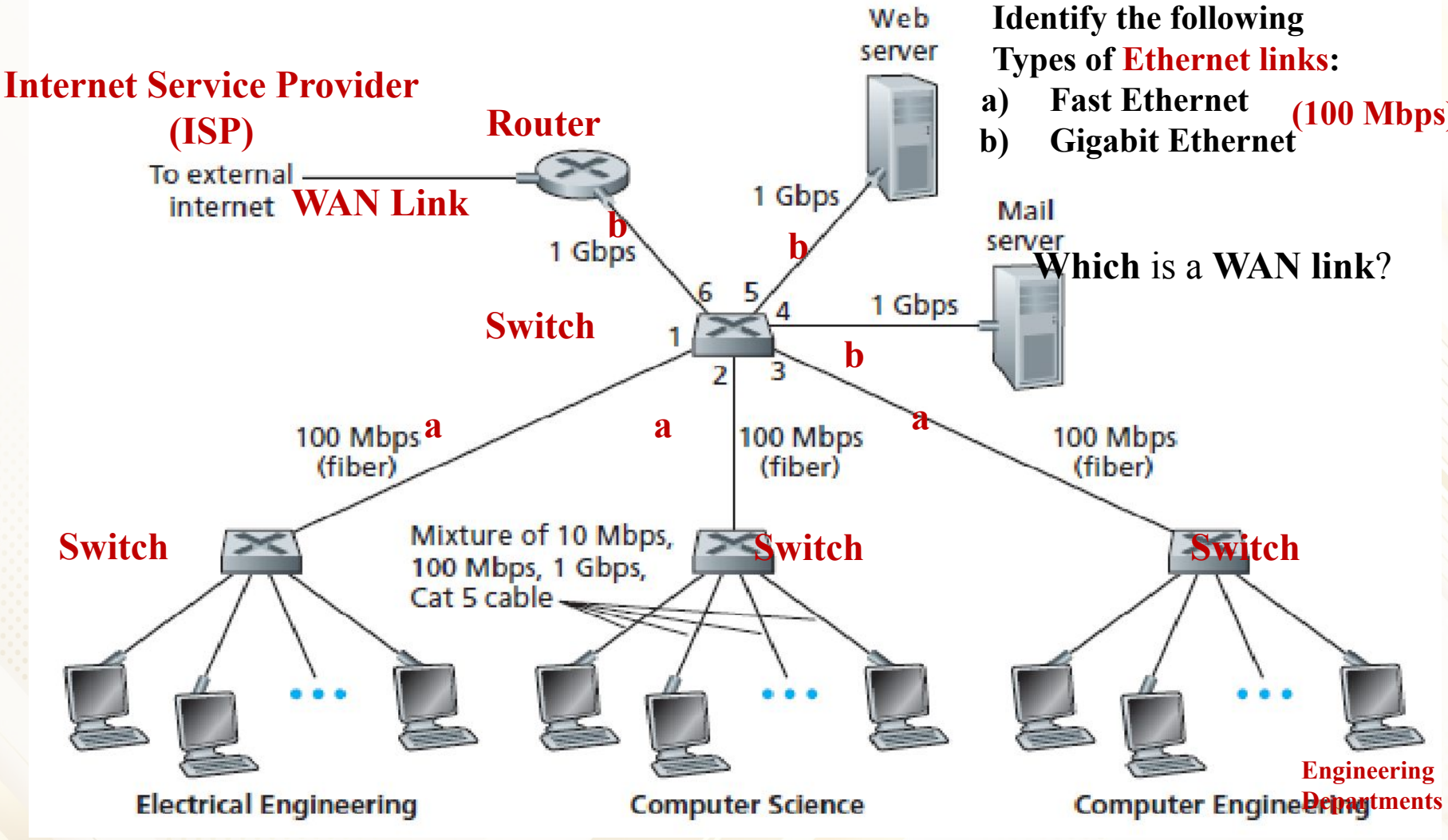
RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Computer Networks

UNIT-4

Introduction to IP

An Example Institutional Network



Identify the following Types of Ethernet links:

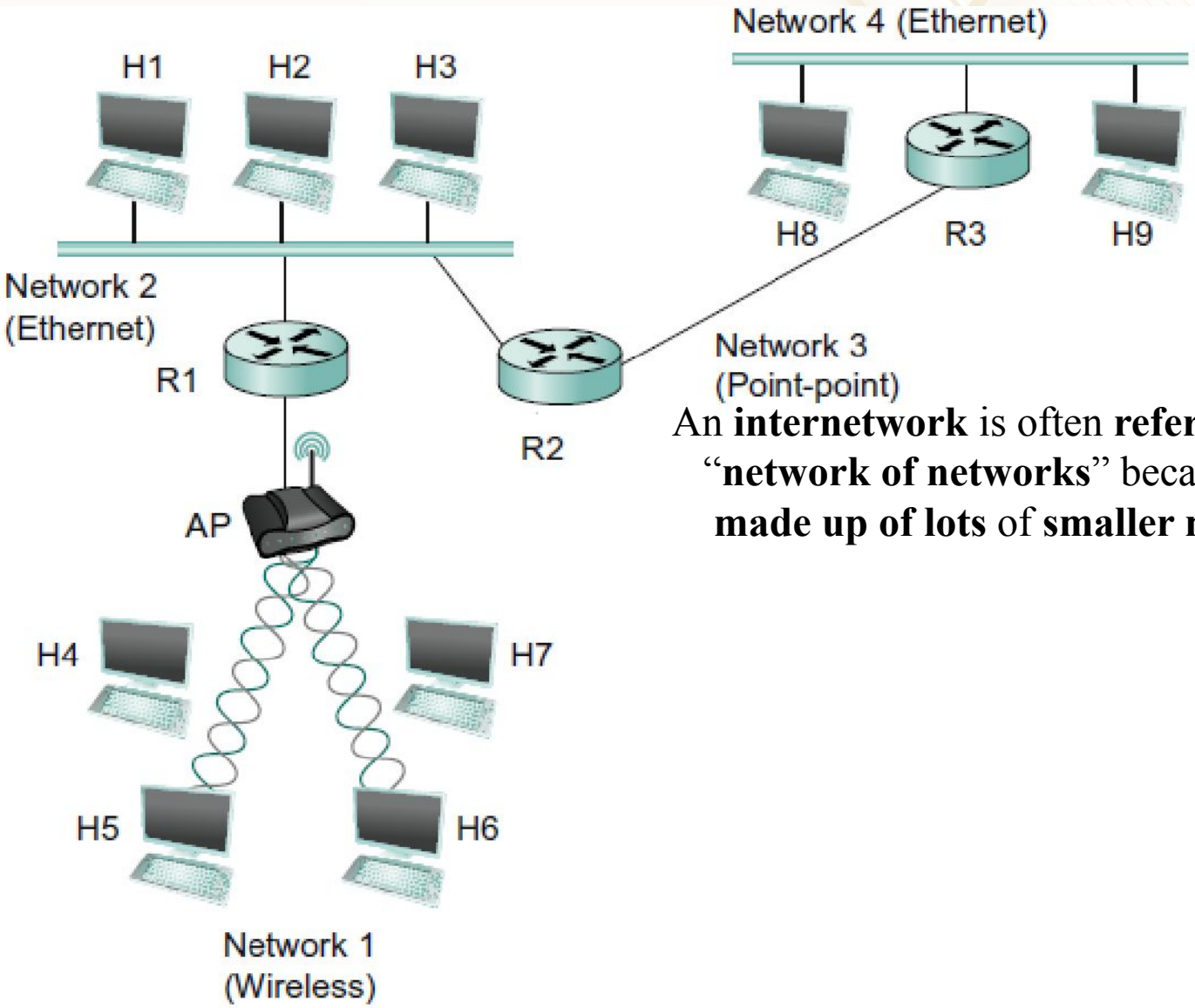
a) **Fast Ethernet** (100 Mbps)

