Computer Networks (CS425)

Instructor: Dr. Dheeraj Sanghi

Prev| Next| Index

Network Layer

What is Network Layer?

The network layer is concerned with getting packets from the source all the way to the destination. The packets may require to make many hops at the intermediate routers while reaching the destination. This is the lowest layer that deals with end to end transmission. In order to achieve its goals, the network layer must know about the topology of the communication network. It must also take care to choose routes to avoid overloading of some of the communication lines while leaving others idle. The network layer-transport layer interface frequently is the interface between the carrier and the customer, that is the boundary of the subnet. The functions of this layer include :

1. Routing - The process of transferring packets received from the Data Link Layer of the source network to the Data Link Layer of the correct destination network is called routing. Involves decision making at each intermediate node on where to send the packet next so that it eventually reaches its destination. The node which makes this choice is called a router. For routing we require some mode of addressing which is recognized by the Network Layer. This addressing is different from the MAC layer addressing.
2. Inter-networking - The network layer is the same across all physical networks (such as Token-Ring and Ethernet). Thus, if two physically different networks have to communicate, the packets that arrive at the Data Link Layer of the node which connects these two physically different networks, would be stripped of their headers and passed to the Network Layer. The network layer would then pass this data to the Data Link Layer of the other physical network..
3. Congestion Control - If the incoming rate of the packets arriving at any router is more than the outgoing rate, then congestion is said to occur. Congestion may be caused by many factors. If suddenly, packets begin arriving on many input lines and all need the same output line, then a queue will build up. If there is insufficient memory to hold all of them, packets will be lost. But even if routers have an infinite amount of memory, congestion gets worse, because by the time packets reach to the front of the queue, they have already timed out (repeatedly), and duplicates have been sent. All these packets are dutifully forwarded to the next router, increasing the load all the way to the destination. Another reason for congestion are slow processors. If the router's CPUs are slow at performing the bookkeeping tasks required of them, queues can build up, even though there is excess line capacity. Similarly, low-bandwidth lines can also cause congestion.

We will now look at these function one by one.

Addressing Scheme
IP addresses are of 4 bytes and consist of :
i) The network address, followed by
ii) The host address
The first part identifies a network on which the host resides and the second part

identifies the particular host on the given network. Some nodes which have more than one interface to a network must be assigned separate internet addresses for each interface. This multi-layer addressing makes it easier to find and deliver data to the destination. A fixed size for each of these would lead to wastage or under-usage that is either there will be too many network addresses and few hosts in each (which causes problems for routers who route based on the network address) or there will be very few network addresses and lots of hosts (which will be a waste for small network requirements). Thus, we do away with any notion of fixed sizes for the network and host addresses.
We classify networks as follows:

1. **Large Networks :** 8-bit network address and 24-bit host address. There are approximately 16 million hosts per network and a maximum of 126 (2^7 - 2) Class A networks can be defined. The calculation requires that 2 be subtracted because 0.0.0.0 is reserved for use as the default route and 127.0.0.0 be reserved for the loop back function. Moreover each Class A network can support a maximum of 16,777,214 (2^24 - 2) hosts per network. The host calculation requires that 2 be subtracted because all 0's are reserved to identify the network itself and all 1s are reserved for broadcast addresses. The reserved numbers may not be assigned to individual hosts.
2. **Medium Networks :** 16-bit network address and 16-bit host address. There are approximately 65000 hosts per network and a maximum of 16,384 (2^14) Class B networks can be defined with up to (2^16-2) hosts per network.
3. **Small networks :** 24-bit network address and 8-bit host address. There are approximately 250 hosts per network.

You might think that Large and Medium networks are sort of a waste as few corporations/organizations are large enough to have 65000 different hosts. (By the way, there are very few corporations in the world with even close to 65000 employees, and even in these corporations it is highly unlikely that each employee has his/her own computer connected to the network.) Well, if you think so, you're right. This decision seems to have been a mistak

Address Classes

The IP specifications divide addresses into the following classes :

- Class A - For large networks

0	7 bits of the network address	24 bits of host address

- Class B - For medium networks

1	0	14 bits of the network address	16 bits of host address

- Class C - For small networks

1	1	0	21 bits of the network address	8 bits of host address

- Class D - For multi-cast messages (multi-cast to a "group" of networks)

1	1	1	0	28 bits for some sort of group address

- Class E - Currently unused, reserved for potential uses in the future

1	1	1	1	28 bits

Internet Protocol

Special Addresses : There are some special IP addresses :

