ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
March 2017,
Vol. 10, No. (1):
Pgs. 33-40

An Insight into IP Addressing

DR. MAMTA PADOLE[1]*, PRATIK KANANI[2], LEENA RAUT[2], DHYANVI JHAVERI[2] and MANALI NAGDA[2]

[1]Department of Computer Science and Engineering, MS University of Baroda, Gujarat, India.
[2]Department of Information Technology, University of Mumbai, Mumbai, India.
*Corresponding author E-mail: Mamta.padole-cse@msu.ac.in

http://dx.doi.org/10.13005/ojcst/10.01.05

(Received: January 19, 2017; Accepted: Febraury 08, 2017)

ABSTRACT

The current version of Internet Protocol (IPv4) has not been substantially changed in the past 25 years. IPv4 has proven to be robust and easily implemented. In the early stage, the deployment of IPv6 is prepared and begun on the IPv4-based network. In the intermediate stage, IPv4 and IPv6 coexist. In the later stage, IPv6 plays a leading role on the network and the IPv4 network is gradually withdrawing from the market. Meanwhile, researchers put forward many transition mechanisms for different network infrastructures and different evolution stages. In this paper, a detailed study is made on IPv4 along with its different smart saving techniques. Which help in delay of IPv4 to IPv6 shifting delays. Also different addressing schemes are discussed which remains unchanged in future. Along with that limitations of IPv4 is also focused so present IPv4 network infrastructure can be more secured till IPv6 realization.

Keywords: Ipv4, IPv6, NAT, Addressing, IP classes, Subnetting, Supernetting, IPv4 limitations.

INTRODUCTION

World wide web, www connects all e-resources together where clients and server can use and give such services. Whenever any service or resource is demanded the client should first able to locate the server carrying the resources. After resource has been found out the particular directory or server disk has to be checked to get the location of the file. Once location is identified then there is a need for different protocols which deliver such resources on the internet in electrical forms while keeping it intact. To get the resource we have different addressing schemes while protocols stand to deliver the content. In this paper Internet Protocol version 4 is studied in order to understand its pros and cons. The different addressing levels such as logical, physical, port and specific addressing is mentioned in their own aspects of need and certainty. Further the relation of such addressing schemes with OSI and TCP/IP models are shown. IPv4 is talked about with its size and different classes, where each class differs by its network and host ID part. IPv4 addresses are already scarce and IPv6 addressing is under deployment progress. Till all the IPv4 devices are improved to IPv6 devices the only option is to use IPv4. In such scenarios how to use IPv4 addressing scheme with more efficiency

is discussed and it covers the different techniques like classful and classless IP addressing.

Subnetting is other way by which one can expand the network while keeping the public network id unchanged. Advance to that the private and public IP addresses are mentioned along with their ranges, so one can make use of them in their private and public networks accordingly. The other possible way to have more users in less range of available IP is DHCP which is focused too, followed by the Network Address Translation technique which makes communication possible for private networks over public domains. At closing different IPv4 loopholes are discussed in order to have present IPv4 network infrastructure more secured and efficient with quality of service.

Levels of Addresses

TCP/IP protocol suit addresses four levels of addressing schemes. Each level represents different addressing techniques and sources [1].

Each addressing level is correlated to a definite layer in the TCP/IP design.

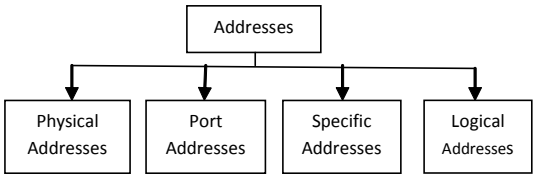

Fig. 1: Classification in Addresses in TCP/IP[1]

Physical Addressing

Physical Address is also known as MAC (Media Access Control) Address. It is a unique identifier, typically associated to an essential circuit card which converts communication data to electrical signals, called as Network Interface Card (NIC) which is critical hardware responsible for the communication to a Data Link Layer. NIC can be wired and wireless based on the need.

It is 2-digit (6 bytes or 48 bits) hexadecimal numbers. By convention, they are ordinarily written in one of the following three formats [3]:

- MM:MM:MM:SS:SS:SS
- MM-MM-MM-SS-SS-SS
- MMM.MMM.SSS.SSS

The leftmost 6 digits that is 24 bits prefix is associated with the adapter manufacturer assigned by IEEE and rightmost 6 digits are identification of each devices.

e.g. 06:01:02:01:2B:4C. In LAN topologies data are in the form of frames are propagated by MAC addresses. Such addresses can be seen at real time by using ipconfig/ifconfig commands on respective windows and linux OS.

