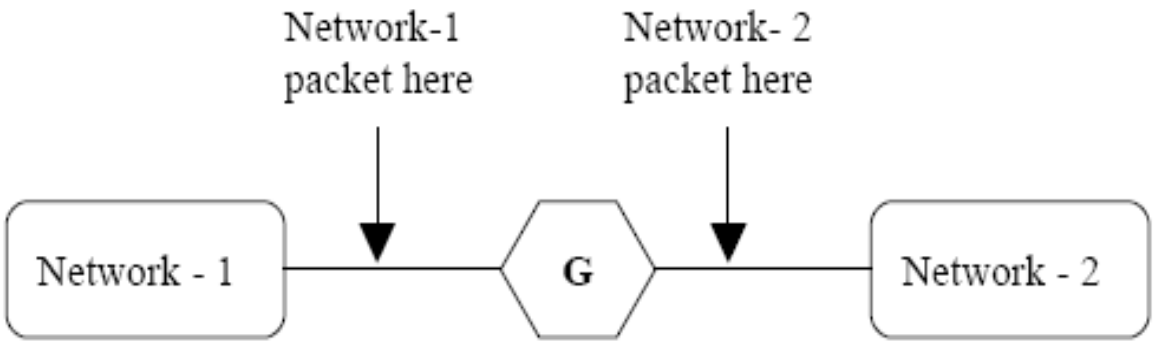
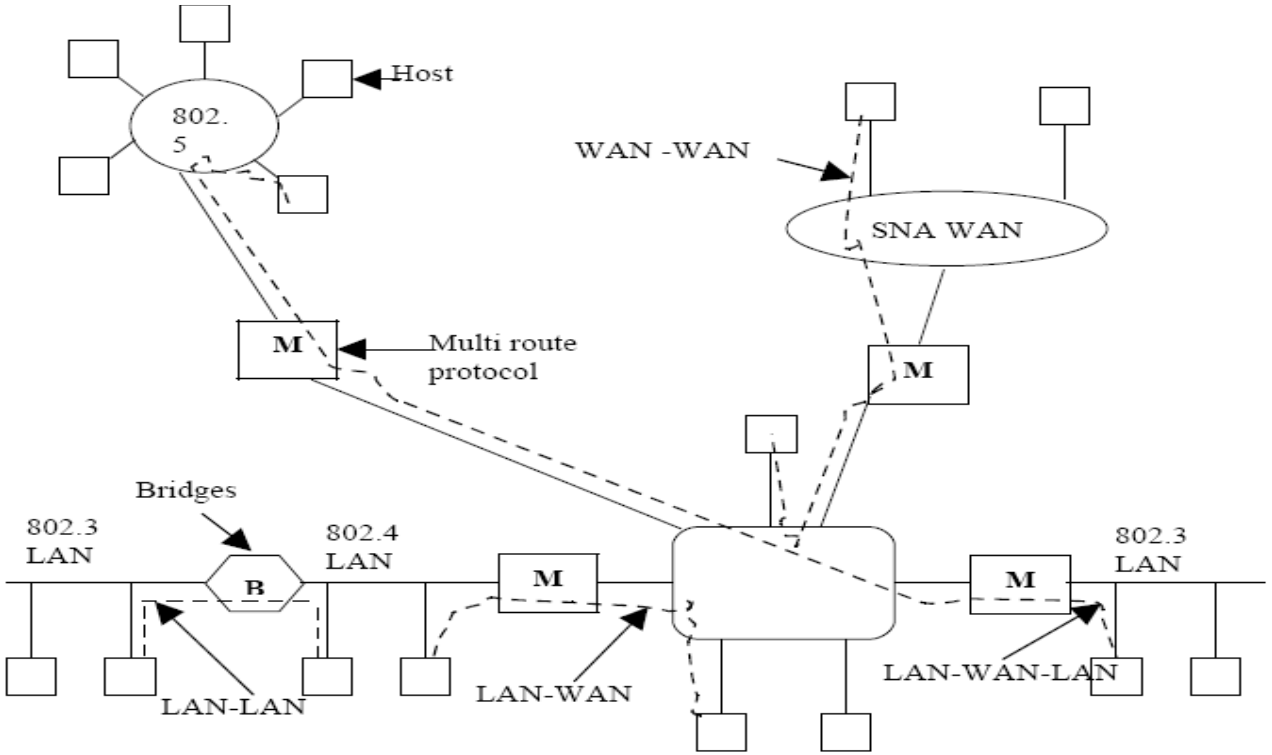
internetworking

- **Internetworking – Definition:**

  Connecting two or more dissimilar networks, using some devices [i.e. gateway] is called Internetworking. The devices used may be:
- (1) **Repeaters**: These are low level devices, which just amplify (or) regenerate weak signals
- (2) **Bridges**: These are store and forward devices; it accepts an entire frame and passes it up to data link layer, where checksum is verified.
- Then the frame is sent down to physical layer, for forwarding on a different network
- (3) **Multiprotocol routers**: Similar to bridges, except that they are found in network layer.
- It take incoming packet from one line and forward them on another, just as router, but the lines may belong to different networks and use3 different protocols
- (4) **Transport Gateways**: It makes a connection between two networks at the transport layer.
- (5) **Application gateways**: Connects two parts of an application in the application layer



Full Gateway between two WANS



* Using the technique of internetworking, it is possible to connect:

