neighbors. Neighboring devices are identified by their device

ID. In IPv6, an interface can be configured with more than one address prefixes, and router can choose to import all those address prefixes into OSPFv3 or no address prefixes will be imported. Unlike OSPF version 2, multiple instances of OSPFv3 can be run on a link. OSPF automatically prefers a loopback interface over any other kind, and it chooses the highest IP address among all loopback interfaces. If no loopback interfaces are present, the highest IP address in the device is chosen. OSPFv3 could not be configured to use any particular interface. (Cisco Systems, Inc. 2015b, cited 22.3.2015.)

## **4 IPV4 TO IPV6 CONVERSION SIMULATION**

### **4.1 GNS3 introduction**

In this thesis, Graphical Network Simulator 3 (GNS3) software, an open source software program, will be used to simulate network topology for IPv4 to IPv6 conversion. GNS3 software is created and developed by GNS3 Technologies Inc. in USA. This software allows users to create network hardware simulation, such as Cisco routers, switches and hosts. There are some other simulators besides GNS3 such as cisco packet tracer, netsim, but the reason why I choose GNS3, and also what makes GNS3 different from others is that GNS3 uses the actual router operating system. By using the real operating system (IOS) of router, the test can be done with different scenarios and strongly realistic. Furthermore, GNS3 could connect with many other software and devices such as Virtual PC Simulator (VPCS), an external physical network or even two separate GNS3 networks through a real network devices such as a real router.

### **4.2 Installation and configuration on GNS3**

This part will introduce installation, setting up and configuration to simulate routers, switches and hosts in GNS3. There are also some important notes for using GNS3, especially to simulate switches in GNS3.

#### **4.2.1 GNS3 installation**

The GNS3-1.2.3-all-in-one version using in this test is the latest version which was found on GNS3 website (<http://www.gns3.com/>). Figure 14 shows the main screen of GNS3 software.

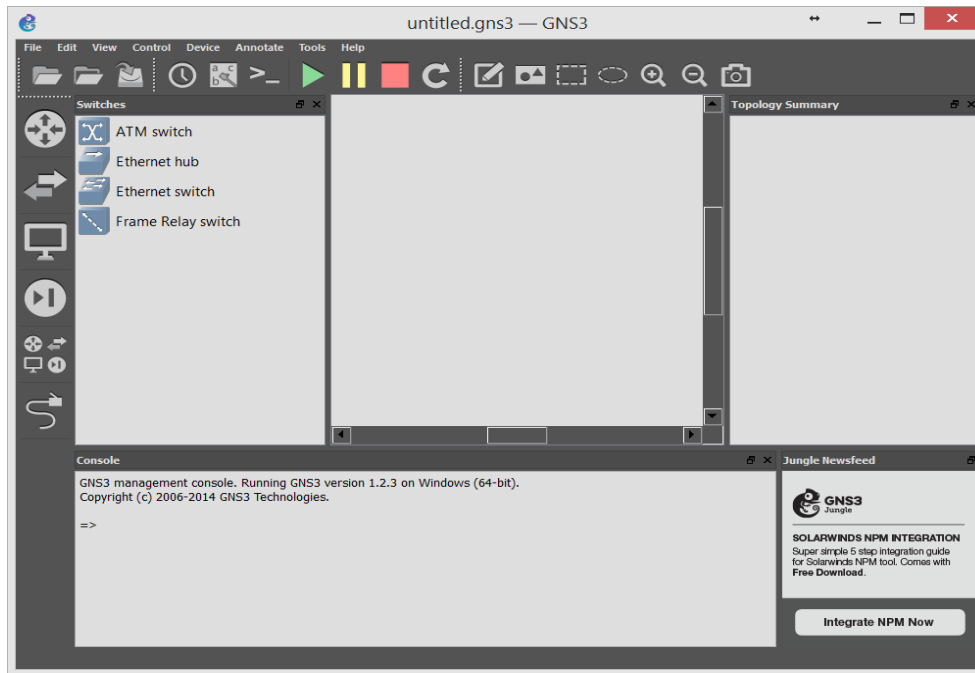


FIGURE 14. Main screen of GNS3 software

#### 4.2.2 Router in GNS3

Router in GNS3 is totally the same with router in real router system because it is using the real Cisco router IOS. There are many Cisco router IOSs can be found and used such as Cisco router 1700, 2600, 2691, 3640, 3725, 3745, 7200. The router IOS which be used in this thesis is Cisco router c3725-adventerprisek9-mz.124-15.T14.bin IOS. This Cisco router IOS can provide different services such as security, VoicelP, and especially support for IPv6 configuration.

#### 4.2.3 Switch in GNS3

Different with router, switches in GNS3 are not good to use in GNS3. They are just basic Ethernet switches with no Command Line Interface (CLI). There is another solution to use the switch in GNS3 is modifying a router to work as switch. To make a router working as switch, add a 16 port module card and turn off IP routing on router by using command “no ip routing”.