Port Addressing

Communication data travels in other forms based on the OSI and TCP/IP layers. They are termed in accordance to a layer. For example at DLL it is called as frame, at NL it is Packet and at PL it is

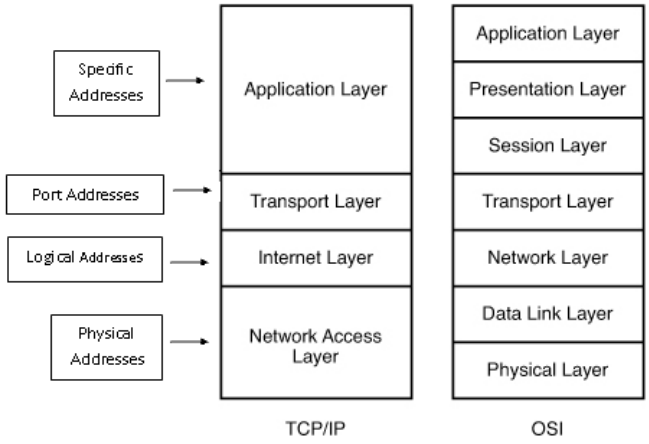

Fig. 2: Relationship in OSI, TCP/IP and Addressing[1,2]

bit. On one host many processes run simultaneously and whenever data arrives at host, host must know to which process the current data belongs to? This issues is solved by port addressing where each port represents a particular process or application on a particular host. For any application while talking to server it should know the server port number while host ports are assigned by host OS.

Port addressing is represented by 16-bit numbers. They range from o-65,535. And they are categorized in three domains based on the range[4].

1) Port 0-1,023 are reserved by systems.
2) Ports 1,024-49,151 are registered ports and
3) Ports 49,152-65,535 are dynamic /private ports.

Specific Addressing

The world wide web represents the e-resources in the form known as Uniform Resource Locator (URL). Each URL represents communication protocol, domain and the path for the resource. It is known as specific addressing. E.g. http://www.msubaroda.ac.in/index.php points to index.php on msu website.

Logical Addressing

This addressing scheme represents a particular entity in the world. Through physical addressing the communication is limited to a number of resources in a smaller range but to communicate across a globe logical addressing is the key. It is 32-bit long address which represents network and host part and hence called as logical addressing. This addressing is commonly referred as Internet Protocols and exists in two flavors called as version 4 and 6 that is IPv4 and IPv6.

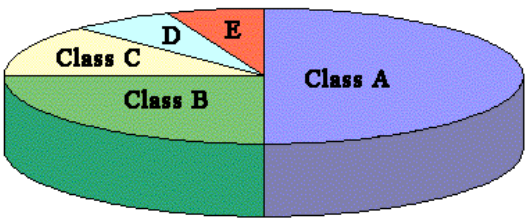

Fig. 3: The allocation of 4,294,967,296 Addresses[6]

Internet Protocol Version 4

The 32 bit long IPv4 address has first field as network id which represents a particular network in the internet and second field is host ID which identifies a particular host on a particular network. The number of possible addresses using IPv4 is 2^{32} 4,294,967,296 (more than 4 billion)[5].

- Class A uses half of them (2,147,483,648 addresses)
- Class B uses one-fourth (1,073,741,824 addresses)
- Class C uses one-eighth (536,870,912)
- Class D and Class E each use 1/16th - they split the rest of the addresses (268,435,456 each)[6]

The 32-bit IP address is divided into four octets, where each octet represents a set of bits stand either for network ID or host ID.

As each filed is an octet in IPv4 so it can have numbers from 0-255. Thery by each octet overall represents the combination of 0-255. Based on the range and octet size IP addresses are classified into different classes as follows.

- Class A : has first octet as network field and remaining three as host fields. It has MSB as zero which represents A class address. It can have total 2^7 networks and 2^{24} hosts. Its network ranges from 0-126.
- Class B : has first two octets as network field and remaining two as host fields. It has MSB as one zero which represents B class address. It can have total 2^{14} networks and 2^{16} hosts. Its network ranges from 128-191.
- Class C : has first three octets as network field and remaining one as host fields. It has MSB as one one zero which represents C class address. It can have total 2^{21} networks and 2^8 hosts. Its network ranges from 192-223.