-> LAN – LAN

-> LAN – WAN

-> WAN – WAN

-> LAN – WAN – LAN

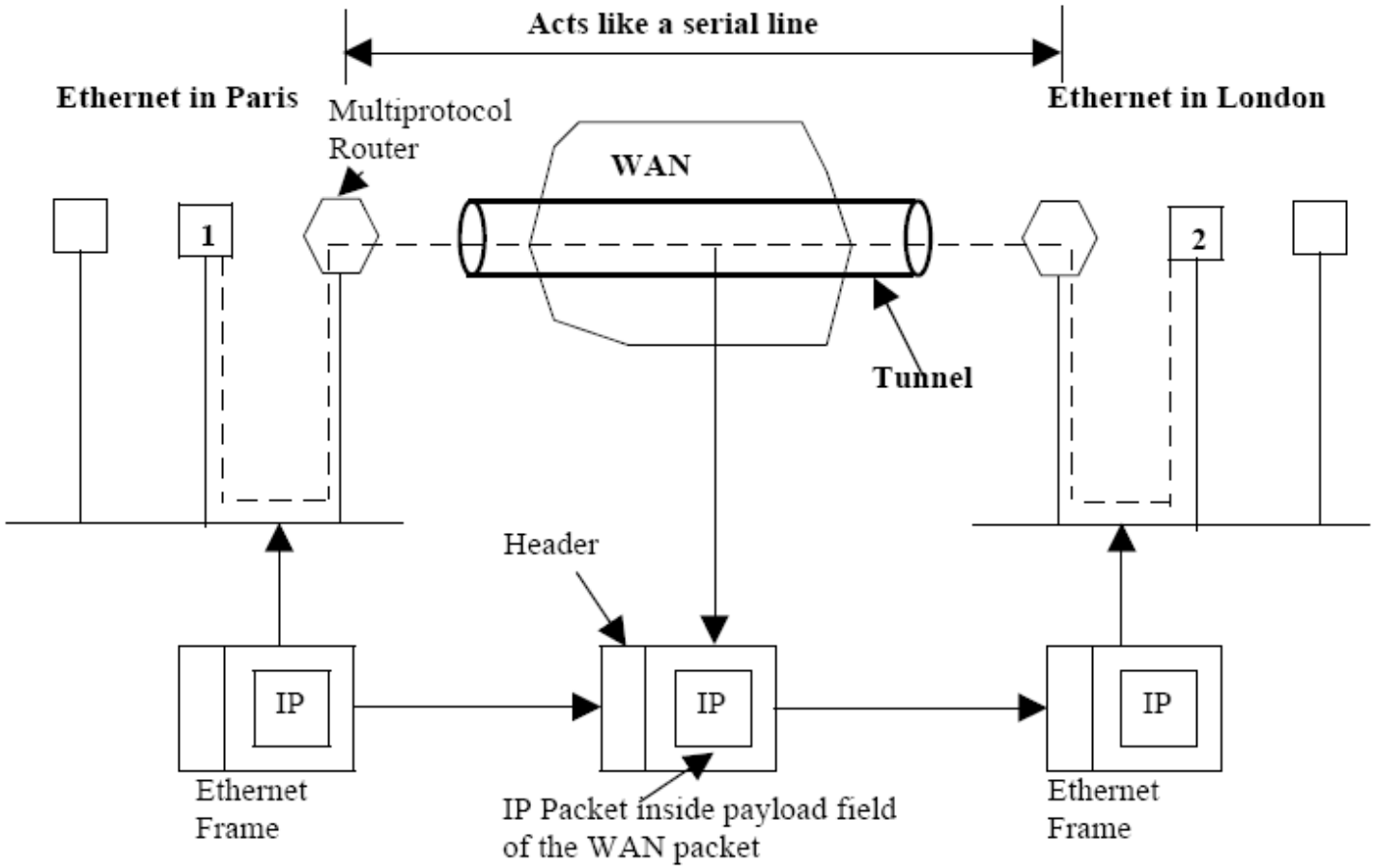
How Networks Differ

Item	Some possibility
Services offered	Connection oriented Vs Connection less
Protocols	IP,IPX,ATM
Addressing	Flat [802] vs. Hierarchical [IP]
Multicasting	Present or Absent
Packet Size	Every network has its maximum
Quality of service	May be present or absent; many different kinds
Error handling	Reliable, ordered and unordered delivery
Flow control	Sliding window
Congestion control	Leaky bucket, choke packets etc..
Security	Privacy rules, encryption etc

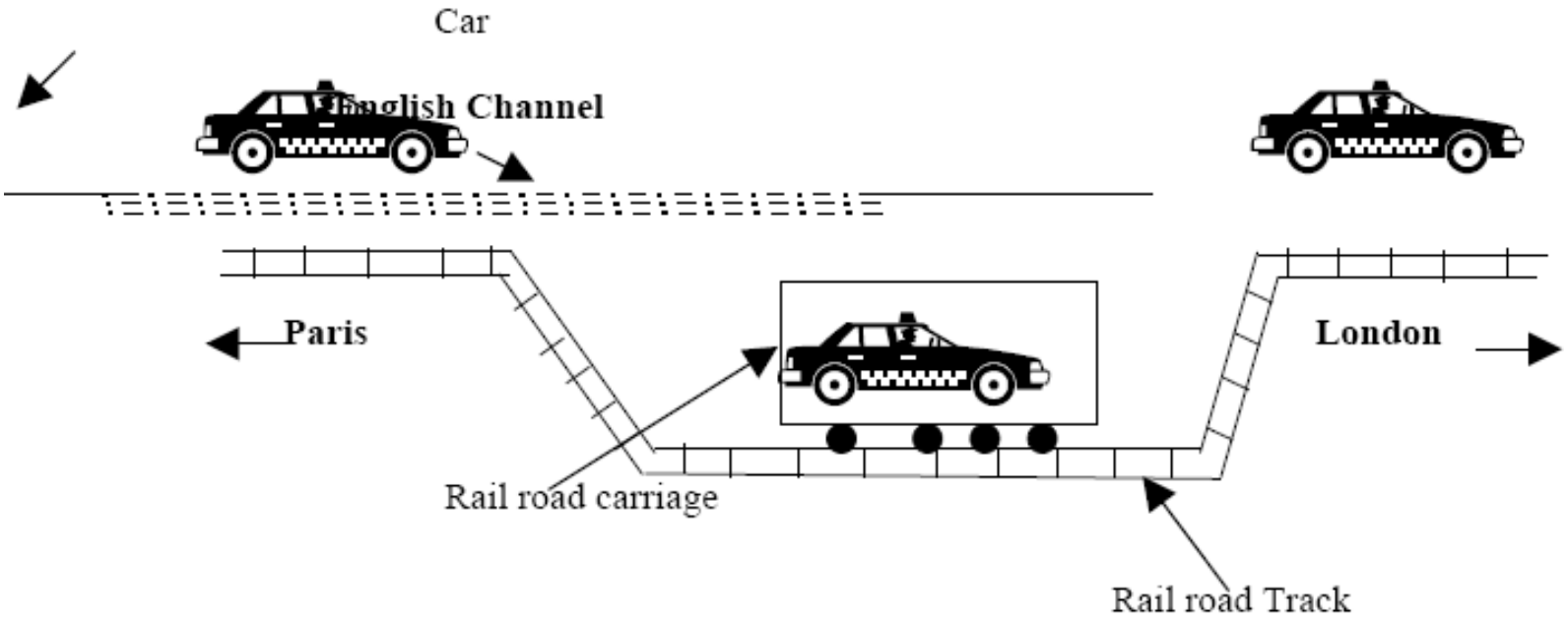
- **5.2 How Networks Can Be Connected**
- Networks can be interconnected by different devices, Let us briefly review that material. In the physical layer, networks can be connected by repeaters or hubs, which just move the bits from one network to an identical network.
- One layer up we find bridges and switches, which operate at the data link layer. They can accept frames, examine the MAC addresses, and forward the frames to a different network while doing minor protocol translation in the process

- In the network layer, we have routers that can connect two networks. If two networks have dissimilar network layers, the router may be able to translate between the packet formats, although packet translation is now increasingly rare. A router that can handle multiple protocols is called a multiprotocol router.
- In the transport layer we find transport gateways, which can interface between two transport connections.
- Finally, in the application layer, application gateways translate message semantics

- **Tunneling**
- * Handling the case of making two different networks internetwork is exceedingly difficult
- * In this technique, the **source and destination host are on the same type** of network, but there is a **different network in between**
- Example:
- * Think of an international bank with a TCP/IP based Ethernet in Paris, a TCP/IP based Ethernet in London and a WAN in between


Acts like a serial line
Ethernet in Paris
Multiprotocol
Router
WAN
Ethernet in London
1
2
Tunnel
Header
IP
IP
IP
Ethernet
Frame
IP Packet inside payload field
of the WAN packet
Ethernet
Frame