There are two issues when modifying a router to use as a switch. First of all, configuring VLANs is different in real system. The “vlan database” command is used to configure VLAN at the privileged EXEC mode, whereas is would normally be done in global configuration mode in real switch with

the “*vlan x*” command. Secondly, because VLAN configuration cannot be saved in start-up configuration file of switch, so it is necessary to load VLAN configuration manually into switch every time when starting GNS3.

#### **4.2.4 Hosts in GNS3**

There are three different ways to set-up a host in GNS3. The easiest way is using the host directly on GNS3. The second way is using VPCS, which was installed in all-in-one version. VPCS can simulate up to 9 PCs, allow to use the commands such as “ping”, “trace”, and it supports for IPv6. The other way to create a host in GNS3 is connecting a virtual machine with a network in GNS3, such as Virtual Box software, a free-of-charge source software. After installing a Virtual Box package, *VirtualBox Host-Only Network adapter* will be installed in Network Connections of Windows. To connect GNS3 topology with this virtual machine, adding a cloud in topology, and then go to *cloud* configuration, in the *NIO Ethernet* tab, selecting *VirtualBox Host-Only Network* and clicking *Add* button. This will give full working operating system if need.

### **4.3 IPv6 migration techniques**

Migrating from IPv4 to IPv6 is a complicated and long-period process. IPv6 is developed when IPv4 is being used widely and stably. Because of that, IPv4 and IPv6 will be used together for a long time, an unlimited period of time. During its development, IPv6 will be deployed based on IPv4 infrastructure. So, it is necessary to understand the techniques to migrate IPv4 to IPv6. There are three main IPv6 migration techniques: dual stack, tunnel technology and NAT-PT. Dual stack allows IPv4 and IPv6 can work together in same network device. Tunnel technology uses IPv4 infrastructure to transfer IPv6 packets between IPv6 networks. NAT-PT is a NAT technology, allow only IPv6 supported devices can communicate with only IPv4 supported devices. This thesis will concentrate on using manual tunnel (static tunnel) technique to migrate from IPv4 to IPv6. (Cisco Systems, Inc. 2006, cited 3.5.2015.)

There are five methods of tunneling IPv6 traffic: manual ipv6 tunnels, automatic IPv4-compatible tunnels, GRE, automatic 6to4 tunnels and intra-site automatic tunnel addressing protocol (ISATAP) tunnels. How to determine tunnel source and destination is the main difference between these tunneling techniques. By using manual tunnel, it will maintain a link between two IPv6 domains over an IPv4 network infrastructure. The main purpose of using manual tunnel is for establishing stable

connections with regular secure communication requirement between two edge routers or between an end system and an edge router, or for connection to remote IPv6 networks. A tunnel interface will be manually configured with an IPv6 address, and tunnel source and destination will be manually configured with IPv4 addresses. Host or router at each end of a configured tunnel must support both IPv4 and IPv6 protocol stacks. (Cisco Systems, Inc. 2011, cited 3.5.2015.)