b) **Gigabit Ethernet**

Which is a **WAN link**?

- **Identify** the **network components** in the **picture**

What is an Internetwork?



Here, let us **restrict** our **discussion** to **internet**, the **principles learnt** will be **extended** to **Internet** later.

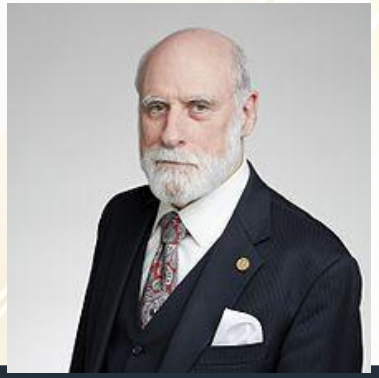
An **internetwork** is often **referred** to as a "**network of networks**" because it is **made up of lots** of **smaller networks**

Internet Protocol (IP)

They received Turing Award in 2004 !!!

Inventors

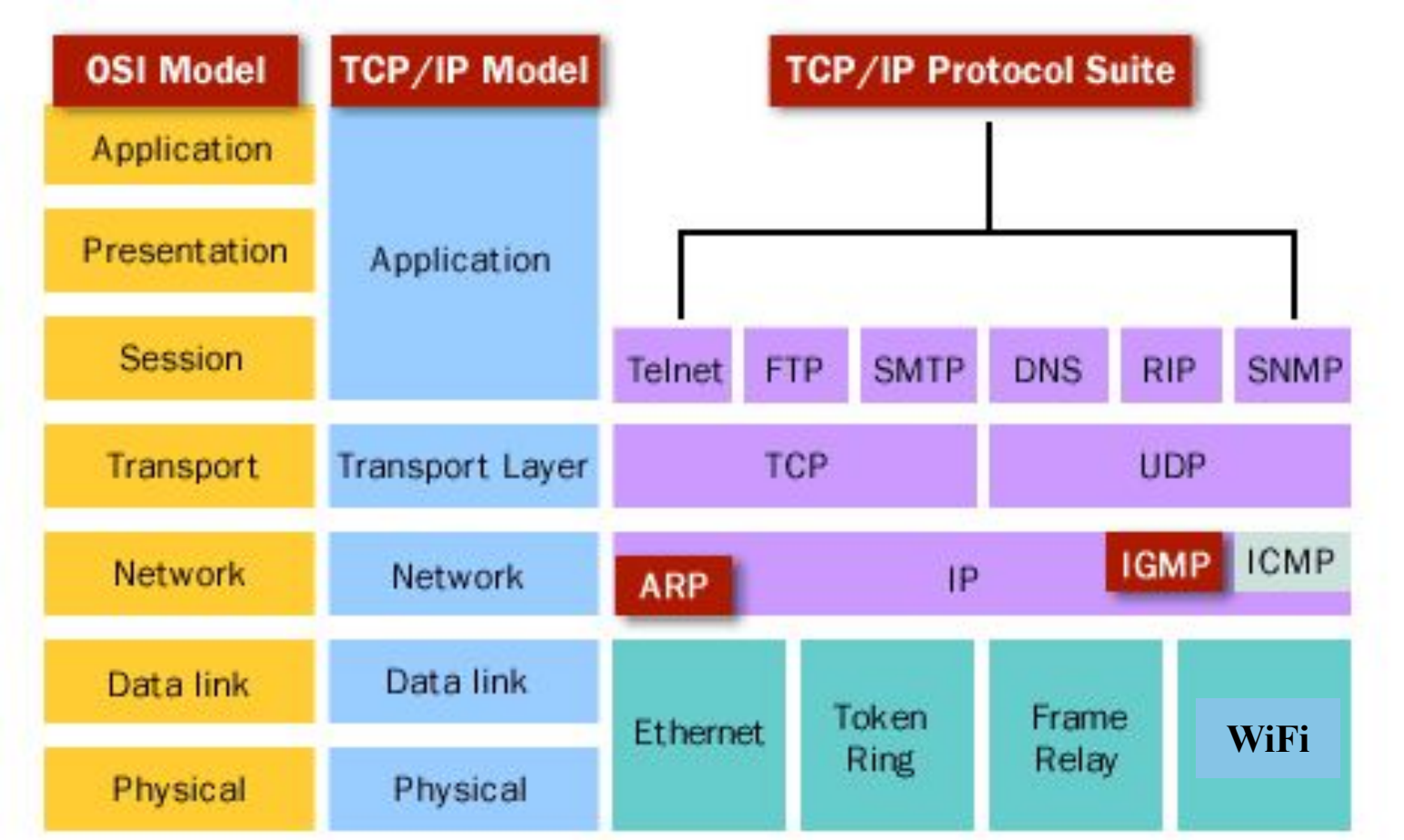
Robert Elliott Kahn
American
Bell Labs
MIT
DARPA



Vinton Gray Cerf
American
Stanford University
DARPA
MCI

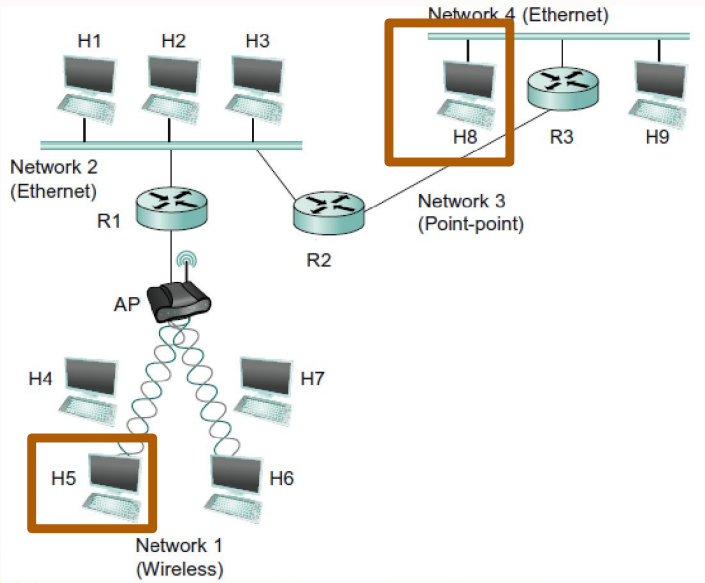
IP was designed in 1970s and commissioned in 1983