- The solution to this problem is a technique called tunneling.
- To send an IP Packet to host-2, host-1 **constructs the packets, containing the IP address** of host-2
- This packet is inserted into an Ethernet frame, addressed to the Paris Multiprotocol router, and puts it on the Ethernet
- When Multiprotocol router gets the frame, it **removes the IP packet**, insert it in the **payload field of WAN** network layer packet and address later to London Multiprotocol Router
- When it gets there, London router removes the IP packet and sends it to host-2 inside an Ethernet frame
- Here the WAN can be seen as a Big Tunnel, extending from one Multiprotocol Router to other
- The IP packets, just travel from one end of the tunnel to the other end
- Only the Multiprotocol router has to understand IP and WAN packets

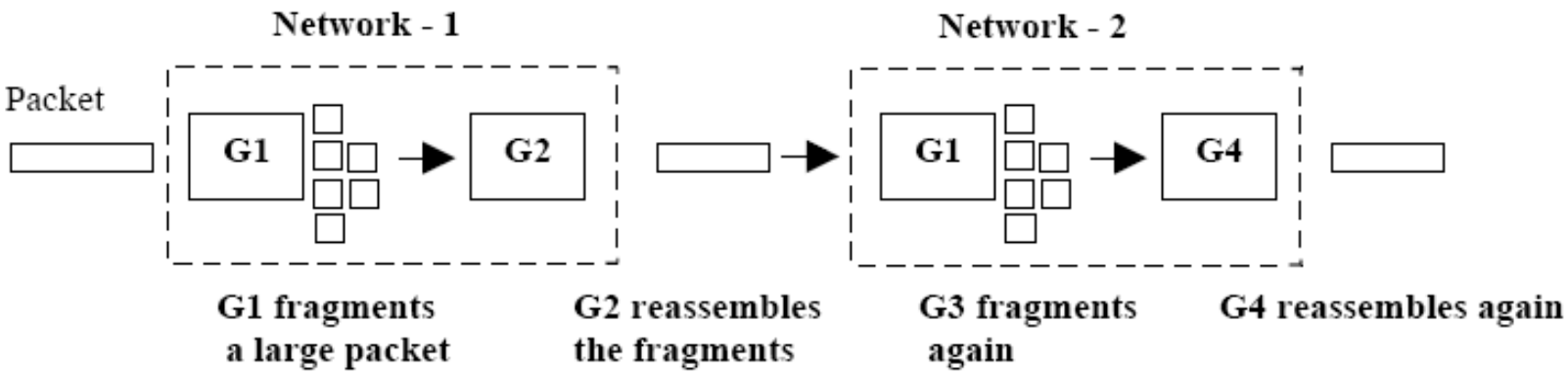

Car
English Channel
Paris
London
Rail road carriage
Rail road Track

- **Fragmentation:**
- What happens when a large packet wants to travel through a network, whose maximum packet size is too small
- The only solution to the above problem is, to allow gateways, to **break packets up into fragments**
- Sending each fragments as a separate internet packet
- Converting a large packet into fragments is easier than recombining the fragments back into the original packet
- Two strategies exist for recombine the fragments back into the original packet:

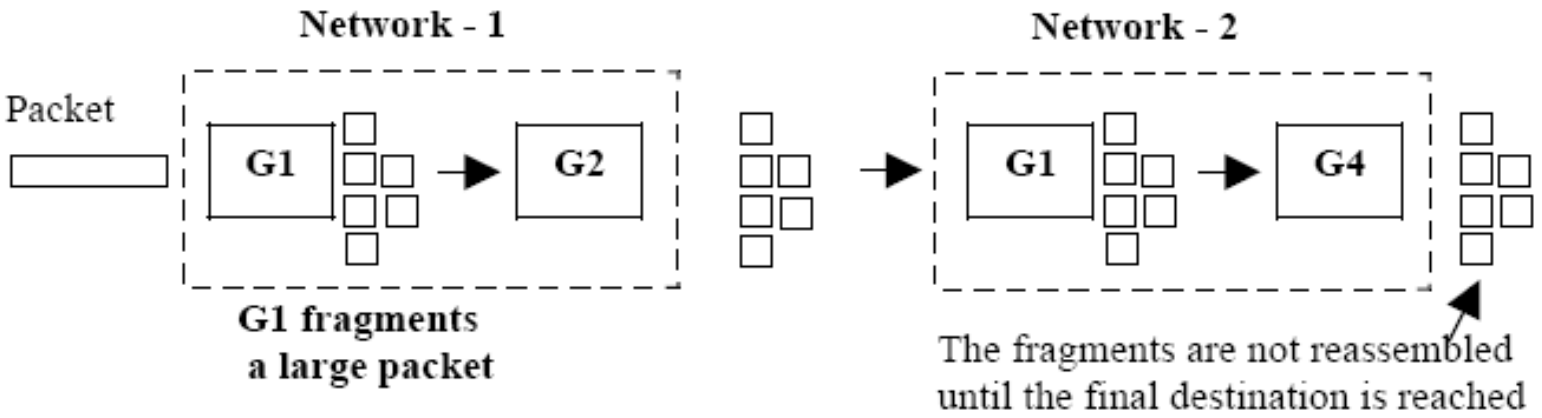
  (1) **Transparent fragmentation**

  (2) **Non-Transparent fragmentation**

- **Transparent fragmentation**
- When an over sized packet arrives at a gateway the gateway breaks it up into fragments
- Each fragment is addressed to the same exit gateway, where pieces are recombined
- In these way, passage through the small packet network has been made transparent


Network - 1
Network - 2
Packet
G1
G2
G1
G4
G1 fragments a large packet
G2 reassembles the fragments
G3 fragments again
G4 reassembles again

- **Non-transparent fragmentation**
- In this case, once a packet has been fragmented, each fragment is treated, as it were an original packet
- All fragments are passed through the exit gateway
- Recombination occurs only at destination host


Network - 1
Network - 2
Packet
G1
G2
G1
G4
G1 fragments
a large packet
The fragments are not reassembled
until the final destination is reached

- **Network Layer in the internet**
- At the network layer, internet can be viewed as a **collection of sub networks** (or) **Autonomous Systems**
- There are no real structures, but several major backbones exist. These are constructed from, high bandwidth lines and fast routers
- Attached to the backbones are regional networks and attached to regional network are LANs at many universities, companies etc..
- The glue that holds the internet together is network layer protocol, Internet Protocol [i.e. **IP**]