#### 4.4 Simulation network topology and configuration

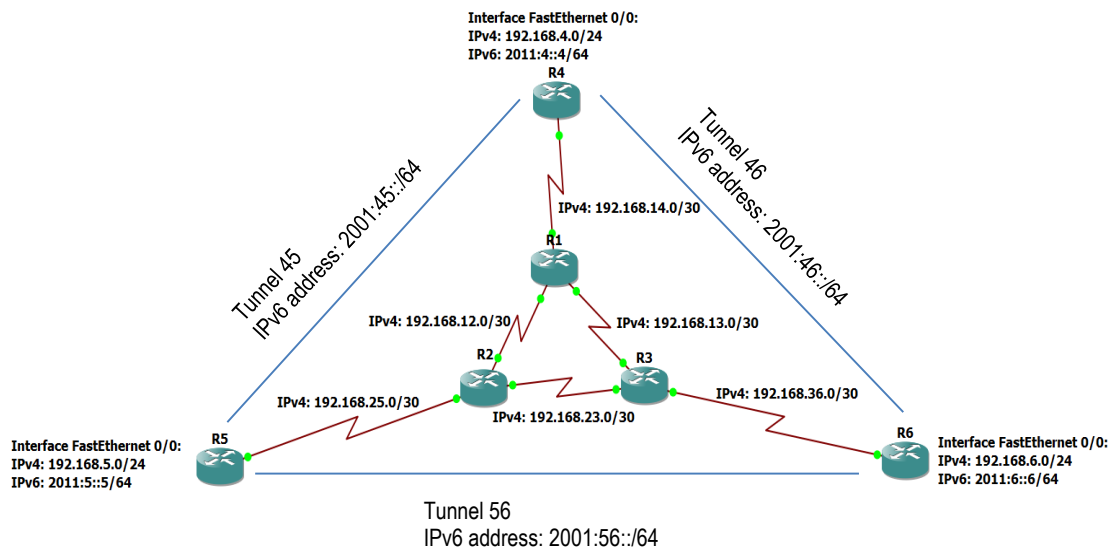
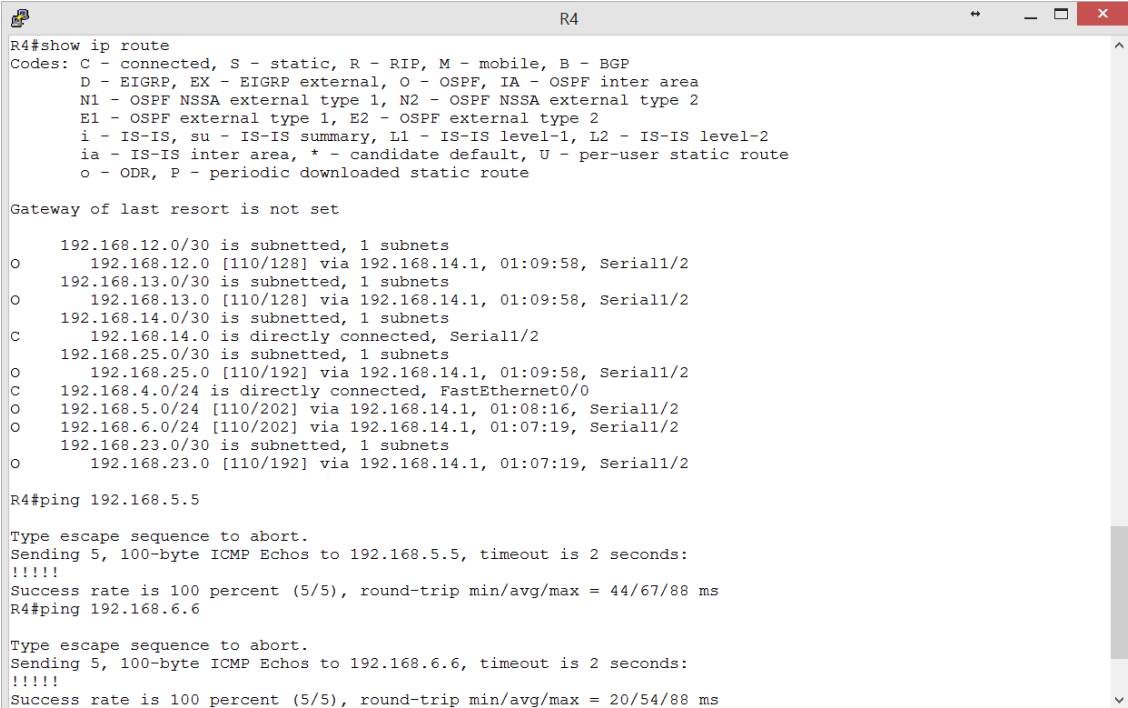


FIGURE 15. Simulation network topology

Figure 15 shows the simulation network topology which simulates a topology of small part of real FPT Company's network. The purpose is to demonstrate the conversion from IPv4 to IPv6. There are three requirements for this lab. The first requirement is setting up this topology with IPv4 network with IPv4 addresses showed in topology and using OSPF for routing between routers, which are showed in appendix 1 and appendix 2. The second requirement is configuring manual tunnel between router R4, R5 and R6 (three routers run IPv6 network), which is shown by configuration in appendix 3. The final requirement is configuring OSPFv3 to make each IPv6 network connect to each other through IPv4 network infrastructure in the middle. The configuration of OSPFv3 for IPv6 network is shown in appendix 4. As figure 15 above, router R1, R2 and R3 only run in IPv4 network infrastructure, and router R4, R5 and R6 run both IPv4 and IPv6 network. IPv6 on router R4, R5 and R6 will need to communicate to each other through IPv4 network infrastructure without any problem.

There are two purposes in this lab. First purpose is showing the way how to deploy IPv6 network based on current IPv4 network without making any interruption which can affect current IPv4 network. The second purpose is showing how to use manual tunnel and OSPFv3 technologies to connect each IPv6 together through IPv4 network at the middle. As mentioned before, to convert from IPv4 to IPv6 network is not an easy job, and cannot be done quickly. There are many cases in which IPv6 networks need to connect each other through IPv4 networks, which did not support IPv6 yet. Manual tunnel and OSPFv3 technology will be one solution to help IPv6 networks connect each other through IPv4 networks without any problem.

