IPv6
Scribe notes for cs625

Venkata Rao Ch
Instructor Dr. Bhaskaran Raman
Y3111052

Introduction:

Due to the exponential growth of the internet the IP address space is exhausted and consequently the IP addresses have become scarce.The problem of running out of IP addresses is not a theoritical problem that might occur at some point in future. It is happening right now. The long term solution is to migrate the whole IP to IPv6, which has 128-bit addresses. This transition may take some years to complete. As a consequence some quick fixes came in the form of CIDR and NAT(Network Address Translation).

CIDR:

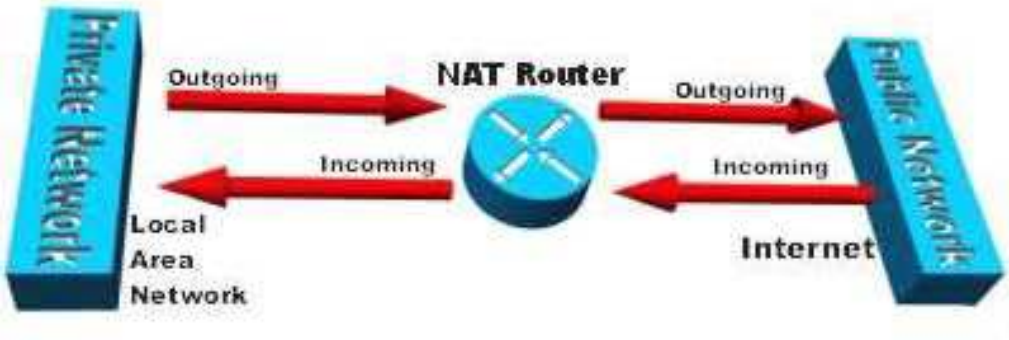
Briefly the basic idea in CIDR is to allocate the IP address(those address that are not used) in variable sized blocks, with out regard to the classes. If a site needs, say, 2000 addresses, it is given a block of 2048-addresses on a 2048 boundary.

NAT:

The idea behind NAT is to assign each company a single IP address(or at most, a small number of them) for internet traffic. With in the company, every computer gets a unique IP address which is used for routing intramural traffic. To handle the packets exiting the company the following scheme will be followed.

Three ranges of IP addresses have been declared as private. Organizations may use them as they wish. The important thing is that no packets containing these addresses may appear on the Internet itself. The three reserved ranges are:

10.0.0.0 -10.255.255.255/8
172.16.0.0 - 172.31.255.255/12
192.168.0.0 -192.168.255.255/16



The operation of NAT Router(NAT box) is as shown above. Assume that within the company premises every machine has a unique address of the form 10.x.y.z. However, when a packet leaves the company premises, it passes through a NAT box that converts the internal IP source address, to the company's true IP address and sends it to the destination.

When a reply comes back to the, it will be addressed to the true address that is assigned to the company. Here come the problem of finding the actual destination. The solution to this problem is as follows. Whenever an outgoing packet enters int ot the NAT box, the 10.x.y.x source address is replaced by the company's true IP address. In addition, the TCP source port field is replaced by an index into the NAT box's 65,536-entry translation table. This table entry contains the original IP address and the original souce port. Finally, both the IP and TCP header checksums are recomputed and inserted into the packet.

When a packet arrives at the NAT box from the ISP, the source port in the TCP header is extracted and used as an index into the NAT box's mapping table. From the entry located, the internal IP address and original TCP source port are extracted and inserted into the packet. Then both the IP and TCP checksums are recomputed and inserted into the packet. The packet is then sent to the company router for normal delivery using the 10.x.y.z address.

Although this scheme solves the problem of scarcity of IP address, there are many objections to it.

1. NAT violates the architectural model of IP, which states that every IP address uniquely identifies a single machine worldwide.
2. Nat change the Internet from a connection less network to a kind of connection oriented network.
3. NAT violate the most fundamental rule of protocol layering.
4. Processes on the Internet are not required to use TCP or UDP.
5. Some applications insert IP addresses in the body of the text.
6. Since the TCP source field is 16 bits at most 65,536 machines can be mapped onto an IP address. Actually the number is slightly less because the first 4096 ports are reserved for special uses.

IPNL(IP Next Layer):

Basically IPNL scheme is an extension to the NAT scheme. The major attributes of IPNL are as follows.

1. It is a NAT extended architecture.

2. It uses Fully Qualified Domain names as end-to-end host identifier in packets.

3. It extends the IP address space such that the globally unique IP address space forms the high order part of the IPNL address and the private addrees forms the low order address space.

IPv6:

While CIDR,NAT and IPNL may buy a few more year's time, everyobne realizes that the days of IP in its current form are numbered. The ultimate goal to get an address space which is never exhausted. There comes IPv6.

IPv6 fixed header(required)

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop limit
			Source Address (16 bytes)
Address			Destination (16 bytes)

The version field is always 6 for IPv6. During the transition period from IPv4, which will take a decade, routers will be able to examine this field to tell what kind of packet they have.

The traffic class field is used to distinguish between packets with different real-time delivery requirements.

The flow label field is also still experimental but will be used to allow a

source and destination to set up a pseudo connection with particular properties and requirements.

The pay load length field tells how many bytes follow the 40-byte header. The name was changed from the IPv4 of Total length field because the meaning was changed slightly: the 40 header bytes are not counted as part of the length(as they used to be).

The next header field tells which of the six extension headers, if any followw this one. If this header is last IP header, the Next header filed tells which transport protocol handler to pass the packet to.

The Hop limit filed is used to keep packets from living forever.

Next comes the 16-byte source address and 16-byte destination address. They are written as eight groups of four hexa decimal digits with colons between the groups.

Eg:

1234:0000:8765:2341:AC72:45EF:CDEF:8000

Extension headers:

Some of the missing IPv4 fields are occasionally still needed, so IPv6 has introduced the concept of an extension header. Six kinds of extension headers are defined at present.

Extension header	Description
Hop-by-hop options	Miscellaneous information for routers
Destination options	Additional information for the destination
Routing	Loose list of routers to visit
Fragmentation	Management of datagram fragments
Authentication	Verification of the sender’s identity
Encrypted security payload	Information about the encrypted contents