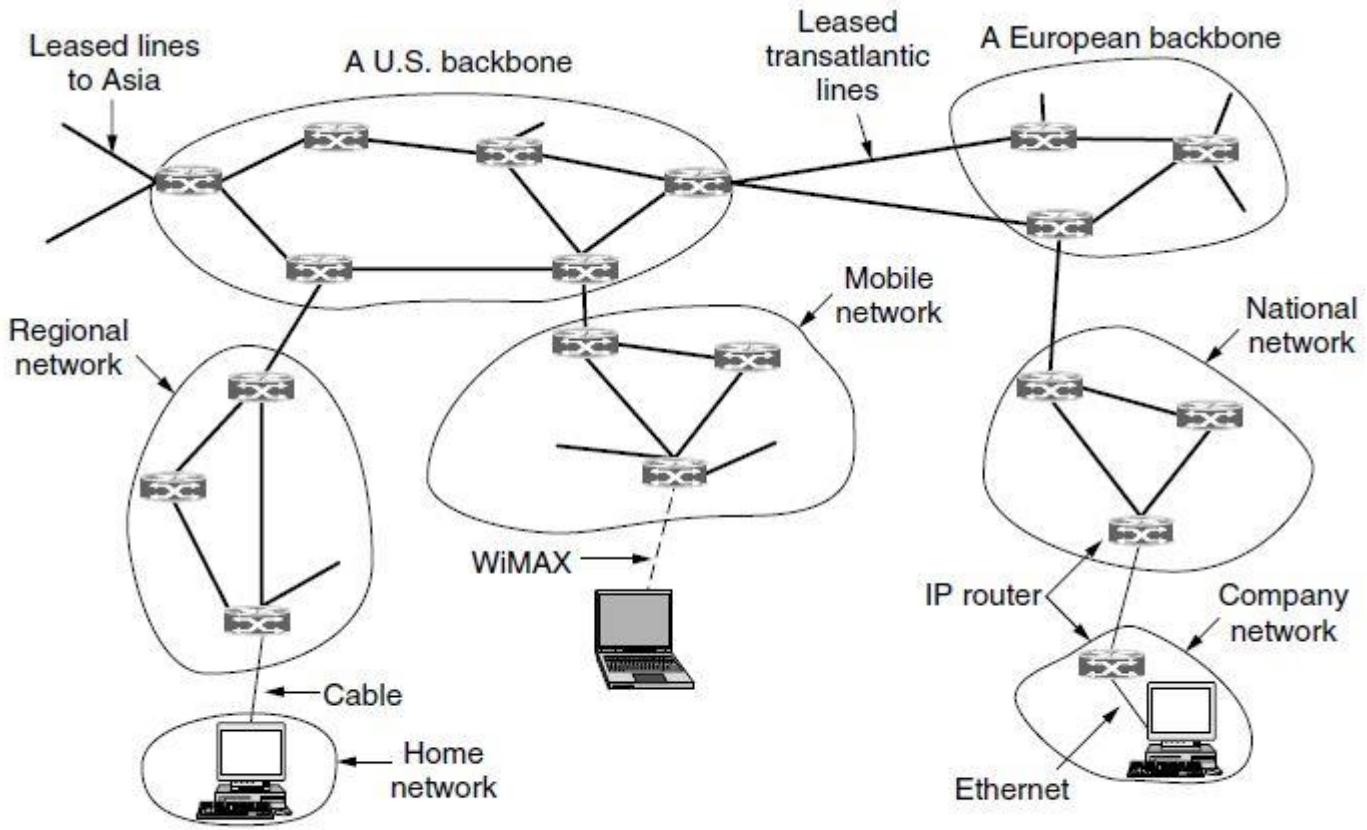
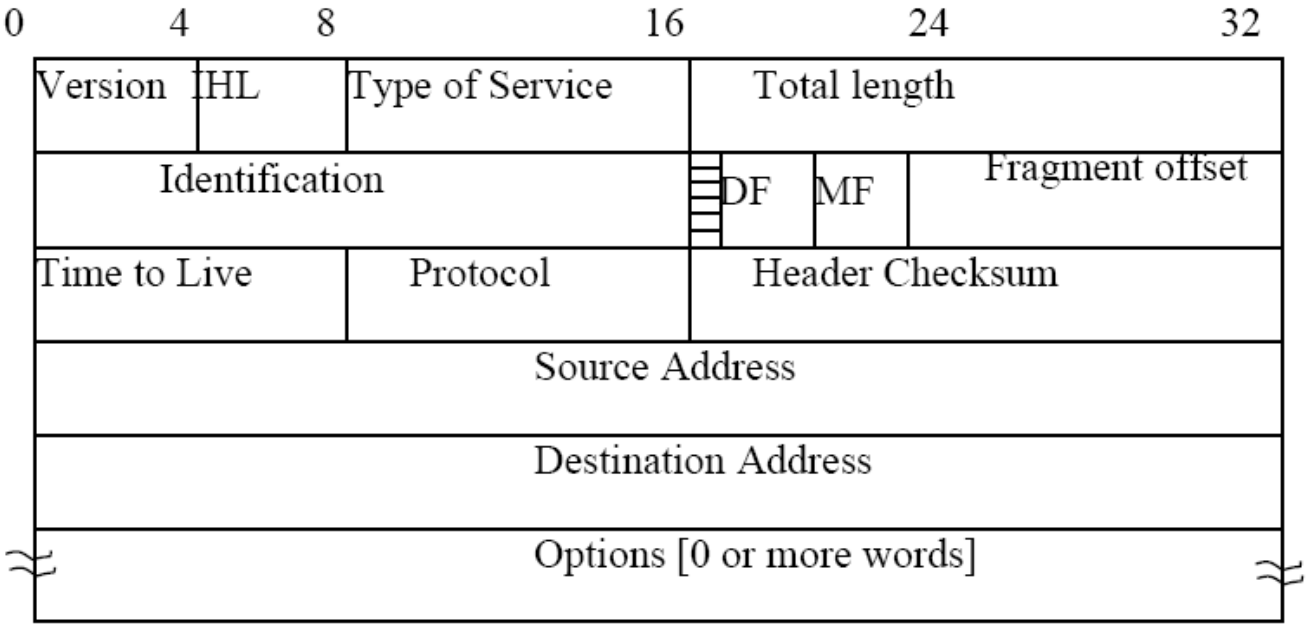


Figure 5-45. The Internet is an interconnected collection of many networks.

- **Internet Protocol [IPV4] and Addressing**
- **Internet Protocol [IPV4]:**
- IP Packet consists of a **header part** and **Text part**
- The header has a **20 byte fixed part** and a variable length **optional part**



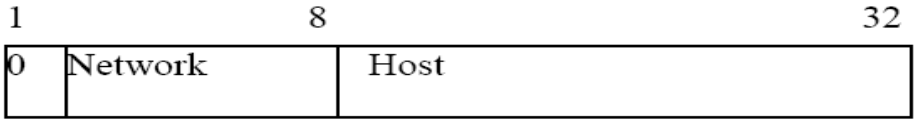
IP Header Format

- **Version field:** It keeps track of which version of the protocol the datagram belongs to
- **IHL:** It is provided to tell how long the header is in 32 bit words
- **Type of service:** Allows the host, to tell the subnet , what kind of service it wants
- Example:
- -> For **file transfer**, error free transmission is more important than fast
- transmission
- **Total Length:** It includes everything in the Packet -> both header and data. The maximum length is **65535** bytes
- **Identification Field:** It allows the destination host, to determine newly arrived fragment belongs to which datagram
- **DF:** It stands for **Don't Fragment**
- It is an order to the routers not to fragment the datagram, because the destination is incapable of putting the pieces back together again
- **MF:** It stands for **More fragments**
- All fragments except the last one, have this bit set