After configuring IPv4 addresses to all routers and running OSPF for routing between routers, testing all IPv4 networks can be connected to each other. The command “*show ip route*” is used to show the routing table on router. Figure 16 shows routing table on R4. Those routes having the letter C are directly connected with another network. The letter O refers to networks from other routers and are studied by OSPF routing protocol. From router R4, try to ping to some random networks in other routers which do not connect directly to router R4, all results are successfully. Doing this test on all other routers and everything works well.



```

R4
R4#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

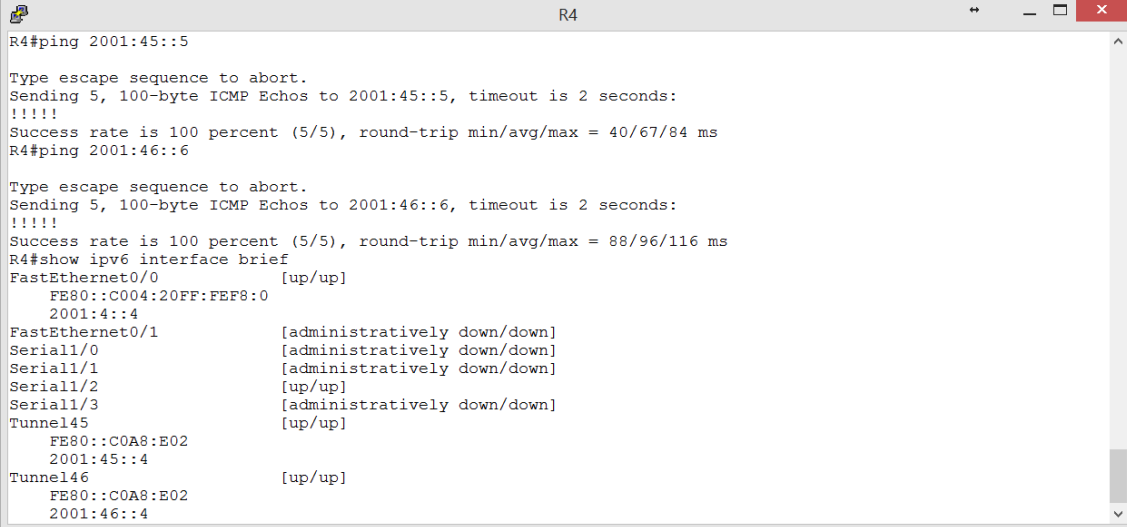
    192.168.12.0/30 is subnetted, 1 subnets
O       192.168.12.0 [110/128] via 192.168.14.1, 01:09:58, Serial1/2
    192.168.13.0/30 is subnetted, 1 subnets
O       192.168.13.0 [110/128] via 192.168.14.1, 01:09:58, Serial1/2
    192.168.14.0/30 is subnetted, 1 subnets
C       192.168.14.0 is directly connected, Serial1/2
    192.168.25.0/30 is subnetted, 1 subnets
O       192.168.25.0 [110/192] via 192.168.14.1, 01:09:58, Serial1/2
C       192.168.4.0/24 is directly connected, FastEthernet0/0
O       192.168.5.0/24 [110/202] via 192.168.14.1, 01:08:16, Serial1/2
O       192.168.6.0/24 [110/202] via 192.168.14.1, 01:07:19, Serial1/2
    192.168.23.0/30 is subnetted, 1 subnets
O       192.168.23.0 [110/192] via 192.168.14.1, 01:07:19, Serial1/2

R4#ping 192.168.5.5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/67/88 ms
R4#ping 192.168.6.6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/54/88 ms

```

FIGURE 16. Routing table on R4

The next configuration is configuring IPv6 addresses and manual tunnel in between router R4, R5 and R6. When checking all tunnels between R4, R5 and R6, they were up after configuring. Figure 17 below show that router R4 already has tunnels to R5, R6 and they connect to each other successfully by using “ping” command to test. Testing on router R5 and R6 are showed in Appendix 5



```

R4#ping 2001:45::5
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:45::5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/67/84 ms
R4#ping 2001:46::6
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:46::6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/96/116 ms
R4#show ipv6 interface brief
FastEthernet0/0      [up/up]
FE80::C004:20FF:FEF8:0
2001:4::4
FastEthernet0/1      [administratively down/down]
Serial1/0             [administratively down/down]
Serial1/1             [administratively down/down]
Serial1/2             [up/up]
Serial1/3             [administratively down/down]
Tunnel145             [up/up]
FE80::C0A8:E02
2001:45::4
Tunnel146             [up/up]
FE80::C0A8:E02
2001:46::4

```

FIGURE 17. Tunnel information on R4

The last configuration is setting up OPFFv3 routing protocol on three routers R4, R5 and R6 to route IPv6 networks. Using command “show ipv6 route” to check all routers which run IPv6 networks had routes to each other’s IPv6 networks and using “ping” command to ping randomly from a router to IPv4 and IPv6 networks of other router to check. All tests were successfully on router R4 as showed in figure 18 bellow. Testing on router R5 and R6 are also successful and are showed in Appendix 6. On the basis of that testing, the conclusion is that deploying IPv6 network by using tunnel technique and OSPF routing protocol did not make any interruption to current IP4 network.



```
R4
R4#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route, M - MIPv6
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       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 - EIGRP, EX - EIGRP external
C 2001:4::/64 [0/0]
  via ::, FastEthernet0/0
L 2001:4::4/128 [0/0]
  via ::, FastEthernet0/0
O 2001:5::/64 [110/11121]
  via FE80::C0A8:1901, Tunnel45
O 2001:6::/64 [110/11121]
  via FE80::C0A8:2402, Tunnel46
C 2001:45::/64 [0/0]
  via ::, Tunnel45
L 2001:45::4/128 [0/0]
  via ::, Tunnel45
C 2001:46::/64 [0/0]
  via ::, Tunnel46
L 2001:46::4/128 [0/0]
  via ::, Tunnel46
O 2001:56::/64 [110/22222]
  via FE80::C0A8:1901, Tunnel45
  via FE80::C0A8:2402, Tunnel46
L FF00::/8 [0/0]
  via ::, Null0
R4#ping 192.168.6.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.6.6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/48/92 ms
R4#ping 2001:56::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:56::6, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 68/112/176 ms
```