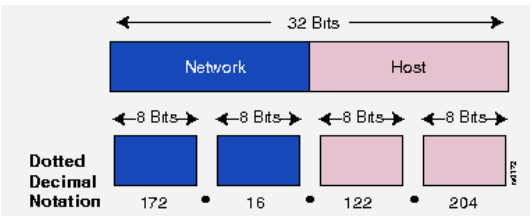

Fig. 4: The basic format of typical IP Address[6]

- Class D : has 1110 as MSB and it ranges from 224-239 that is 224.0.0.0 to 239.255.255.255. Class D is reserved for multicasting of data. It does not have any subnet masks[5].
- Class E : has 11110 as MSB and it ranges from 240-255. It is kept for Research and Development purposes[5].

Classful Network Masks

Network masks are used to separate network and host part at destination so receiver can find the particular host on the network. Defaults masks represent 1 as network field and 0 as host field[6].

Class A has default mask as 255.0.0.0
Class B has default mask as 255.255.0.0
Class C has default mask as 255.255.255.0

IPv4 Efficient Utilization

IP addresses are under the control of Internet Assigned Numbers Authority (IANA) which oversees IP allocation, DNS root zone management and Autonomous Systems numbering and other internet related media types, symbols and numbers[7]. There are certain techniques which help to have greater numbering by using smaller addresses.

Classless Addressing

Classful addressing will have default mask or subnet masks from the given classes only that is A, B and C. while classless address is one where IP addresses with different subnet masks in the same network are used to enable efficient use of IP addresses[8].

Subnetting

Ipv4 represents network field and host field. When some part of host field that is fewer MSBs from Host field is taken and used as sub network field it is called as subnetting. Through subnetting the network can expand while keeping network IP as same[9].

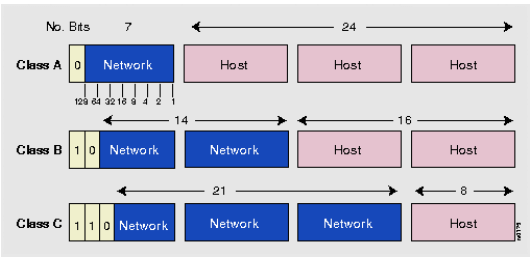

Fig. 5: Different IP classes[6]

Public and private IPs

A public IP address is the address that is when assigned to a device, it can be directly accesses over the internet. All servers and publicly known devices has public IP addresses. A public IP address is globally unique and it can be obtained from ISPs[11].

IPv4 has limited number of addresses and if each device is given a public IP then the IPv4 addressing scheme is not sufficient, to solve this problem each organization has one public IP to represent itself and all internal networks and devices ha private IP addresses. These are the addresses which any one can use for their personal use without any permissions. So this way number of addresses can be saved as each organizations only uses private IPs to have inter networking[11].

The IANA has held in reserve the following three blocks of the IP address from each of class A, B and C for private networks[12]:

10.0.0.0 – 10.255.255.255
(Total Addresses: 16,777,216)
172.16.0.0 – 172.31.255.255
(Total Addresses: 1,048,576)
192.168.0.0 – 192.168.255.255
(Total Addresses: 65,536)

Dynamic Host Configuration Protocol (DHCP)

DHCP is a client/server protocol responsible for dynamically distributes network configuration parameters, such as interfaces, services and IP addresses. When the devices have static IP allocations and they are inactive the IP address is wasted for that time. The solution is to have DHCP configuration on server side which allocates IPs dynamically to users whenever they need it. And once they are power off the IP is taken

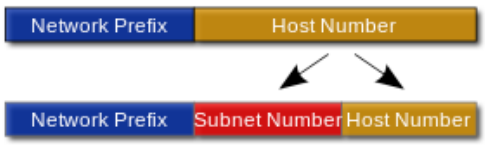

Fig. 6: Subnetting[10]

back and can be assigned to other users. Whenever any device resumes in a network it will get a new IP from DHCP server[13,14].