1. Broadcast Addresses They are of two types :
   (i) Limited Broadcast : It consists of all 1's, i.e., the address is 255.255.255.255 . It is used only on the LAN, and not for any external network.
   (ii) Directed Broadcast : It consists of the network number + all other bits as1's. It reaches the router corresponding to the network number, and from there it broadcasts to all the nodes in the network. This method is a major security problem, and is not used anymore. So now if we find that all the bits are 1 in the host no. field, then the packet is simply dropped. Therefore, now we can only do broadcast in our own network using Limited Broadcast.
2. Network ID = 0
   It means we are referring to this network and for local broadcast we make the host ID zero.
3. Host ID = 0
   This is used to refer to the entire network in the routing table.
4. Loop-back Address
   Here we have addresses of the type 127.x.y.z It goes down way upto the IP layer and comes back to the application layer on the same host. This is used to test network applications before they are used commercially.

Subnetting
Sub netting means organizing hierarchies within the network by dividing the host ID as per our network. For example consider the network ID : 150.29.x.y
We could organize the remaining 16 bits in any way, like :
4 bits - department
4 bits - LAN
8 bits - host
This gives some structure to the host IDs. This division is not visible to the outside world. They still see just the network number, and host number (as a whole). The network will have an internal routing table which stores information about which router to send an address to. Now consider the case where we have : 8 bits - subnet number, and 8 bits - host number. Each router on the network must know about all subnet numbers. This is called the subnet mask. We put the network number and subnet number bits as 1 and the host bits as 0. Therefore, in this example the subnet mask becomes : 255.255.255.0 . The hosts also need to know the subnet mask when they send a packet. To find if two addresses are on the same subnet, we can AND source address with subnet mask, and destination address with with subnet mask, and see if the two results are the same. The basic reason for sub netting was avoiding broadcast. But if at the lower level, our switches are smart enough to send directed messages, then we do not need sub netting. However, sub netting has some security related advantages.

Supernetting
This is moving towards class-less addressing. We could say that the network number is 21 bits (for 8 class C networks) or say that it is 24 bits and 7 numbers following that. For example : a.b.c.d / 21 This means only look at the first 21 bits as the network address.

Addressing on IITK Network
If we do not have connection with the outside world directly then we could have Private IP addresses (172.31) which are not to be publicised and routed to the

outside world. Switches will make sure that they do not broadcast packets with such addressed to the outside world. The basic reason for implementing subnetting was to avoid broadcast. So in our case we can have some subnets for security and other reasons although if the switches could do the routing properly, then we do not need subnets. In the IITK network we have three subnets -CC, CSE building are two subnets and the rest of the campus is one subset

Packet Structure

<table>
<tr><td>Version Number (4 bits)</td><td>Header Length (4 bits)</td><td>Type of Service (8 bits)</td><td colspan="2">Total Length (16 bits)</td></tr>
<tr><td colspan="3">ID (16 bits)</td><td>Flags (3bits)</td><td>Flag Offset (13 bits)</td></tr>
<tr><td colspan="2">Time To Live (8 bits)</td><td>Protocol (8 bits)</td><td colspan="2">Header Checksum (16 bits)</td></tr>
<tr><td colspan="5">Source (32 bits)</td></tr>
<tr><td colspan="5">Destination (32 bits)</td></tr>
<tr><td colspan="5">Options</td></tr>
</table>

Version Number : The current version is Version 4 (0100).

1. **Header Length :** We could have multiple sized headers so we need this field. Header will always be a multiple of 4bytes and so we can have a maximum length of the field as 15, so the maximum size of the header is 60 bytes (20 bytes are mandatory).
2. **Type Of Service (ToS) :** This helps the router in taking the right routing decisions. The structure is :
   First three bits : They specify the precedences i.e. the priority of the packets.
   Next three bits :
      D bit - D stands for delay. If the D bit is set to 1, then this means that the application is delay sensitive, so we should try to route the packet with minimum delay.
      - T bit - T stands for throughput. This tells us that this particular operation is throughput sensitive.
      - R bit - R stands for reliability. This tells us that we should route this packet through a more reliable network.