TCP/IP Protocols

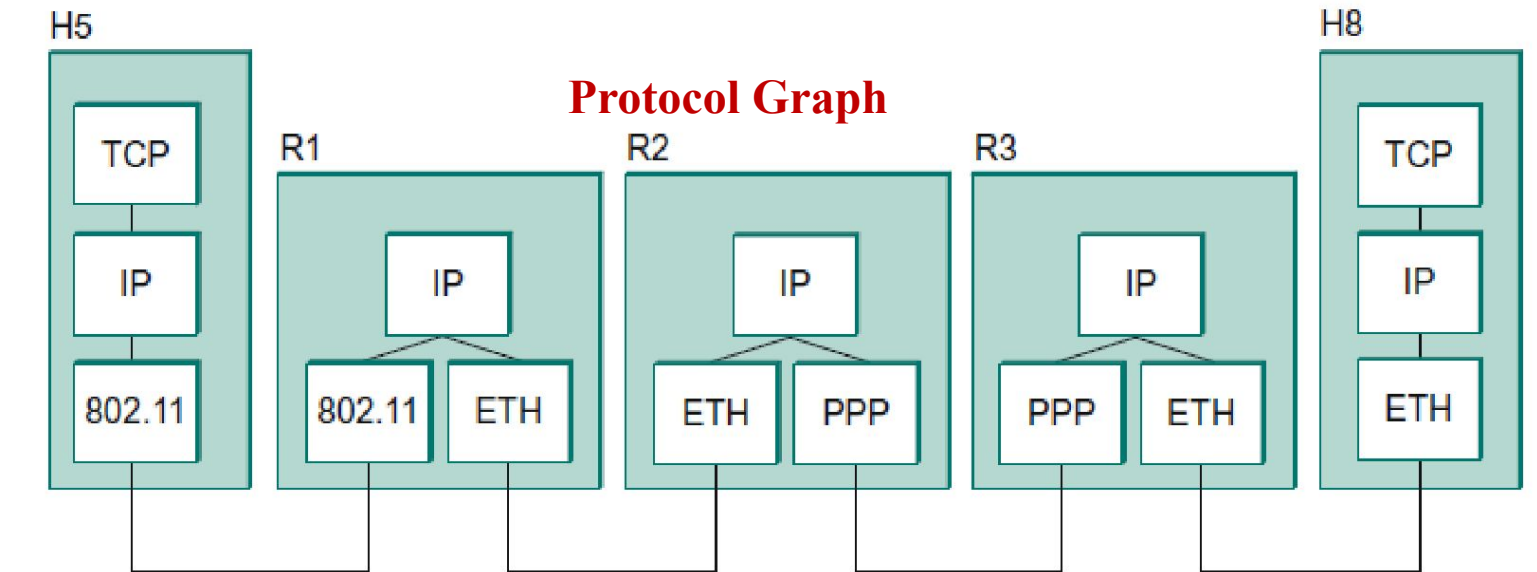


- Always remember which OSI layer each protocol that you study belongs, you need to have the overall context

Protocol Graph of IP Running



- IP **runs** on **all the nodes** (**both hosts and routers**) in a collection of networks
  - This is the **reason,** an **IP network diagram** also **shows** the **hosts** on the network too
  - But. Bridges do not understand IP protocol
- IP **defines** the **infrastructure** that allows these **nodes** and **networks** to **function** as a **single logical internetwork**
- Picture below shows how hosts **H5** and **H8** are **logically connected** by the **internet**, including the **protocols** running on **each node**.



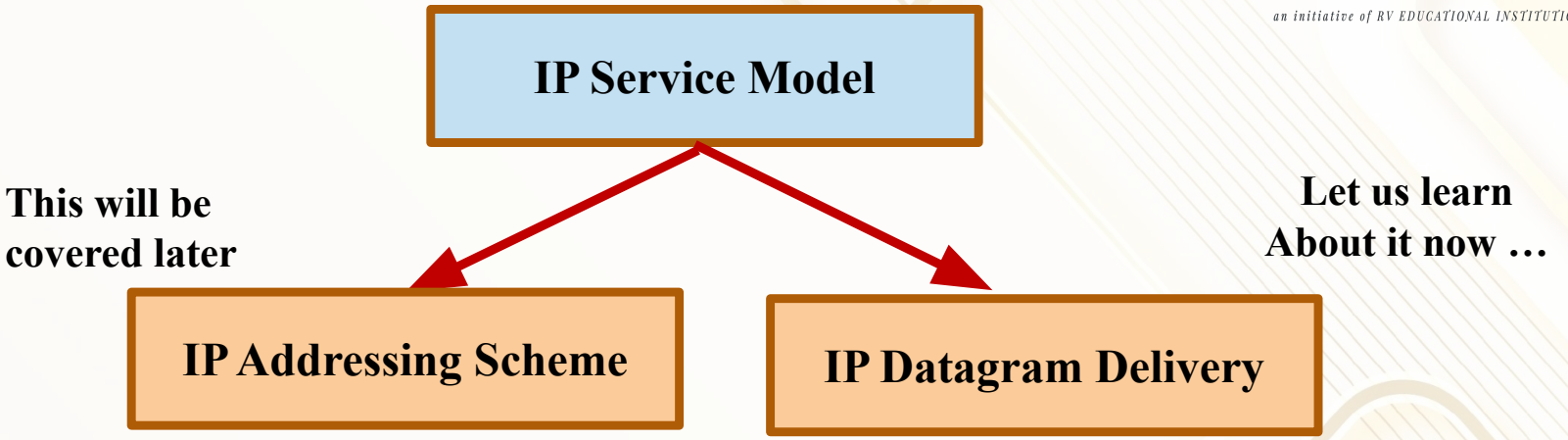
An Introduction: Internet Protocol (IP)

- The **Internet Protocol** is the key **protocol** used today to build scalable, **heterogeneous internetworks**.
- It was originally known as the **Kahn-Cerf protocol** after its **inventors**
- Note that **higher-level protocols**, such as **Level 4** protocols (**TCP** and **UDP**), typically run on top of **IP** (**Level 3**) **on** the **hosts**
- **IP** is a **scalable internetworking protocol** which is the **most popular** and **widely** used to **implement** the **Internet**
- Since its invention in 1970s, many new protocols and technologies have come up and all of them were found to be working seamlessly without any changes to IP protocol
  - It shows how **futuristic** these **inventors** of IP protocol **were**!!!