FIGURE 18. IPv6 routing table and “ping” command on R4

## 5 CONCLUSIONS AND DISCUSSION

The thesis was aimed to research and deploy IPv6 over IPv4 network infrastructure. The deployment is based on GNS3 simulation software. On balance, the goals of the thesis were reached and all requirements from company where this thesis is made for had been implemented. The work was challenging and interesting.

Doing the research helped me create a big picture about IPv4 and IPv6, and from that point of view, I came to the realization that IPv6 is indeed the next level of addressing on the Internet. There are many advantages compared with IPv4, regarding structure, the way to address, header and new technologies IPv6 supports. It also help me understand about basic technologies to deploy IPv6 on an IPv4 network.

The simulation was made to demonstrate how to configure IPv6 network based on IPv4 network infrastructure without making any interruption on current IPv4 network. Due to limitation of working time, not all of IPv6 deployment technologies were demonstrated. However, the demonstration matched my expectations and I was pleased to be able to deploy IPv6 network based on IPv4 network infrastructure without making any interruption. This will be the foundation for next step of FPT Company when they will deploy IPv6 technology on real company's network system.

Although this thesis was successful, there are still some missing points in this thesis. First of all, knowledge of IPv4, IPv6, routing, and conversion technologies in this thesis were introduced basically. In addition, the demonstration was made in simulation software because I did not have chance to work in real devices.

During the time working with my thesis, I was able to improve my knowledge in both research area and practice area. Furthermore, I also improved my skills such as time management and project management. I would like to close by my appreciation to my supervisors and my opponent who have helped me during this thesis.

## 6 REFERENCES

APNIC. 2015. IPv4 exhaustion details. Cited 30.4.2015, <https://www.apnic.net/community/ipv4-exhaustion/ipv4-exhaustion-details>.

Cisco Systems, Inc. 2004. CCNP1: Advanced IP Addressing Management. Cited 30.4.2015, <http://www.ciscopress.com/articles/article.asp?p=330807&seqNum=10>.

Cisco Systems, Inc. 2006. IP6 tunnel through an IPv4. Cited 3.5.2015, <http://www.cisco.com/c/en/us/support/docs/ip/ip-version-6/25156-ipv6tunnel.html>.

Cisco Systems, Inc. 2011. Implementing tunneling for IPv6. Cited 3.5.2015, [http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12\\_4t/ipv6\\_12\\_4t\\_book/ip6-tunnel.html](http://www.cisco.com/c/en/us/td/docs/ios/ipv6/configuration/guide/12_4t/ipv6_12_4t_book/ip6-tunnel.html).

Cisco Systems, Inc. 2015a. IPv6 Routing. Cited 22.3.2015, [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_pi/configuration/15-s/iri-15-s-book/ip6-route-static.pdf](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_pi/configuration/15-s/iri-15-s-book/ip6-route-static.pdf).

Cisco Systems, Inc. 2015b. IPv6 Routing: OSPFv3. Cited 22.3.2015, [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_ospf/configuration/15-sy/iro-15-sy-book/ip6-route-ospfv3.html).

Cisco Systems, Inc. 2015c. IPv6 Routing: EIGRP Support. Cited 22.3.2015, [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute\\_eigrp/configuration/15-sy/ire-15-sy-book/ip6-route-eigrp.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/iproute_eigrp/configuration/15-sy/ire-15-sy-book/ip6-route-eigrp.html).

Computer Networking Notes. 2015. Special IPv6 Addresses. Cited 19.3.2015, <http://computernetworkingnotes.com/ipv6-features-concepts-and-configurations/special-ipv6-to-devices.html>.

Das, K. 2008a. IPv6-Auto Configuration vs DHCPv6. Cited 20.3.2015, <http://ipv6.com/articles/general/Auto-Configuration-vs-DHCPv6.htm>.

Das, K. 2008b. IPv6 deployment around the world. Cited 20.3.2015, <http://ipv6.com/articles/deployment/IPv6-Deployment-Status.htm>.

Das, K. 2008c. Mobile IPv6. Cited 21.3.2015, <http://ipv6.com/articles/mobile/Mobile-IPv6.htm>

H3C Technologies Co. 2015. IPv6 RIPng Introduction. Cited 17.3.2015, [http://www.h3c.com/portal/Products\\_\\_\\_Solutions/Technology/IP\\_Routing/Technology\\_Introduction/200702/201204\\_57\\_0.htm](http://www.h3c.com/portal/Products___Solutions/Technology/IP_Routing/Technology_Introduction/200702/201204_57_0.htm).