- **Fragment Offset:** It tells where in the current datagram this fragment belongs
- **Time to Live:** It is a counter, used to limit packet life times
- **Protocol field:** It tells which transport process, to give it to TCP is one possibility, but so are UDP and others
- **Header Checksum:** It verifies the header only.
- It is useful for detecting errors generated by bad memory words, **Source Address and Destination Address:** It indicate the network number and host Number
- **Option Field:** It was designed to allow subsequent versions of the protocol, to include Information not present in the original design

- **IP Addresses ,Class full and Special addressing**
- Every host and the router on the internet has an IP address which encodes its **network number** and **host number**
- All IP addresses are **32 bit** long and are used in the source address and destination address fields of IP packet
- Here **Five classes** of address formats are used [i.e. Class A, B, C, D, E]
- Network numbers are assigned by the **Network Information Centre** [NIC] to avoid conflicts
- Network address which are 32 bit numbers are usually written in **dotted decimal**

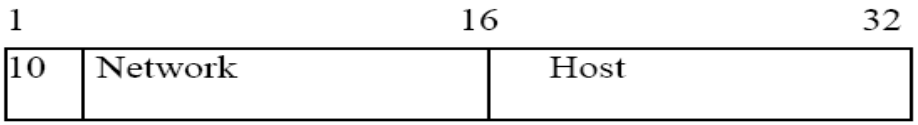
Class - A



Range of host address

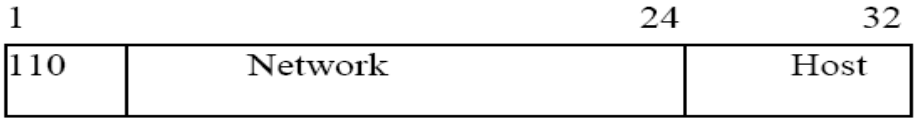
1.0.0.0 to 127.255.255.255

Class - B



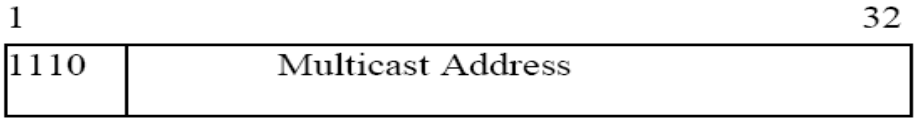
128.0.0.0 to 191.255.255.255
127.255.255.255

Class - C



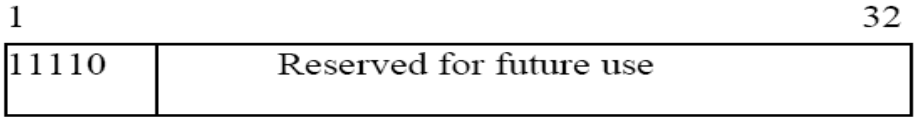
192.0.0.0 to 223.255.255.255
127.255.255.255

Class - D



224.0.0.0 to 239.255.255.255
127.255.255.255

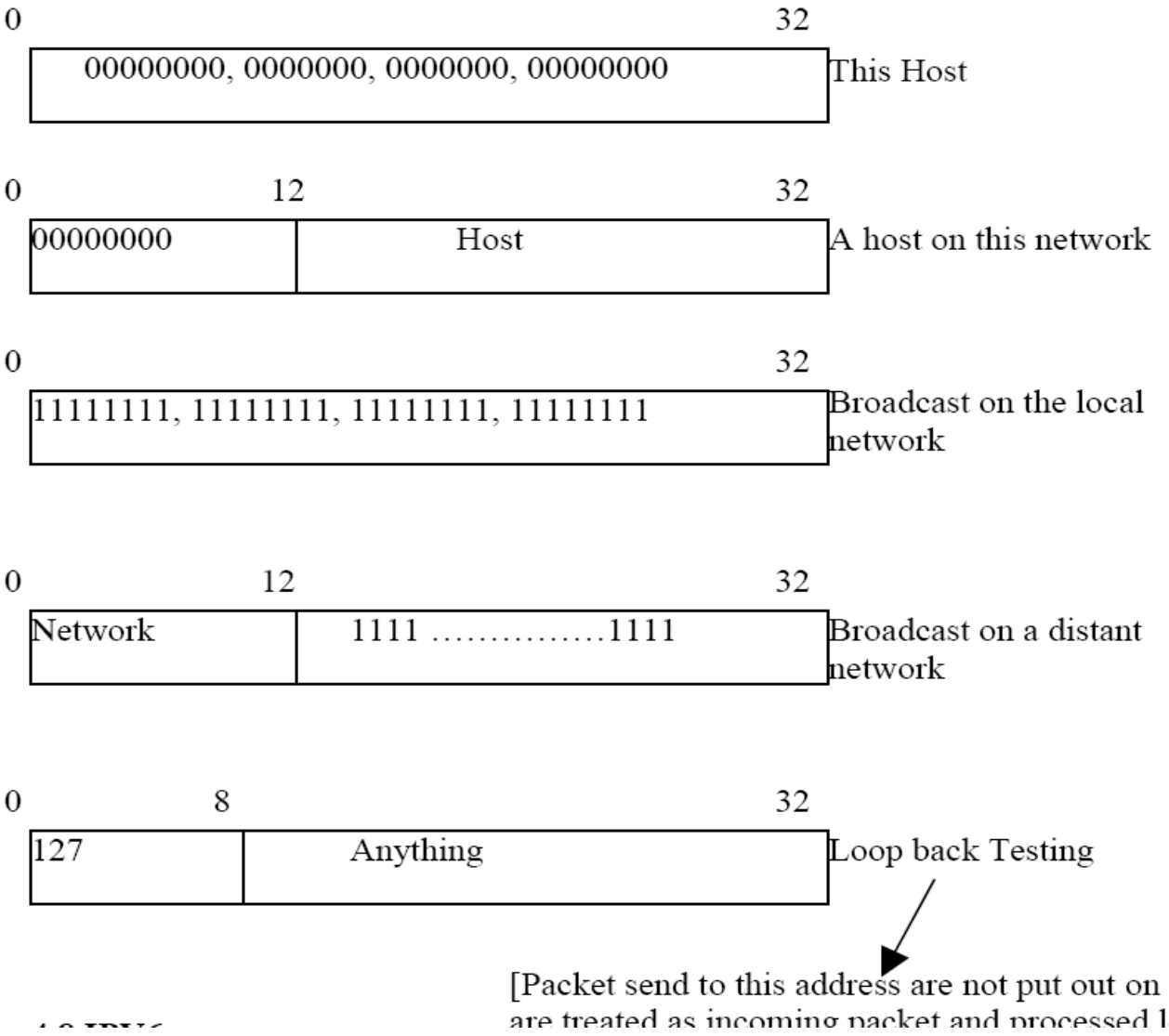
Class - E



240.0.0.0 to 247.255.255.255
127.255.255.255

- Network addresses, which are 32-bit numbers, are usually written in dotted decimal notation. In this format, each of the 4 bytes is written in decimal, from 0 to 255.
- The lowest IP address is 0.0.0.0 and the highest is 255.255.255.255
- The values 0 and 1 (all 1s) have special meanings
- 0 -> means **This Network** or **this host**
- 1 -> Used as a broadcast address to mean all hosts on the indicated network

Example:


0
32
00000000, 0000000, 0000000, 00000000
This Host
0
12
32
00000000
Host
A host on this network
0
32
11111111, 11111111, 11111111, 11111111
Broadcast on the local network
0
12
32
Network
1111 ……1111
Broadcast on a distant network
0
8
32
127
Anything
Loop back Testing
[Packet send to this address are not put out on to the wire they are treated as incoming packet and processed locally]

- Sub network or subnets:
- It is a logically visible subdivision of an ip network.
- Subnet ting is dividing the network into two or more networks is called subnet ting.
- Benefit of Subnets:

- Reduces the network traffic.
- Security
- Performance
- Troubleshooting - it is easier to find a problem in a smaller network than a large one.

subnetting(cont..)