Network Address Translation (NAT)[15]

An Autonomous System uses a network infrastructure made up of private IP addresses. To have communication over the internet public IP addresses are needed since private IP addresses are rejected by ISP routers. In such scenarios to have the communication of private devices to the public world NAT is used. NAT can be a device, gateway or a firewall which has public IP address and represents organization over public network. Whenever the devices with private IPs makes request for public resources the NAT device first receives it and it will convert the packet address to itself and makes request on behalf of device using its own public identity. And on response from server it does the reverse way [15]. In Fig. 7 NAT device has public address as 126.22.99.144 and all private IPs are of range 10.25.1.X.

Limitations of IPv4

The current version of IPv4 has not been changed from last 25 years. However continuous growth of internet enabled devices has put IPv4 addressing at an end[17].

• Insufficient IP address space

With only 32-bit capacity, IPv4 addresses have become comparatively inadequate, forcing some organizations to use NAT. NAT does not support standards-based network layer security and can create problems when connecting two organizations that use the identical private address.

• Address prefix allocation

The existing IPv4 Internet routing communications is a mixture of both flat and hierarchical routing.

• Complexity of configuration

Most IPv4 implementations are either manually configured or DHCP. With more computers and devices using IP, there is a need for a simpler and more automatic configuration of addresses.

• Data security

IPSec is a Internet Protocol security standard which protects the private communication over public infrastructures. IPSec is an optional field in IPv4 and most of the times other alternatives are used which can be vulnerable.

• Quality of Service (QoS)

While standards for QoS exist for IPv4, no recognition of packet flow for QoS handling by routers is existing within the IPv4 header. IPv4 QoS field has partial functionality and payload detection using a TCP and UDP port is not promising when the IPv4 packet payload is encrypted.

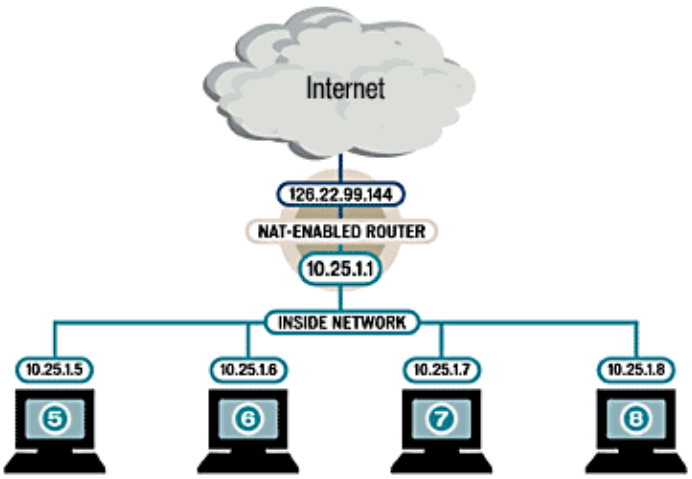

Fig. 7 Network Address Translation[16]

VI. IPV6

The current version of Internet Protocol IPv4 has not been substantially changes in the past 25 years.IPv4 has proven to be robust and easily implemented. In the early stage, the deployment of IPv6 is prepared and begun on the IPv4-based network. In the intermediate stage, IPv4 and IPv6 coexist. In the later stage, IPv6 plays a leading role on the network and the IPv4 network is gradually withdrawing from the market. Meanwhile, researchers put forward many transition mechanisms for different network infrastructures and different evolution stages. The deployment of IPv6, however, is still far below expectation. The causes include, certain technologies such as NAT alleviate the IPv4 address exhaustion. There is no IPv6-based killer application yet. The costs for network upgrade are huge. In view of the facts, it is generally accepted in the Industry that the IPv6 evolution process has changed from the IPv4/IPv6 transition into the long-term IPv4- IPv6 coexistence. Actually, the delayed deployment of IPv6 makes the IPv4/IPv6 transition more complex. According to the related statistics, the IPv4 allocation pool has been depleted around 2012. By now, no IPv4 address will be available for any new user. The originally most ideal dual-stack mode is facing a new problem, how to maintain IPv4 services in the case of IPv4 address shortage. In addition, having the technology complexity, the original transition technologies need to be optimized and improved. The following parts respectively describe the basic transition technologies and the comprehensive application of these technologies. According to different network infrastructures, users can choose a proper approach to overcome the difficulties in the transition period. It helps users to implement a smooth transition from the IPv4- based network to IPv6.