IBM Knowledge Center. 2015. Types and Categories of IPv6 Addresses. Cited 18.3.2015, [http://www-01.ibm.com/support/knowledgecenter/SSB27U\\_5.4.0/com.ibm.zvm.v54.kijl0/hcsk7b3014.htm%23wq23](http://www-01.ibm.com/support/knowledgecenter/SSB27U_5.4.0/com.ibm.zvm.v54.kijl0/hcsk7b3014.htm%23wq23).

IETF. 1981. RFC 791: Internet Protocol Darpa Internet Program Protocol Specification. Cited 21.4.2015, <https://tools.ietf.org/html/rfc791>.

IETF. 1995. RFC 1752: The Recommendation for the IP Next Generation Protocol. Cited 21.4.2015, <https://tools.ietf.org/html/rfc1752>.

IETF. 1996. RFC 1918: Address Allocation for Private Internets. Cited 21.4.2015, <https://tools.ietf.org/html/rfc1918>.

IETF. 1998. RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. Cited 21.4.2015, <https://www.ietf.org/rfc/rfc2460.txt>.

Intense School and InfoSec Institute. 2013. CCNA Prep: Analyzing Classful IPv4 Networks. Cited 13.3.2015, <http://resources.intenseschool.com/ccna-prep-analyzing-classful-ipv4-networks/>.

Johansson, A., Edvina. 2015. DHCPv6-an introduction to the new host configuration protocol. Cited 21.3.2015, <http://ipv6friday.org/blog/2011/12/dhcpv6/>.

Kozierok. C. 2005a. IPv6/IPv4 Address Embedding. Cited 18.3.2015, [http://www.tcpipguide.com/free/t\\_IPv6IPv4AddressEmbedding.htm](http://www.tcpipguide.com/free/t_IPv6IPv4AddressEmbedding.htm).

Kozierok. C. 2005b. IPv6 Autoconfiguration and Renumbering. Cited 21.3.2015, [http://www.tcpipguide.com/free/t\\_IPv6AutoconfigurationandRenumbering.htm](http://www.tcpipguide.com/free/t_IPv6AutoconfigurationandRenumbering.htm).

Kozierok. C. 2005c. Mobile IP Addressing: Home and "Care-Of" Addresses. Cited 21.3.2015, [http://www.tcpipguide.com/free/t\\_MobileIPAddressingHomeandCareOfAddresses-2.htm](http://www.tcpipguide.com/free/t_MobileIPAddressingHomeandCareOfAddresses-2.htm).

Microsoft TechNet. 2003. IPv6 Address Types. Cited 16.3.2015, <https://technet.microsoft.com/en-us/library/cc757359%28v=ws.10%29.aspx>.

Microsoft TechNet. 2004. Chapter 3 - IP Addressing Cited 30.4.2015, <https://technet.microsoft.com/en-us/library/bb726995.aspx>.

Microsoft TechNet. 2009. IPv6 Routing (TechRef). Cited 21.3.2015, <https://technet.microsoft.com/en-us/library/dd379520%28v=ws.10%29.aspx>.

Paper, W. 2006. IPv6 Extension Headers Review and Considerations. Cited 19.3.2015, [http://www.cisco.com/en/US/technologies/tk648/tk872/technologies\\_white\\_paper0900aecd8054d37d.html](http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html).

Paper, W. 2011. DHCPv6 Based IPv6 Access Services. Cited 21.3.2015, [http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper\\_c11-689821.html](http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html).

Paquet, C.& Teare, D. 2003, Building Scalable Cisco Internetworks (BSCI), 1st edition. CA: Cisco Systems.

Sequeira, A. 2013, Interconnecting Cisco Network Devices, Part1 (ICND1) Foundation Learning Guide, 4th Edition, CA: Cisco Press.

Stretch. 2008. EUI-64 in IPv6. Cited 21.3.2015, <http://packetlife.net/blog/2008/aug/4/eui-64-ipv6/>.

Tutorials Point. 2015. IPv6-Routing. Cited 22.3.2015,  
[http://www.tutorialspoint.com/ipv6/ipv6\\_routing.htm](http://www.tutorialspoint.com/ipv6/ipv6_routing.htm).

VNNIC. 2015. Điều chỉnh Kế hoạch hành động quốc gia về IPv6. Cited 21.3.2015,  
<http://www.vnnic.vn/tintuc/%C4%90i%E1%BB%81u-ch%E1%BB%89nh-k%E1%BA%BF-ho%E1%BA%A1ch-h%C3%A0nh-%C4%91%E1%BB%99ng-qu%E1%BB%91c-gia-v%E1%BB%81-ipv6-29-10-2014>.

White, R. 2015. Working with IP Addresses. The Internet Protocol Journal 9 (1). Cited 13.3.2015,  
[http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_9-1/ip\\_addresses.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_9-1/ip_addresses.html).