   Last two bits: The last two bits are never used. Unfortunately, no router in this world looks at these bits and so no application sets them nowadays. The second word is meant for handling fragmentations. If a link cannot transmit large packets, then we fragment the packet and put sufficient information in the header for recollection at the destination.
3. **ID Field :** The source and ID field together will represent the fragments of a unique packet. So each fragment will have a different ID.
4. **Offset :** It is a 13 bit field that represents where in the packet, the current fragment starts. Each bit represents 8 bytes of the packet. So the packet size can be at most 64 kB. Every fragment except the last one must have its size in bytes as a multiple of 8 in order to ensure compliance with this structure. The reason why the position of a fragment is given as an offset value instead of simply numbering each packet is because refragmentation may occur somewhere on the path to the other node. Fragmentation, though supported by IPv4 is not encouraged. This is because if even one fragment is lost the entire packet needs to be discarded. A quantity M.T.U (Maximum Transmission Unit) is defined for each link in the route. It is the size of the largest packet that can be handled by the link. The Path-M.T.U is then defined as the size of the largest packet that can be handled by the path. It is the smallest of all the MTUs along the path. Given

information about the path MTU we can send packets with sizes smaller than the path MTU and thus prevent fragmentation. This will not completely prevent it because routing tables may change leading to a change in the path.

5. **Flags :**It has three bits -
   - M bit : If M is one, then there are more fragments on the way and if M is 0, then it is the last fragment
   - DF bit : If this bit is sent to 1, then we should not fragment such a packet.
   - Reserved bit : This bit is not used.

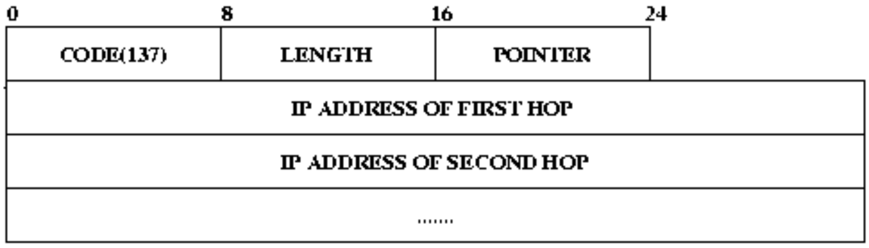
   Reassembly can be done only at the destination and not at any intermediate node. This is because we are considering Datagram Service and so it is not guaranteed that all the fragments of the packet will be sent thorough the node at which we wish to do reassembly.
6. **Total Length :** It includes the IP header and everything that comes after it.
7. **Time To Live (TTL) :** Using this field, we can set the time within which the packet should be delivered or else destroyed. It is strictly treated as the number of hops. The packet should reach the destination in this number of hops. Every router decreases the value as the packet goes through it and if this value becomes zero at a particular router, it can be destroyed.
8. **Protocol :** This specifies the module to which we should hand over the packet (UDP or TCP). It is the next encapsulated protocol.

Value	Protocol
0	Pv6 Hop-by-Hop Option.
1	ICMP, Internet Control Message Protocol.
2	IGMP, Internet Group Management Protocol. RGMP, Router-port Group Management Protocol.
3	GGP, Gateway to Gateway Protocol.
4	IP in IP encapsulation.
5	ST, Internet Stream Protocol.
6	TCP, Transmission Control Protocol.
7	UCL, CBT.
8	EGP, Exterior Gateway Protocol.
9	IGRP.
10	BBN RCC Monitoring.
11	NVP, Network Voice Protocol.
12	PUP.
13	ARGUS.
14	EMCON, Emission Control Protocol.
15	XNET, Cross Net Debugger.
16	Chaos.
17	UDP, User Datagram Protocol.
18	TMux, Transport Multiplexing Protocol.
19	DCN Measurement Subsystems.
-	
-	
255	

9. **Header Checksum :** This is the usual checksum field used to detect errors. Since the TTL field is changing at every router so the header checksum (upto the options field) is checked and recalculated at every router.
10. **Source :** It is the IP address of the source node
11. **Destination :** It is the IP address of the destination node.
12. **IP Options :** The options field was created in order to allow features to be added into IP as time passes and requirements change. Currently 5 options are specified although not all routers support them. They are:
    - **Securtiy:** It tells us how secret the information is. In theory a military router might use this field to specify not to route through certain routers. In

practice no routers support this field.

- **Source Routing:** It is used when we want the source to dictate how the packet traverses the network. It is of 2 types
  -> Loose Source Record Routing (LSRR): It requires that the packet traverse a list of specified routers, in the order specified but the packet may pass though some other routers as well.
  -> Strict Source Record Routing (SSRR): It requires that the packet traverse only the set of specified routers and nothing else. If it is not possible, the packet is dropped with an error message sent to the host.