Need of IPv6[18]

The business and private user situations that benefit from IPv6 have been identified and described:

- E-government: A government network comprises interconnections of various government sections and central services networks, offering services for internal clients as well as citizens (e.g. election, tax declaration, car registration, etc.). By removing NAT, IPv6 is expected to foster e-government services and to facilitate management of the network.
- Mobile Worker:Employers of cell phones expect to stay connected without interruption while roaming between different access networks and service providers. Therefore Mobile IP has been consistent. Since IPv6 provides adequate addresses and advanced features, it is expected that a mobility service will be based on Mobile IPv6.
- Public Safety: Public safety establishments call for IP-based broadband communication that is exchange of videos, pictures, documents, messages, and all, on-site as well as with the command control centre. The IPv6 benefits in this scenario are auto configuration, enhanced mobility, and easier interworking between different organisations.
- Direct secure end-to-end communication: Employers of mobile devices expect to get access to their corporate network or to work with co-workers while being mobile and remote. In this scenario, Mobile IPv6 route optimization could be deployed in order to provide a direct end-to-end link between mobile device and its peer without inefficient triangular routing over a mobility anchor point.
- Corporate network: Business networks are evolving from border-protected sets of internal resources to an extended enterprise planning. Forthcoming IPv4 address shortage and possible benefits of IPv6 demand for IPv6 migration.
- Personal Area Network (PAN): Users may carry numerous devices like phone, laptop, sensors, input devices and one of the devices could provide admission to the Internet (via WLAN,3G), providing mobility service for the PAN via IPv6-based network mobility(NEMO).
- Access security: IEEE 802.1X is deployed to regulate access to a network. Once connected, an infected or malicious node is able to target its neighbours. In IPv6, secure neighbour discovery (SEND) can prevent this type of attack.
- Home network connectivity and networked

gaming: Networked games are becoming more widespread. IPv6 would provide a clear network layer without NAT boxes that would facilitate the deployment of networked games requiring the users to have IPv6 connectivity at home.

- Collective transports: Cooperative transport e.g. a plane provides Internet connection to passengers and airline applications. IPv6-based network flexibility provides address solidity in case various upstream technologies are used.

IPv6 Header Formats

Each field epitomises the following signification in IPv6 Headers[20].

- Version: This field is 4 bits long. The value 6 indicates that the packet is an IPv6 packet.
- Traffic Class: This field is 8 bits long. It is similar to the TOS field in IPv4.
- Flow Label: This field is 20 bits long. It is a new field in IPv6. The Flow Label field can be used to tag packets of a specific flow to differentiate the packets at the network layer.

The routers in the forwarding path can identify and process a flow based on the flow Label. With this label, a router need not check deep into the packet to identify the flow, because this information is available in the IPv6 header. Similarly, the destination node can identify a flow based on the specific flow label. In addition, QoS processing can still be performed based on the flow label even after IPsec is applied, because the flow label is carried in the header.

- Payload Length: This field is 16 bits long. It indicates the IPv6 payload length in octets, that is, the length of the section behind the basic header of the IPv6 packet, including all the extension headers.
- Next Header: This field is 8 bits long. It identifies the type of the header next to the current header (the basic header or an extension header). The type defined in this field is the same as the protocol field value in IPv4. IPv6 defines extension headers that form a chain of headers linked together by the Next Header field, contained in the basic header or each extension header. This mechanism provides more efficiency in the processing of extension headers. The intermediate routers process only the extension headers that need be processed. This improves the forwarding efficiency.
- Hop Limit: This field is 8 bits long. It is similar to the TTL field in IPv4. Every node decrements the value of this field by 1 before forwarding the packet. If the value of this field is already 0, the node simply discards the packet.
- Source Address: This field is 128 bits long. It indicates the source address of the packet.
- Destination Address: This field is 128 bits long. It indicates the destination address of the packet.

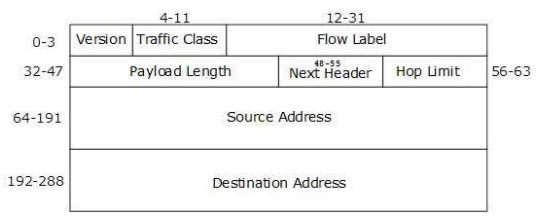

Fig. 8: IPv6 Header[19]

Address Format[21,22]

IPv6 addresses are represented as a sequence of 16-bit hexadecimal fields separated by colons (:) in the format: x:x:x:x:x:x:x:x.