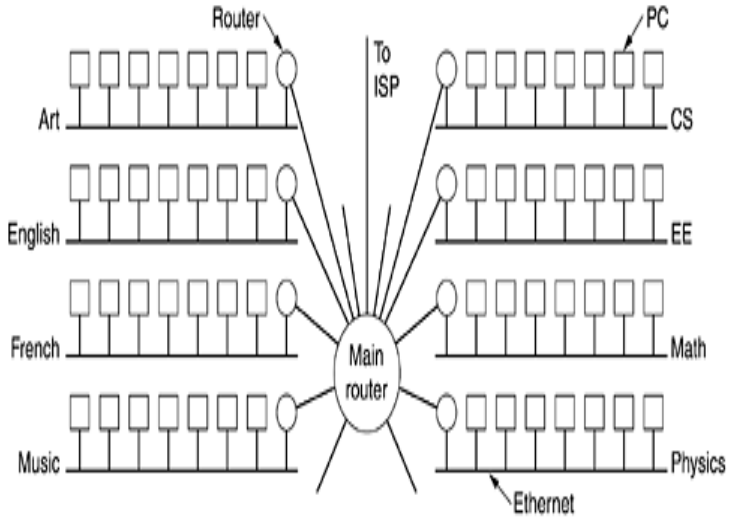
- all the hosts in a network must have the same network number. This is the property of IP addressing it can cause problems when networks size increase.
- For example, consider a university that started out with one class B network address used by the Computer Science Dept.
- A year later, the Electrical Engineering Dept. wanted to get on the Internet, so they bought a repeater to extend the CS Ethernet to their building.
- As time went on, many other departments acquired computers and the limit of four repeaters per Ethernet was quickly reached.

subnetting(cont..)

- If an organization size increasing Getting a second network address would be hard to do since network addresses are scarce and the university already had enough addresses for over 60,000 hosts.
- The solution is to allow a network to be split into several parts for internal use but still act like a single network to the outside world.
- A typical campus network nowadays might look like that of Fig. 5-57, with a main router connected to an ISP or regional network and numerous Ethernets spread around campus in different departments

subnetting(cont..)

Figure 5-57. A campus network consisting of LANs for various departments.



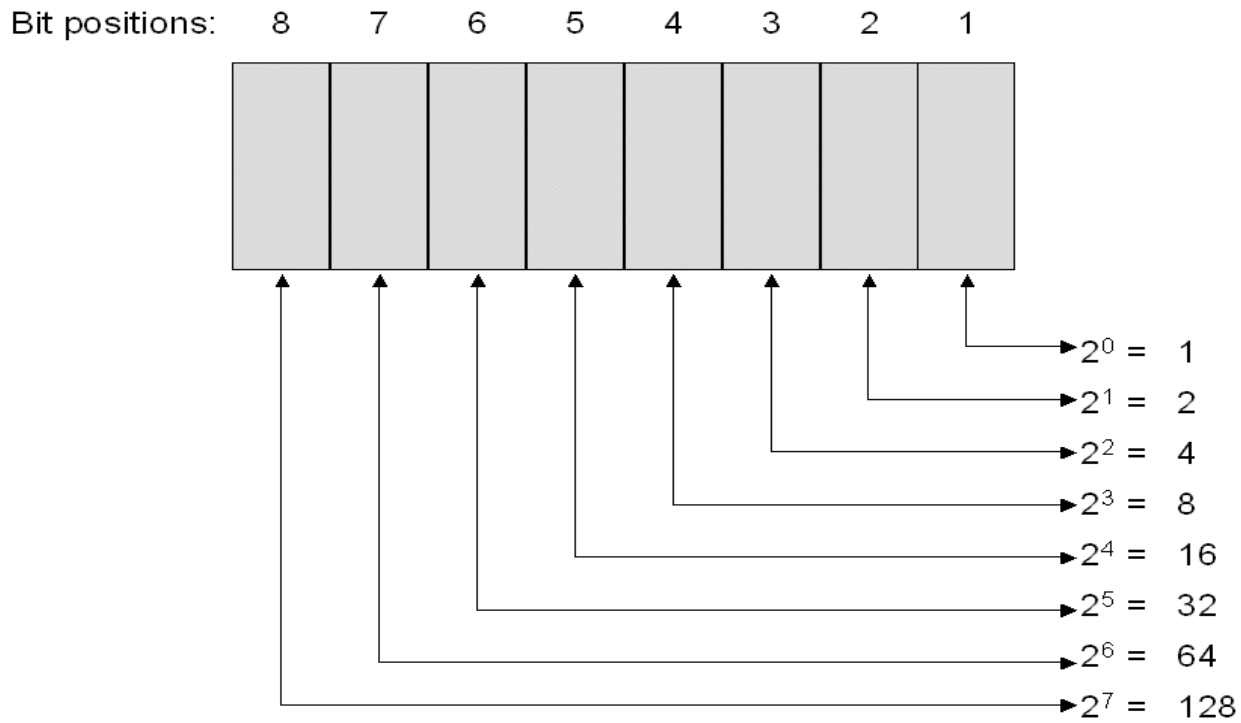
- In the Internet literature, the parts of the network (in this case, Ethernets) are called subnets.

subnetting(cont..)

- a different scheme was invented. Basically, instead of having a single class B address with 14 bits for the network number and 16 bits for the host number, some bits are taken away from the host number to create a subnet number.
- For example, if the university has 35 departments, it could use a 6-bit subnet number and a 10-bit host number, allowing for up to 64 Ethernets, each with a maximum of 1022 hosts
- To implement subnetting, the main router needs a subnet mask

subnetting(cont..)

- An IP address has two components, the network address and the host address
- Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>).
- A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address
- Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s.
- Within a given network, two host addresses are reserved for special purpose. The "0" address is assigned a network address and "255" is assigned to a broadcast address



	128	64	32	16	8	4	2	1
8 bit binary digit	1	0	1	1	0	0	0	1
	128 + 32 + 16 + 1 = 177							

1 Translating Binary to Decimal

Both IP addresses and subnet masks are composed of 32 bits divided into 4 octets of 8 bits each. Here is how a single octet translates from binary to decimal. Consider an octet of all ones: 11111111.