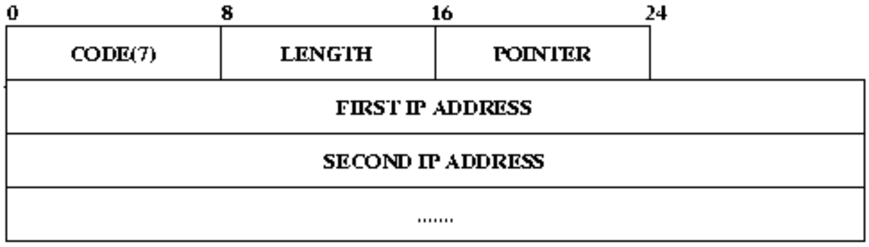


0	8	16	24
CODE(137)	LENGTH	POINTER	
IP ADDRESS OF FIRST HOP			
IP ADDRESS OF SECOND HOP			
....			

The format of Source Route options in an IP Datagram

The above is the format for SSRR. For LSRR the code is 131.

- **Record Routing :**

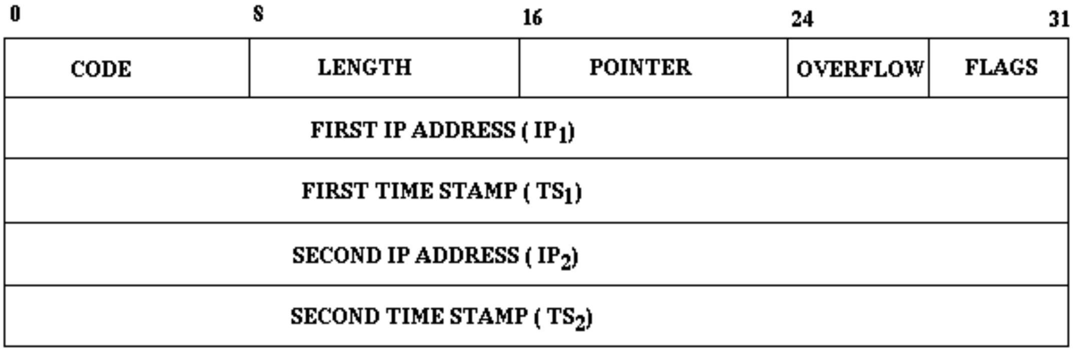


0	8	16	24
CODE(7)	LENGTH	POINTER	
FIRST IP ADDRESS			
SECOND IP ADDRESS			
....			

Format of the Record Route option in an IP Datagram

In this the intermediate routers put there IP addresses in the header, so that the destination knows the entire path of the packet. Space for storing the IP address is specified by the source itself. The pointer field points to the position where the next IP address has to be written. Length field gives the number of bytes reserved by the source for writing the IP addresses. If the space provided for storing the IP addresses of the routers visited, falls short while storing these addresses, then the subsequent routers do not write their IP addresses.

- **Time Stamp Routing :**



0	8	16	24	31
CODE	LENGTH	POINTER	OVERFLOW	FLAGS
FIRST IP ADDRESS (IP_1)				
FIRST TIME STAMP (TS_1)				
SECOND IP ADDRESS (IP_2)				
SECOND TIME STAMP (TS_2)				

Format Of Timestamp Option

It is similar to record route option except that nodes also add their timestamps to the packet. The new fields in this option are
-> Flags: It can have the following values

    - 0- Enter only timestamp.
    - 1- The nodes should enter Timestamp as well as their IP.
    - 3 - The source specifies the IPs that should enter their timestamp. A special point of interest is that only if the IP is the same as that at the pointer then the time is entered. Thus if the source specifies IP1 and IP2 but IP2 is first in the path then the field IP2 is left empty, even after having reached IP2 but before reaching IP1.

  -> Overflow: It stores the number of nodes that were unable to add their timestamps to the packet. The maximum value is 15.

- **Format of the type/code field**

Copy Bit	Type of option	Option Number.

    - **Copy bit:** It says whether the option is to be copied to every fragment or not. a value of 1 stands for copying and 0 stands for not copying.
    - **Type:** It is a 2 bit field. Currently specified values are 0 and 2. 0 means the option is a control option while 2 means the option is for measurement
    - **Option Number:** It is a 5 bit field which specifies the option number.

  For all options a length field is put in order that a router not familiar with the option will know how many bytes to skip. Thus every option is of the form

- **TLV: Type/Length/Value.** This format is followed in not only in IP but in nearly all major protocols.

---

back to top
Prev| Next | Index