IP Service Model

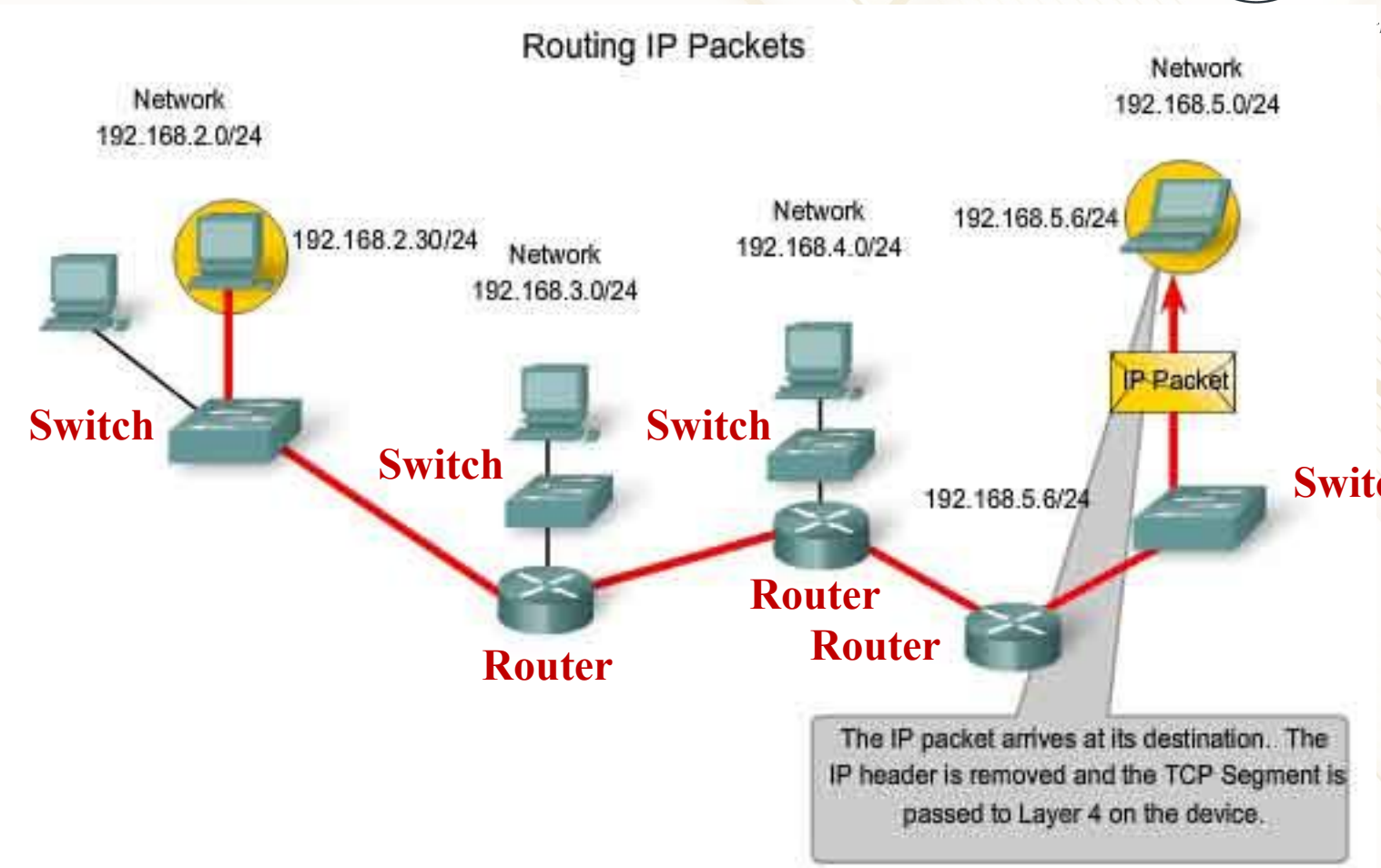
- **Service model** of a **system** is defining what the **intended system** would **deliver** to the **end user**. What **it guarantees** and what **it does not!**!!
- The main intent of IP was to provide **host-to-host services**.
- The main concern in defining a service model for an internetwork is that we can provide a host-to-host service only if this service can somehow be provided over each of the underlying physical networks.
- For example, it would be no good deciding that our internetwork service model was going to provide guaranteed delivery of every packet in 1 ms or less if there were underlying network technologies that could arbitrarily delay packets.
- The philosophy used in defining the IP service model, therefore, was to make it undemanding enough that just about any network technology that might turn up in an internetwork would be able to provide the necessary service that this IP service model guarantees

Two Parts of IP Service Model



- **IP addressing scheme,** which provides a way to identify all hosts in the internetwork,
- **IP Datagram** (**connectionless**) model of **data delivery**.
- This service model is sometimes called **best effort** because, although IP makes every effort to deliver datagrams, it makes no guarantees.
- Let us now look first at the **data delivery model**

IP Datagram Delivery



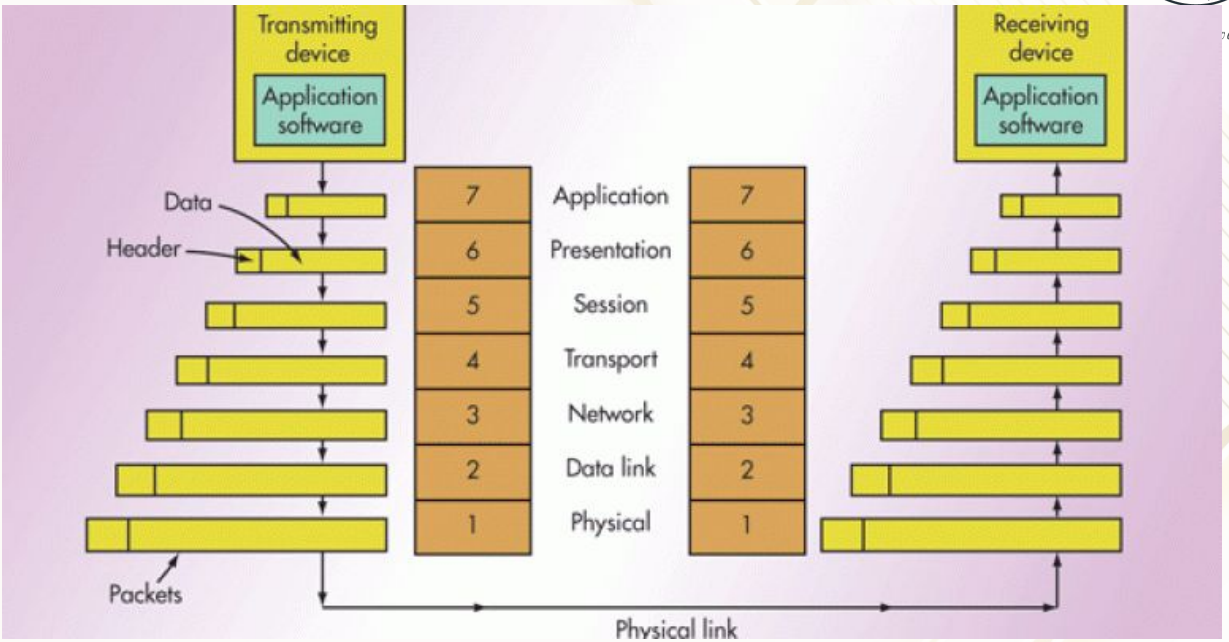
- IP packets travel through Routers from one network to the other
- They get into L2 and L1 to get transmitted through routers