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      1     1     1    1    1    1    1
128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 255
```

Here's another: 10111001

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      0     1     1    1    0    0    1
128 +  0 + 32  +16 + 8 + 0 + 0 + 1 = 185
```

and 00000000

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 0      0     0     0    0    0    0    0
 0   +  0 +  0 +  0 + 0 + 0 + 0 + 0 = 0
```

2 Converting Decimal to Binary

Converting decimal to binary is similar. Consider 175:

```
128    64    32    16    8    4    2    1
---    --    --    --    -    -    -    -
 1      0     1     0    1    1    1    1
128 +  0 + 32 +  0 + 8 + 4 + 2 + 1 = 175
```

subnetting(cont..)

- The default subnet mask for
- class A is 255.0.0.0
- class B is 255.255.0.0
- class C is 255.255.255.0

Bits Available for Creating Subnets

Address Class	Host Bits	Bits Available for Subnet
A	24	22
B	16	14
C	8	6

Calculating Subnets

There are two simple formulas to calculate these numbers:

Number of hosts per subnet = (2) - 2

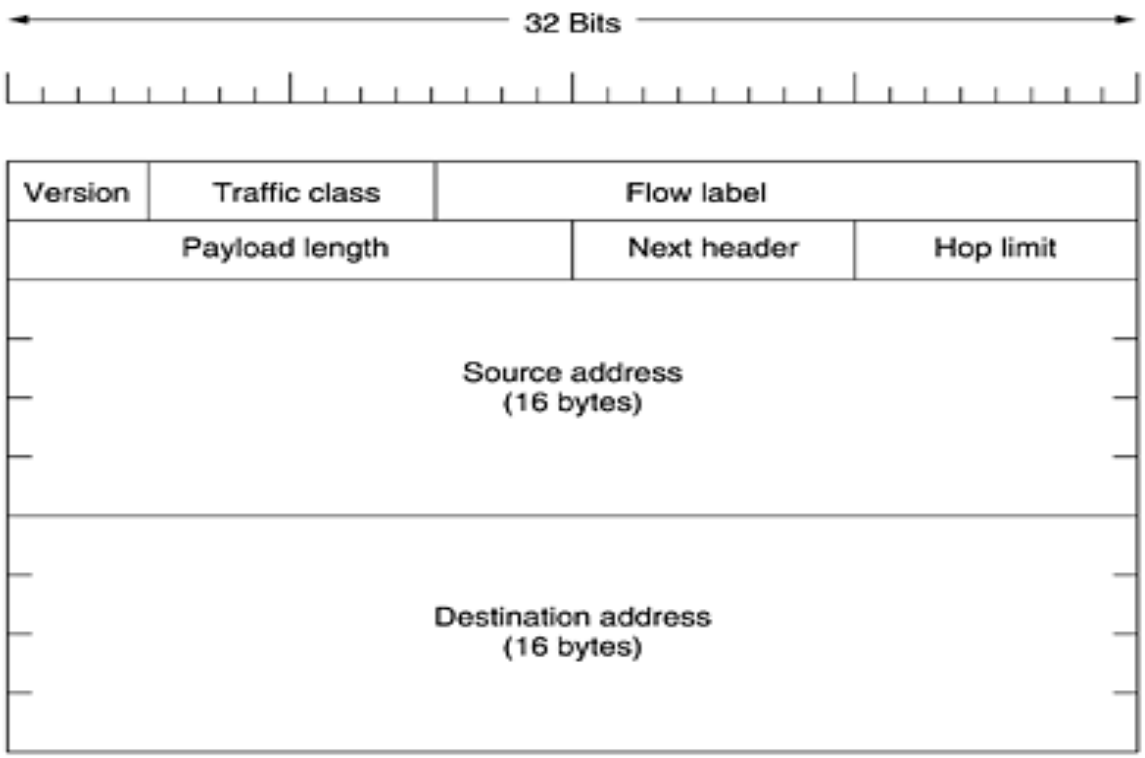
Tink –pair –share (group activity)

- Example : A network on the internet has subnet mask of 255.255.240.0 . What is the max number of hosts it can handle?

- **IPv6 (Internet Protocol version 6)** is the latest revision of the Internet Protocol (IP), the primary communications protocol upon which the entire Internet is built.
- IPv6 is intended to replace the older IPv4,
- IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 running out of addresses

- Each device on the Internet, such as a computer or mobile telephone, must be assigned an IP address in order to communicate with other devices.
- With the ever-increasing number of new devices being connected to the Internet, there is a need for more addresses than IPv4 can accommodate.
- IPv6 uses 128-bit addresses, allowing for 2^{128}, or approximately - 340,282,366,920,938,463,463,374,607,431,768,211,456 3.4×10^{38} addresses — more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses.

- **Main Features:**
- IPV6 has **larger address** than IPV4. They are **16 bytes long** which provide an effectively unlimited supply of Internet address
- IPV6 is the simplification of the header. It contains only **7 fields**. This allows routers to **process packets faster** and thus **improve throughput**
- This process **speeds up packet processing time**


32 Bits
Version
Traffic class
Flow label
Payload length
Next header
Hop limit
Source address
(16 bytes)
Destination address
(16 bytes)

- **Version:** The Version field is always 6 for IPv6 (and 4 for IPv4).,
- **Traffic class :** (8-bits): These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN)..

  Flow Label : Used identify packets that are in flow in between the source and destination or which should have a same routing behavior at intermediate points.
- Each flow is designated by the **source address, destination address and flow numbers**
- **Payload Length Field**: This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated;
- The Payload length field tells how many bytes follow the 40-byte header
- **Next header field**: It tells the type of the next header (eg: TCP,UDP or extension headers)
- **Hop limit:** It is same as time to live field in IPV4, [i.e. a field that is decremented on each hop]
- **Source and destination Address:** IPV6 uses a fixed length 16 byte address

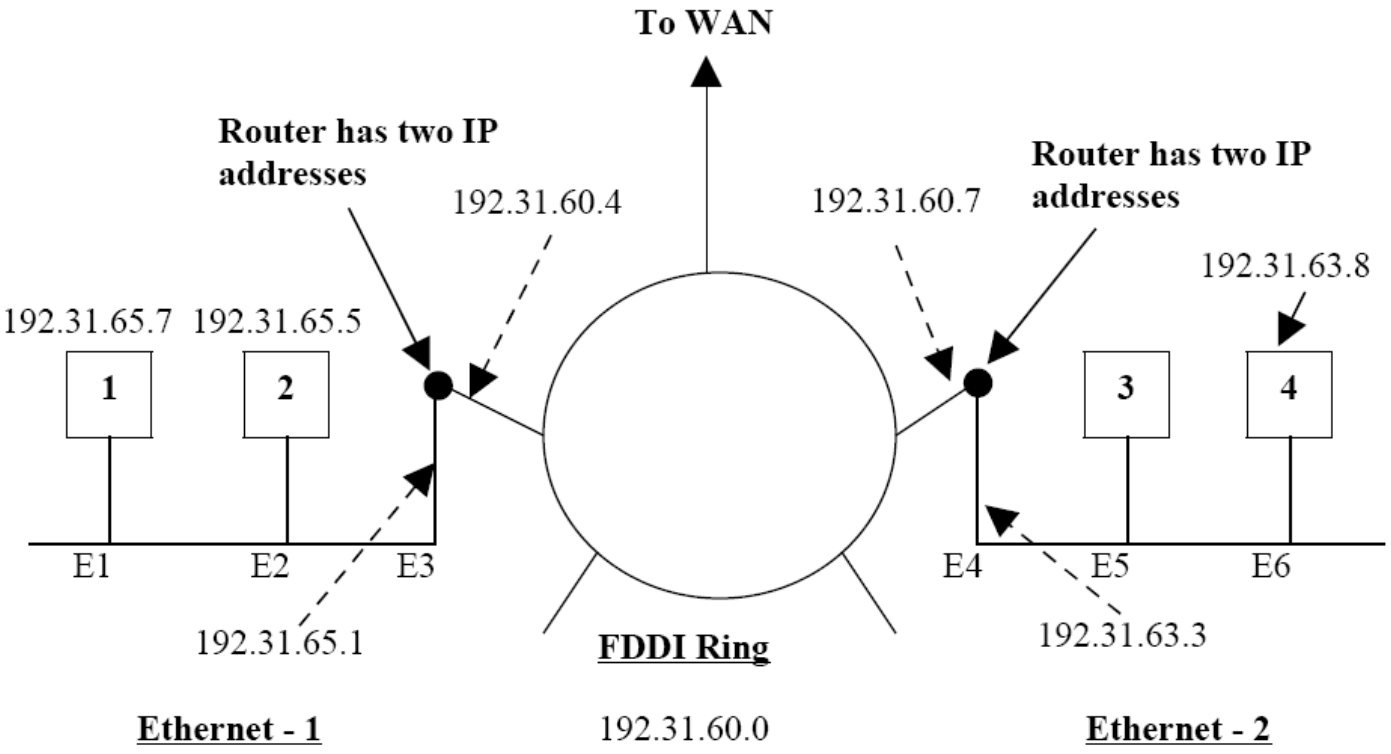
- **Internet Control Protocols:**
- **ICMP [Internet Control Message Protocol]**
- Used to **test** the internet
- Routers continuously monitor the operation of the internet
- When something **unexpected occurs**, the event is reported by ICMP
- Different types of ICMP messages are defined and each ICMP message type is encapsulated in an IP packet

Some of the message types are listed below:

Message Type	Description
Destination Unreachable	Packet could not be delivered
Time exceeded	Time to live field hit zero
Parameter problem	Invalid header field
Source Quench	Choke packet
Echo request	Ask a machine if it is alive
Echo Reply	Yes I am alive
Time stamp request	Same as Echo, but with time stamp
Time stamp reply	Same as Echo, but with time stamp

- **A**ddress **R**esolution **P**rotocol [**ARP**]
- Every host on the internet has one or more IP addresses
- For sending a packet this addresses are not used because the data link layer hardware, does not understand IP