## 7 APPENDICES

### IPV4 INTERFACE CONFIGURATION ON ROUTER R1, R2, R3, R4, R5, R6

### APPENDIX 1

```
R1(config)#interface s1/0
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.12.1 255.255.255.252
R1(config)#interface s1/1
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.13.1 255.255.255.252
R1(config)#interface s1/2
R1(config-if)#no shutdown
R1(config-if)#ip address 192.168.14.1 255.255.255.252
```

---

```
R2(config)#interface s1/0
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.12.2 255.255.255.252
R2(config)#interface s1/2
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.23.2 255.255.255.252
R2(config)#interface s1/3
R2(config-if)#no shutdown
R2(config-if)#ip address 192.168.25.2 255.255.255.252
```

---

```
R3(config)#interface s1/1
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.13.2 255.255.255.252
R3(config)#interface s1/2
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.36.1 255.255.255.252
R3(config)#interface s1/3
R3(config-if)#no shutdown
R3(config-if)#ip address 192.168.23.1 255.255.255.252
```

---

```
R4(config)#interface s1/2
R4(config-if)#no shutdown
R4(config-if)#ip address 192.168.14.2 255.255.255.252
R4(config)#interface f0/0
R4(config-if)#no shutdown
R4(config-if)#ip address 192.168.4.4 255.255.255.0
```

---

```
R5(config)#interface s1/0
R5(config-if)#no shutdown
R5(config-if)#ip address 192.168.25.1 255.255.255.252
R5(config)#interface f0/0
R5(config-if)#no shutdown
R5(config-if)#ip address 192.168.5.5 255.255.255.0
R6(config)#interface s1/0
R6(config-if)#no shutdown
R6(config-if)#ip address 192.168.36.2 255.255.255.252
R6(config)#interface f0/0
R6(config-if)#no shutdown
R6(config-if)#ip address 192.168.6.6 255.255.255.0
```

```
R1(config)#router ospf 100
R1(config-router)#network 192.168.12.1 0.0.0.3 area 0
R1(config-router)#network 192.168.13.1 0.0.0.3 area 0
R1(config-router)#network 192.168.14.1 0.0.0.3 area 0


---


R2(config)#router ospf 100
R2(config-router)#network 192.168.12.2 0.0.0.3 area 0
R2(config-router)#network 192.168.23.2 0.0.0.3 area 0
R2(config-router)#network 192.168.25.2 0.0.0.3 area 0


---


R3(config)#router ospf 100
R3(config-router)#network 192.168.13.2 0.0.0.3 area 0
R3(config-router)#network 192.168.23.1 0.0.0.3 area 0
R3(config-router)#network 192.168.36.1 0.0.0.3 area 0


---


R4(config)#router ospf 100
R4(config-router)#network 192.168.14.2 0.0.0.3 area 0
R4(config-router)#network 192.168.4.4 0.0.0.255 area 0


---


R5(config)#router ospf 100
R5(config-router)#network 192.168.25.1 0.0.0.3 area 0
R5(config-router)#network 192.168.5.5 0.0.0.255 area 0


---


R6(config)#router ospf 100
R6(config-router)#network 192.168.36.2 0.0.0.3 area 0
R6(config-router)#network 192.168.6.6 0.0.0.255 area 0
```



```
R4(config)#Interface f0/0
R4(config-if)#Ipv6 address 2001:4::4/64
R4(config-if)#exit
R4(config)#interface tunnel 45
R4(config-if)#tunnel source 192.168.14.2
R4(config-if)#tunnel destination 192.168.25.1
R4(config-if)#tunnel mode ipv6ip
R4(config-if)#ipv6 address 2001:45::4/64
R4(config-if)#exit
R4(config)#interface tunnel 46
R4(config-if)#tunnel source 192.168.14.2
R4(config-if)#tunnel destination 192.168.36.2
R4(config-if)#tunnel mode ipv6ip
R4(config-if)#ipv6 address 2001:46::4/64
R4(config-if)#exit
```

---

```
R5(config)#Interface f0/0
R5(config-if)#Ipv6 address 2001:5::5/64
R5(config-if)#exit
R5(config)#interface tunnel 45
R5(config-if)#tunnel source 192.168.25.1
R5(config-if)#tunnel destination 192.168.14.2
R5(config-if)#tunnel mode ipv6ip
R5(config-if)#ipv6 address 2001:45::5/64
R5(config-if)#exit
R5(config)#interface tunnel 56
R5(config-if)#tunnel source 192.168.25.1
R5(config-if)#tunnel destination 192.168.36.2
R5(config-if)#tunnel mode ipv6ip
R5(config-if)#ipv6 address 2001:56::5/64
R5(config-if)#exit
```