IP Datagram Delivery Model

- The **IP datagram** is **fundamental** to the **Internet Protocol**
- **Datagram** is a type of packet that happens to be sent in a **connectionless** manner over a network.
- **Every datagram** carries **enough information** to let the network forward the packet to its correct destination.
- There is no need for any advance setup mechanism to tell the network what to do when the packet arrives.
- IP packet is just sent and the network makes its best effort to get it to the desired destination.
- The "**best-effort**" part means that if something goes wrong and the packet gets lost, corrupted, mis-delivered, or in any way fails to reach its intended destination, the network does nothing
  - It made its best effort, and that is all it has to do.
- It does not make any attempt to recover from the failure. This is sometimes called an unreliable service.

Quiz 1: Purpose of Headers

RV UNIVERSITY
Go, change the world
e of RV EDUCATIONAL INSTITUTIONS



- **Purpose** of **headers** in a packet: **Header** of a **Level (Ln)** is **processed** by:

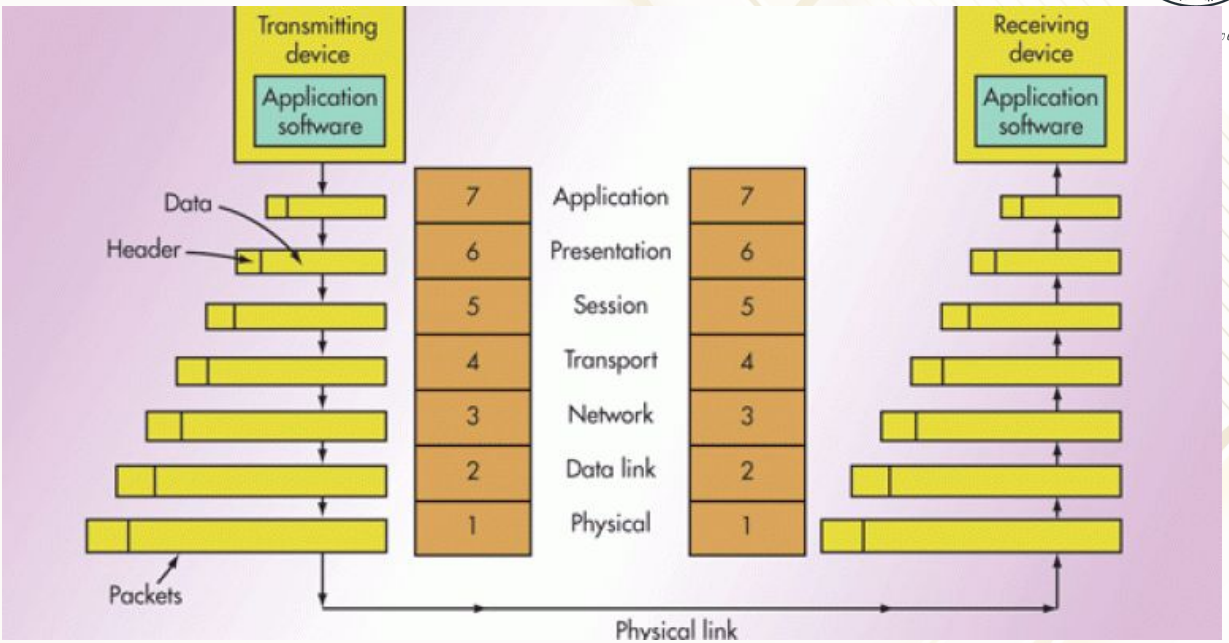
A. Level: Ln
B. Level: Ln+1
C. Level: Ln-1
D. None

ANS:

Option A. The information in the header of a level is to share any specific information that the peer at the same level on the receiving side should know or handle.

Quiz 2: Purpose of Data or Payload

RV UNIVERSITY
Go, change the world
...e of RV EDUCATIONAL INSTITUTIONS



- **Purpose** of **Payload** in a packet: **Payload** of a **Level (Ln)** is **processed** by:

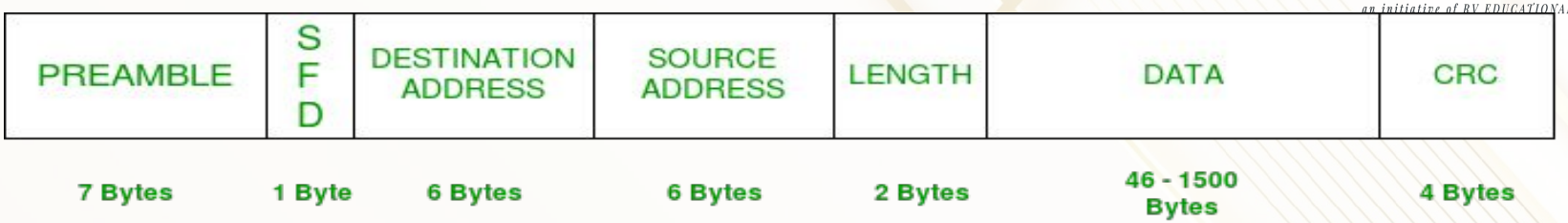
A. Level: Ln
B. Level: Ln+1
C. Level: Ln-1
D. None

ANS:

Option B. The information in the Payload is meant for the Layer(s) above the packet at one level which is carrying it to the receiving end. Normally the payload is not processed by the layer carrying it. The payload is stripped by a particular level and passed on to the next higher level without any changes to it, at the receiving end.