Following are two examples of IPv6 addresses: 2001:DB8:7654:3210:FEDC:BA98:7654:3210 2001:DC8:0:0:8:800:200C:417A

IPv6 addresses frequently contain successive hexadecimal fields of zeros. Two colons (::) may be used to compress successive hexadecimal fields of zeros at the start, middle, or end of an IPv6 address (the colons represent successive hexadecimal fields of zeros). The table below lists compressed IPv6 address formats. A double colon may be used as part of the ipv6-address argument when successive 16-bit values are denoted as zero. You can configure multiple IPv6 addresses per interfaces, but only one link-local address.

e.g. 2001:0:0:0:0DB8:800:200C:417A can be written as

e.g. 2001::0DB8:800:200C:417A is equivalent to FF01:0:0:0:0:0:0:101 FF01::101

REFERENCES

1. Addressing, MVN UNiversity (2016, Oct.2). [Online], Available : http://mvn.edu.in/lms/mod/book/view.php?id=58
2. How TCP/IP works, informbit (2016, Oct.4). [Online], Available : http://www.informit.com/articles/article.aspx?p=1807488&seqNum=2
3. Introduction to MAC addresses. Lifewire (2016, Oct.2). [Online], Available : https://www.lifewire.com/introduction-to-mac-addresses-817937
4. Registered ports, Wikipedia (2016, Oct.10). [Online], Available : https://en.wikipedia.org/wiki/Registered_port
5. Internet protocol version 4, Tutorial point (2016, Oct.12). [Online], Available : https://www.tutorialspoint.com/ipv4/ipv4_quick_guide.htm
6. IP – Addresses Classful, infocellar(2016, Oct.20). [Online], Available : http://infocellar.com/networks/ip/classful.htm
7. IANA, Wikipedia (2016, Oct.25). [Online], Available : https://en.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority
8. Classful vs Classless Networks, Cisco (2016, Oct.28). [Online], Available : https://learningnetwork.cisco.com/thread/34420
9. IP Addressing and subnetting for new users, Cisco (2016, Nov.2). [Online], Available : http://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html
10. Subnetworks , wikipedia(2016, Nov.5). [Online], Available : https://en.wikipedia.org/wiki/Subnetwork
11. Public and private IP Addresses, IPlocation (2016, Nov. 5). [Online], Available : https://www.iplocation.net/public-vs-private-ip-address
12. Public and private IP Addresses, Siliconindia (2016, Nov.10). [Online], Available : http://www.siliconindia.com/online-courses/tutorials/What-are-Private-and-Public-IP-Addresses-id-109.html
13. DHCP, Wikipedia(2016, Nov.12). [Online], Available : https://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
14. What is DHCP?, Microsoft (2016, Nov.20). [Online], Available : https://technet.microsoft.com/en-us/library/cc781008(v=ws.10).aspx
15. NAT, Wikipedia (2016, Nov.25). [Online], Available : https://en.wikipedia.org/wiki/Network_address_translation
16. NAT, Computerworld (2016, Dec.10). [Online], Available : http://www.computerworld.com/article/2591804/lan-wan/network-address-translation.html
17. A primer on IPv6 white paper, Digi International (2016, Dec.20). [Online], Available : https://www.digi.com/pdf/wp_ipv6.pdf
18. IPv6 security models and dual stack (IPv6/IPv4) implications (2016, Dec 22). [Online] Available :http://cordis.europa.eu/fp7/ict/security/docs/ipv6-security-models-and-implications-executive-summary.pdf
19. IPv6 Headers, Tutorialspoint, (2016, Dec. 23). [Online], Available : https://www.tutorialspoint.com/ipv6/ipv6_headers.htm
20. IPv6 Packet, Wikipedia, (2016, Dec. 23). [Online], Available : https://en.wikipedia.org/wiki/IPv6_packet
21. Configuring IPv6, Cisco, (2016, Dec. 24). [Online], Available http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/unicast/configuration/guide/l3_cli_nxos/l3_ipv6.pdf
22. IPv6 Address types, Tutorialspoint, (2016, Dec. 23). [Online], Available : https://www.tutorialspoint.com/ipv6/ipv6_address_types.htm.