---

```
R6(config)#Interface f0/0
R6(config-if)#Ipv6 address 2001:6::6/64
R6(config-if)#exit
R6(config)#interface tunnel 46
R6(config-if)#tunnel source 192.168.36.2
R6(config-if)#tunnel destination 192.168.14.2
R6(config-if)#tunnel mode ipv6ip
R6(config-if)#ipv6 address 2001:46::6/64
R6(config-if)#exit
R6(config)#interface tunnel 56
R6(config-if)#tunnel source 192.168.36.2
R6(config-if)#tunnel destination 192.168.25.1
R6(config-if)#tunnel mode ipv6ip
R6(config-if)#ipv6 address 2001:56::6/64
R6(config-if)#exit
```

```
R4(config)#ipv6 unicast-routing
R4(config)#interface tunnel 45
R4(config-if)#ipv6 ospf 1 area 0
R4(config-if)#exit
R4(config)#interface tunnel 46
R4(config-if)#ipv6 ospf 1 area 0
R4(config-if)#exit
R4(config)#interface f0/0
R4(config-if)#ipv6 ospf 1 area 0
R4(config-if)#exit
```

---

```
R5(config)#ipv6 unicast-routing
R5(config)#interface tunnel 45
R5(config-if)#ipv6 ospf 1 area 0
R5(config-if)#exit
R5(config)#interface tunnel 56
R5(config-if)#ipv6 ospf 1 area 0
R5(config-if)#exit
R5(config)#interface f0/0
R5(config-if)#ipv6 ospf 1 area 0
R5(config-if)#exit
```

---

```
R6(config)#ipv6 unicast-routing
R6(config)#interface tunnel 46
R6(config-if)#ipv6 ospf 1 area 0
R6(config-if)#exit
R6(config)#interface tunnel 56
R6(config-if)#ipv6 ospf 1 area 0
R6(config-if)#exit
R6(config)#interface f0/0
R6(config-if)#ipv6 ospf 1 area 0
R6(config-if)#exit
```

## TUNNEL INFORMATION ON R5, R6

## APPENDIX 5

```

R5
R5#ping 2001:45::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:45::4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/62/80 ms
R5#ping 2001:56::6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:56::6, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 40/73/104 ms
R5#show ipv6 interface brief
FastEthernet0/0          [up/up]
    FE80::C005:2BFF:FE64:0
    2001:5::5
FastEthernet0/1          [administratively down/down]
Serial1/0                [up/up]
Serial1/1                [administratively down/down]
Serial1/2                [administratively down/down]
Serial1/3                [administratively down/down]
Tunnel145                [up/up]
    FE80::C0A8:1901
    2001:45::5
Tunnel156                [up/up]
    FE80::C0A8:1901
    2001:56::5

```

```

R6
R6#ping 2001:45::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:45::4, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/101/152 ms
R6#ping 2001:56::5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:56::5, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/96/112 ms
R6#show ipv6 interface brief
FastEthernet0/0          [up/up]
    FE80::C006:23FF:FE48:0
    2001:6::6
FastEthernet0/1          [administratively down/down]
Serial1/0                [up/up]
Serial1/1                [administratively down/down]
Serial1/2                [administratively down/down]
Serial1/3                [administratively down/down]
Tunnel146                [up/up]
    FE80::C0A8:2402
    2001:46::6
Tunnel156                [up/up]
    FE80::C0A8:2402
    2001:56::6

```

```

R5#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        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 - EIGRP, EX - EIGRP external
O   2001:4::/64 [110/11121]
    via FE80::C0A8:E02, Tunnel145
C   2001:5::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:5::5/128 [0/0]
    via ::, FastEthernet0/0
O   2001:6::/64 [110/11121]
    via FE80::C0A8:2402, Tunnel156
C   2001:45::/64 [0/0]
    via ::, Tunnel145
L   2001:45::5/128 [0/0]
    via ::, Tunnel145
O   2001:46::/64 [110/22222]
    via FE80::C0A8:E02, Tunnel145
    via FE80::C0A8:2402, Tunnel156
C   2001:56::/64 [0/0]
    via ::, Tunnel156
L   2001:56::5/128 [0/0]
    via ::, Tunnel156
L   FF00::/8 [0/0]
    via ::, Null0
R5#ping 192.168.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/62/72 ms
R5#ping 2001:46::4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:46::4, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/106/196 ms

```

```

R6#show ipv6 route
IPv6 Routing Table - 10 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
        U - Per-user Static route, M - MIPv6
        I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
        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 - EIGRP, EX - EIGRP external
O   2001:4::/64 [110/11121]
    via FE80::C0A8:E02, Tunnel146
O   2001:5::/64 [110/11121]
    via FE80::C0A8:1901, Tunnel156
C   2001:6::/64 [0/0]
    via ::, FastEthernet0/0
L   2001:6::6/128 [0/0]
    via ::, FastEthernet0/0
O   2001:45::/64 [110/22222]
    via FE80::C0A8:E02, Tunnel146
    via FE80::C0A8:1901, Tunnel156
C   2001:46::/64 [0/0]
    via ::, Tunnel146
L   2001:46::6/128 [0/0]
    via ::, Tunnel146
C   2001:56::/64 [0/0]
    via ::, Tunnel156
L   2001:56::6/128 [0/0]
    via ::, Tunnel156
L   FF00::/8 [0/0]
    via ::, Null0
R6#ping 192.168.5.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/47/72 ms
R6#ping 2001:45::5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:45::5, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/83/100 ms

```