Purpose of Each Ethernet Header Elements

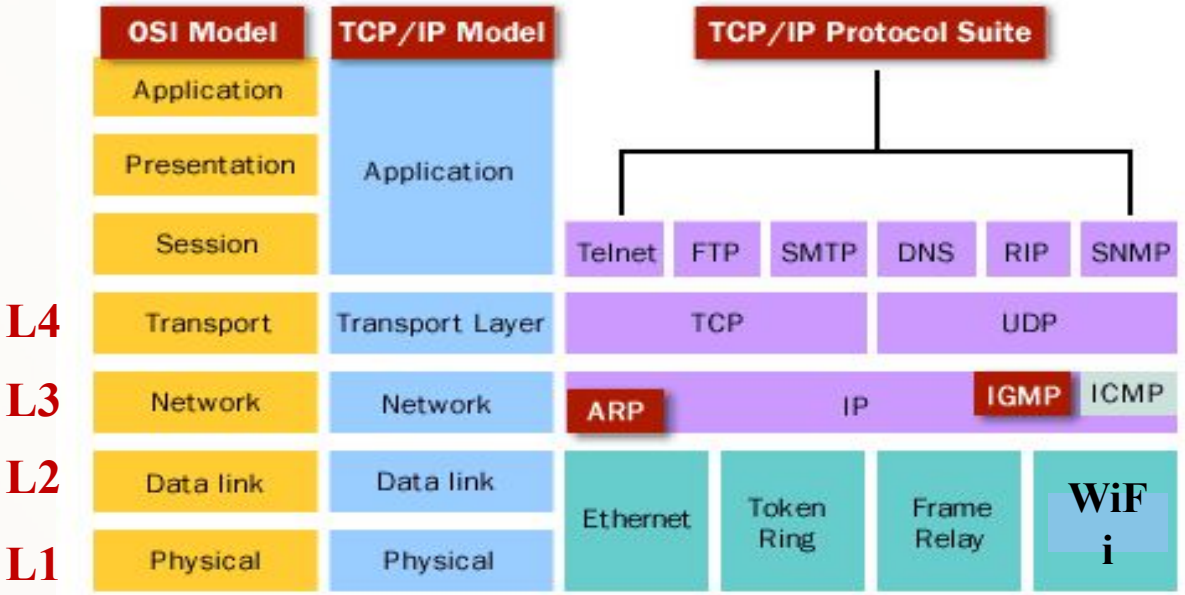
RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS



- Which **Level** of OSI **processes** the **Ethernet Header**? **L2 and L1**
- Give the **purpose** of **each header elements** in the **Ethernet Header**:

Ethernet Header Elements	The L2 Layer receiving the Frame recognizing what it has to do based on the header fields
Preamble	To deduce the amount of data that I need to pass up to L3
SFD	Is the frame received without any errors?
Destination Address	This is already stripped by L1 after recognizing the start of frame
Source Address	Whom should I respond to if I need to reply?
Length	My own address, because of which I am looking at this frame!!!
CRC	

Quiz 3: IP Payloads



- The **IP Payload** is the **data** that **belongs** to the **Layer**:

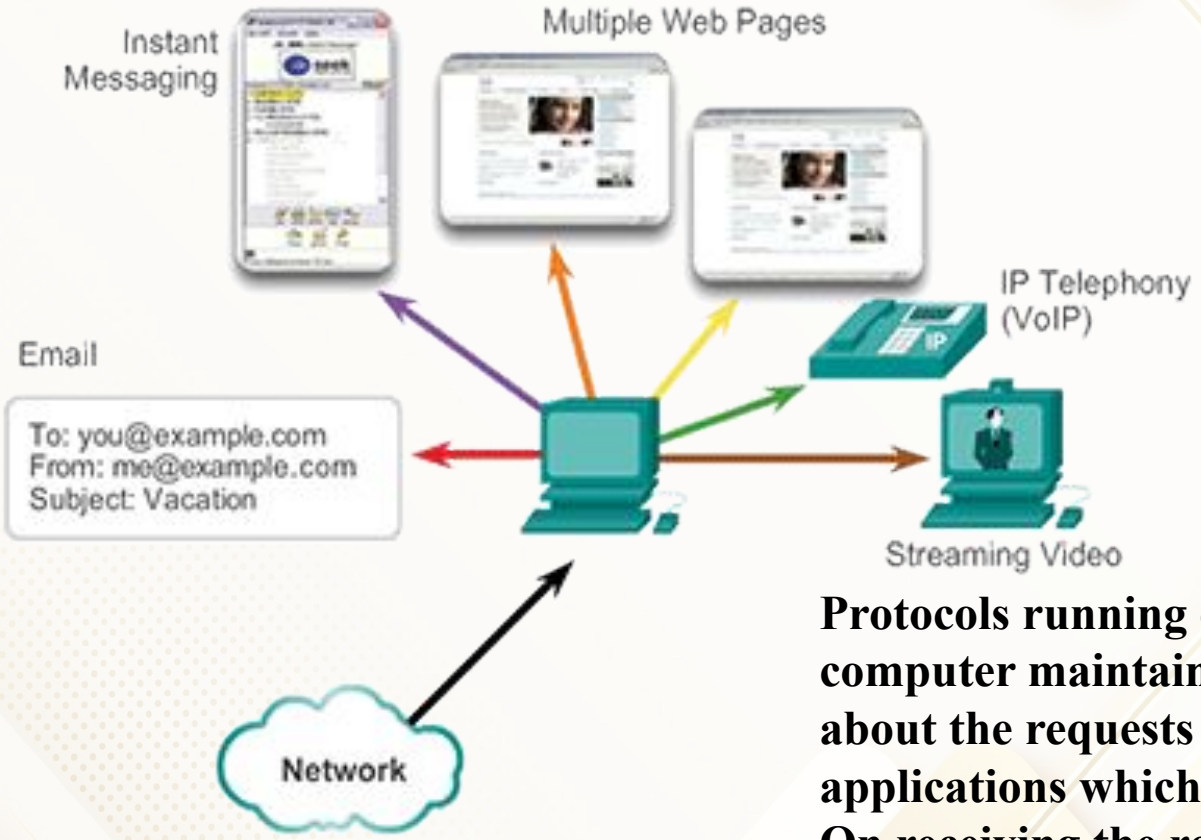
A. L2
B. L3
C. L4
D. None

ANS:

Option C. The data passed down by the L4 to IP layer (L3) is being carried by the IP packet as payload.

The TCP and UDP protocols pass their data down through IP layer to the intended recipient on the other end of the network.

Multiple Applications Using the Network



Packets/data from each application flows in both Directions over the network

Similar to people from different places and countries travelling together in an international air travel, the Data from different applications travel over the network one after the other

Protocols running on the sending computer maintains the information about the requests sent out and the applications which have initiated them. On receiving the responses de-multiplexing of the data to the respective application is done.