- Nowadays, most hosts at companies and universities are attached to a LAN by an interface board that only understands LAN addresses.
- Manufactures of Ethernet boards, request a block of addresses from a central authority to ensure no two boards have same address
- Ethernet boards sends and receive frames based on **48 – bit Ethernet addresses** [They know nothing at about 32 – bit IP addresses]
- **How do IP addresses get mapped onto data link layer addresses [i.e. Ethernet] ?**
- Example:
- In the below fig we have **two Ethernet** one with IP address **192.31.65.0** and one with **192.31.63.0**
- These two are connected via **FDDI** [Fiber Distributed data Interface] ring with IP address **192.31.60.0**, each machine on FDDI ring has an FDDI address, labeled through F1 to F3
- Each machine on Ethernet has **Unique Ethernet address**, [E1 through E6

147


To WAN
Router has two IP addresses
192.31.60.4
192.31.60.7
Router has two IP addresses
192.31.63.8
192.31.65.7
192.31.65.5
1
2
3
4
E1
E2
E3
E4
E5
E6
192.31.65.1
192.31.63.3
FDDI Ring
Ethernet - 1
192.31.60.0
Ethernet - 2

- **How user on host-1 sends a packet to a user on host-2?**
- Let us start out by seeing how a user on host 1 sends a packet to a user on host 2.
- Let us assume the sender knows the name of the intended receiver, possibly something like mary@eagle.cs.uni.edu.
- The first step is to find the IP address for host 2, known as eagle.cs.uni.edu. This lookup is performed by the Domain Name System.
- For the moment, we will just assume that DNS returns the IP address for host 2 (192.31.65.5).
- The upper layer software on host-1 **builds a packet** with destination IP address and gives it to **IP software** to transmit
- The IP software checks whether the destination is on its own network
- But IP software, **needs a way** to find the destination Ethernet address
- **1st Solution:**
- Using **Configuration File,** in the system maps IP addresses onto Ethernet addresses, In case of thousands of machines, updating these files is an error prone, time consuming job
- **2nd Solution:**
- Host-1 output a **broadcast packet** on to Ethernet asking: **Who owns IP address 192.31.65.5**?
- Every machine checks its IP addresses, host-2 alone respond with Ethernet address [E2]
- Thus host-1 learns that IP address 192.31.65.5 is on host with Ethernet address [E2]
- The protocol for asking this question and getting reply is called **A**ddress **R**esolution **P**rotocol [**ARP**]

- **R**everse **A**ddress **R**esolution **P**rotocol [**RARP**]
- Given an Ethernet address, what is the corresponding IP address? This problem occurs when booting a Diskless work station
- The solution is to use the **RARP**
- The RARP allow a newly booted workstation to broadcast its Ethernet address and say **"My 48 – bit Ethernet address is 14.04.05.18.01.25, Does any one out there know my IP address?"**
- The **RARP Server**, sees this request, looks up the Ethernet address in its Configuration files and sends back the corresponding IP address
- **Drawbacks:**
- RARP uses destination address of all 1's [i.e. limited broadcasting] to reach RARP server. However such a broadcast are not forwarded by routers, so RARP server is needed on each network
- To overcome this drawback, use alternative Bootstrap protocol called **BOOTP**
- BOOTP uses UDP messages, which forwarded over routers
- It provides **additional information**, to diskless work station such as
- -> Include IP address of File server holding memory image
- -> IP address of default routers
- -> Subnet mask to use

- A serious problem with BOOTP is that it requires manual configuration of tables mapping IP address to Ethernet address.
- When a new host is added to a LAN, it cannot use BOOTP until an administrator has assigned it an IP address and entered its (Ethernet address, IP address) into the BOOTP configuration tables by hand.
- To eliminate this error-prone step, BOOTP was extended and given a new name: DHCP (Dynamic Host Configuration Protocol).
- DHCP allows both manual IP address assignment and automatic assignment.

- To find its IP address, a newly-booted machine broadcasts a DHCP DISCOVER packet.
- The DHCP relay agent on its LAN intercepts all DHCP broadcasts.
- When it finds a DHCP DISCOVER packet, it sends the packet as a unicast packet to the DHCP server, possibly on a distant network.
- The only piece of information the relay agent needs is the IP address of the DHCP server.

Figure 5-63. Operation of DHCP.