Different applications using the network can be categorized as TDM: Time-Division Multiplexing

Types of Payloads IP needs to Carry

- Since both TCP and UDP run on top of IP, IP should be able to carry the data given by both these protocols
- The data from TCP can be very large in size since it supports applications like FTP which supports file transfer
  - Files sizes can be as big as a few Giga Bytes
- IP should also be able to carry smaller size data of a few bytes of size, generated by UDP
- IP protocol needs to support two different wide range of requirements in terms of **size of data**
- TCP is connection-oriented and UDP is connectionless, it needs to support both types of **connectivity**
  - Given that **IP** itself is **connectionless** and **best-effort protocol**

IP needs to send the Payload over L2-L1

- Typical Datalink technologies are Ethernet and WiFi
- The **MTU** (Maximum Transmission Unit) of these technologies are:
  - **Ethernet**: 1500 bytes
  - **WiFi**: 2312 bytes (this does not include WiFi Header)
- Whereas the IP is receiving much bigger size data from the layers above which need to be sent over the above datalink layers with limited frame sizes
- There is a need for the bigger chunks of data to be segmented and sent over the physical network (L2-L1)
- The receiving end needs to reassemble the data back again before passing it above
- This is the motivation for the IP layer to include the **Fragmentation and Reassembly functionality**
- Now, Let us see how it is accomplished

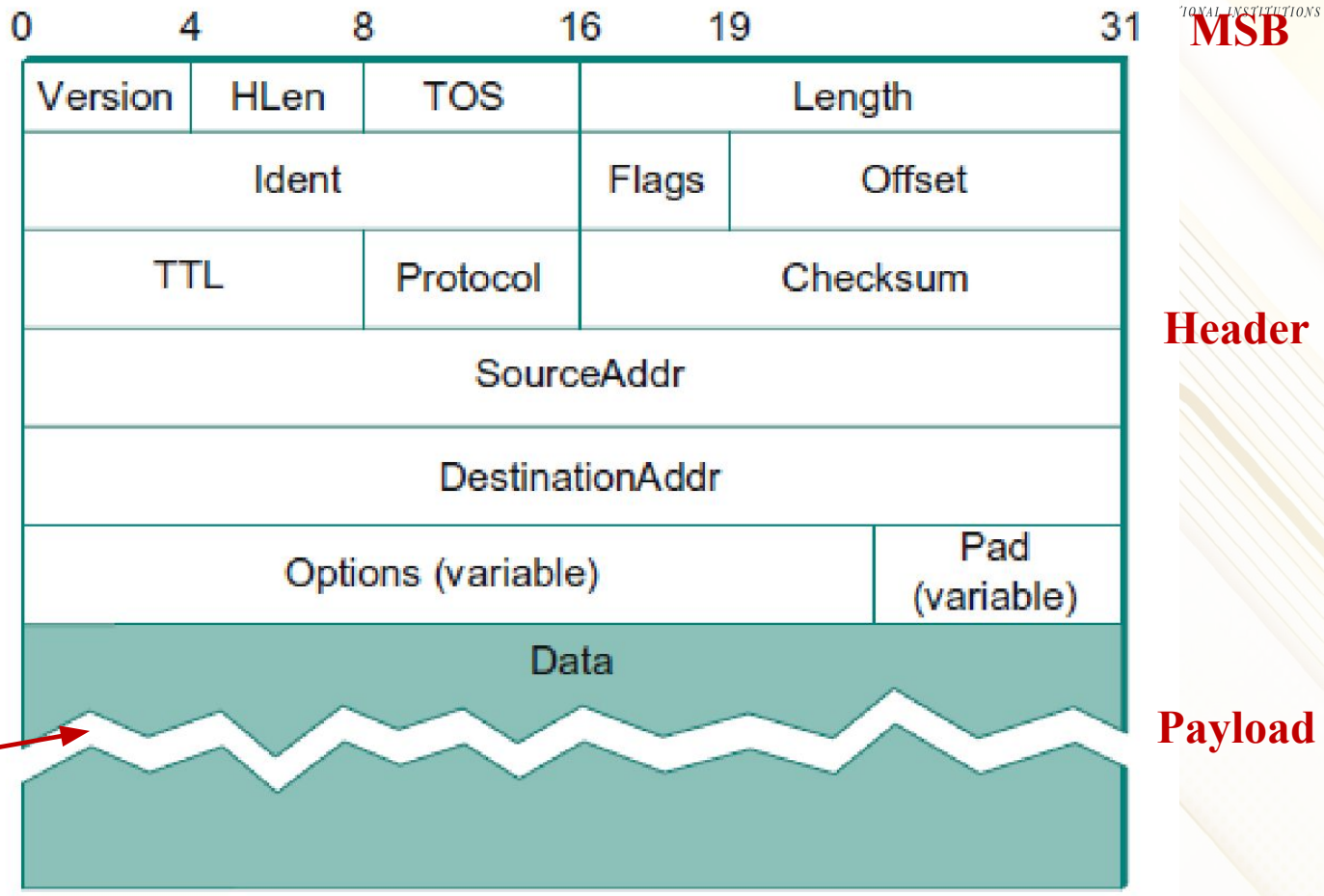
IPv4 Datagram Format

RV UNIVERSITY
Go, change the world

LSB

32 bits boundaries are used for the packet formats of L3 and above because it is easier for representation and processing by software

Note: **Datagram** includes **both** the **header** and the **data**

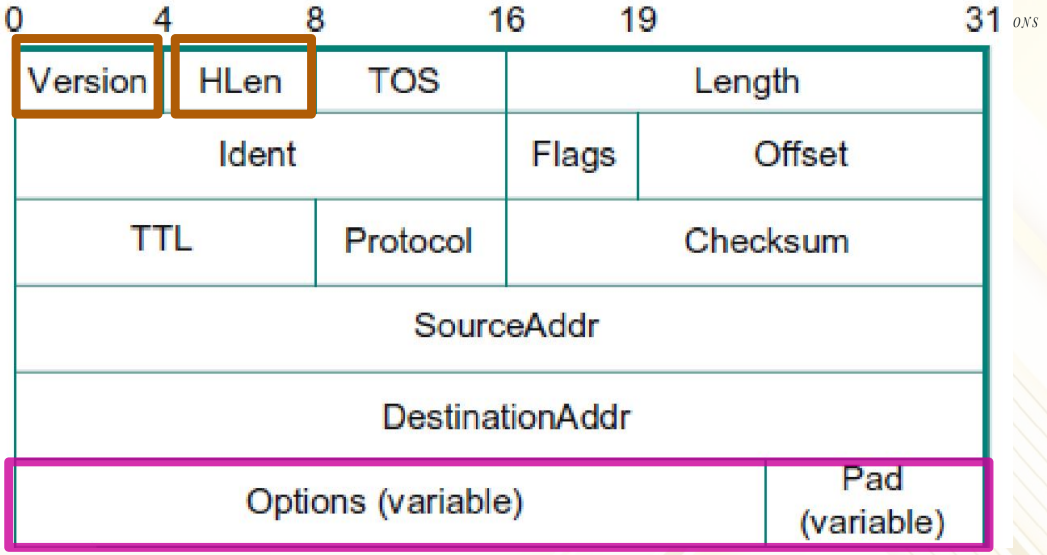


Break in between Indicates that the data part is much bigger than what is shown

- The packet format is shown here is different from what was used for Ethernet and WiFi frame formats

IPv4 Header Format - 1

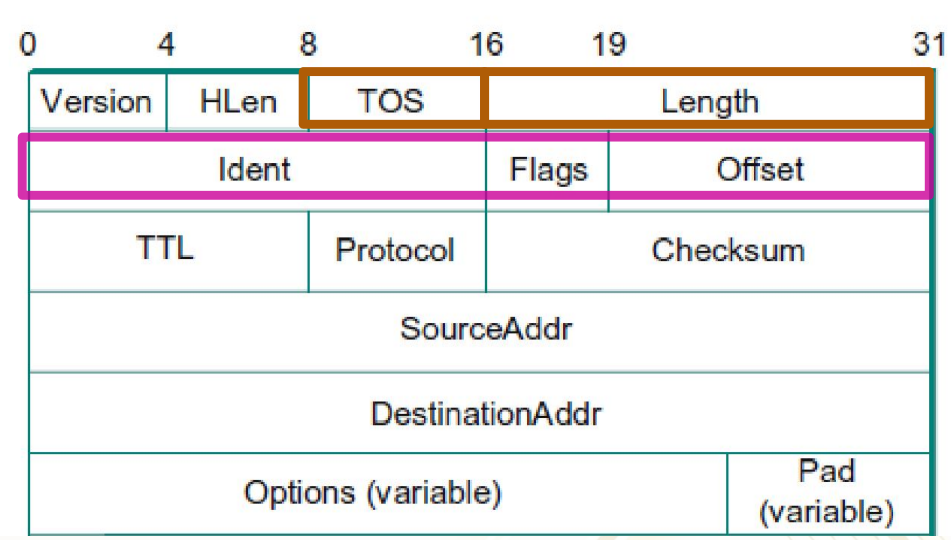
- **Version (4 bits)** gives the **IP format** that the rest of the header follows
  - **IPv4**: Version is 4
  - **IPv6**: Version is 6
- Based on this value the rest of the fields of the IP header are understood



- **HLen (4 bits):** It specifies the **length** of the **header** in **32-bit words**
  - The last word (32 bits) is **optional** whose **length** is **variable** **(multiples of 4 bytes)**
  - Most of the time the **IP header** is with **zero optional fields**
  - Which means that the **IP header** is of **20 bytes** length (only five 32-bit words)
  - So, **HLen** will have the **value** as 5 (since it is the length of the header field in 32-bit words)
  - Here, five 32-bit words, which is the first 20 bytes of IP header

IPv4 Header Format - 2

- **TOS (8 bits)**: Type of Service:
  - It's basic function is to allow packets to be treated differently based on application needs
  - Treatment means whether to delay it or forward it ahead of rest of the packets in the network, etc.

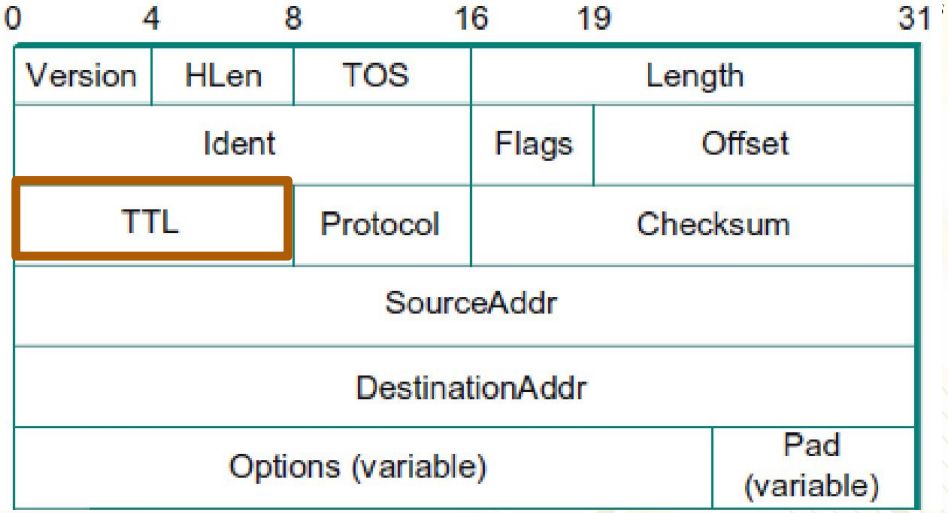


- **Length (16 bits)**: Length of the **datagram**, **including** the **header**.
- Unlike HLen field, the **Length** field counts **bytes** rather than words
- Thus, the **maximum size** of an **IP datagram** is **65,535 bytes**
- The physical network over which IP is running, however, may not support such long packets.
- For this reason, IP supports a **fragmentation and reassembly** process
- The **elements** of the **second word** is related to **SAR**, explained later

SAR: Segmentation and Reassembly, segmentation is another name for fragmentation

IPv4 Header Format - 3

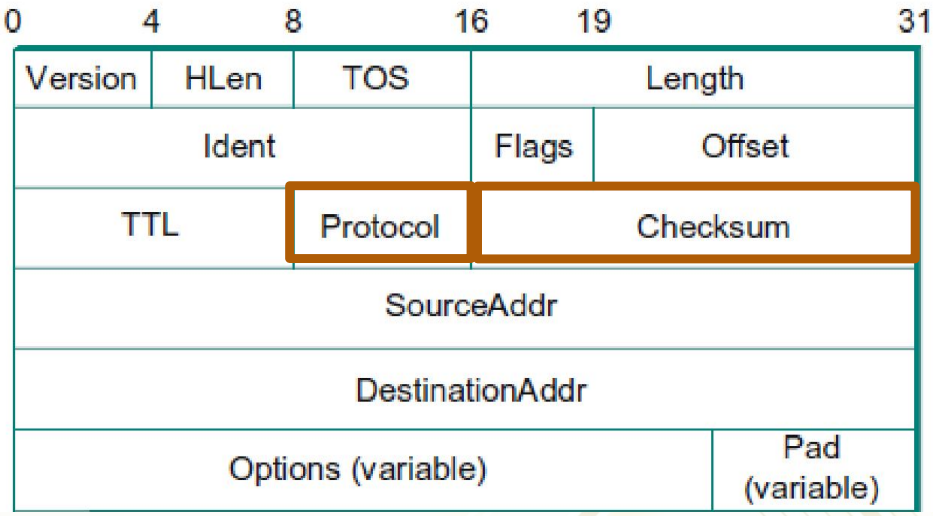
- **TTL (8 bits)**: Time to Live:
  - The intent of the field is to catch packets that have been going around in routing loops
  - And discard them, rather than let them consume resources indefinitely
  - It is different from frames going around in loops because of Bridges forming a loop



- **TTL** is originally used to count the number of seconds spent by an IP packet in the network before getting discarded.
- The routers while forwarding IP packets decrement the TTL by one
- Currently it is used to count the **number of hops**, that is the number of routers, the IP packet is passing through
- The **default initial value** set by the sender host is **64**

IPv4 Header Format - 4

- **Protocol (8 bits)**: The Protocol field is simply a de-multiplexing key that identifies the higher-level protocol which is using the IP layer services
- There are values defined for TCP (**6**) and UDP (**17**)
- And many other protocols that may be above the IP in the protocol graph.

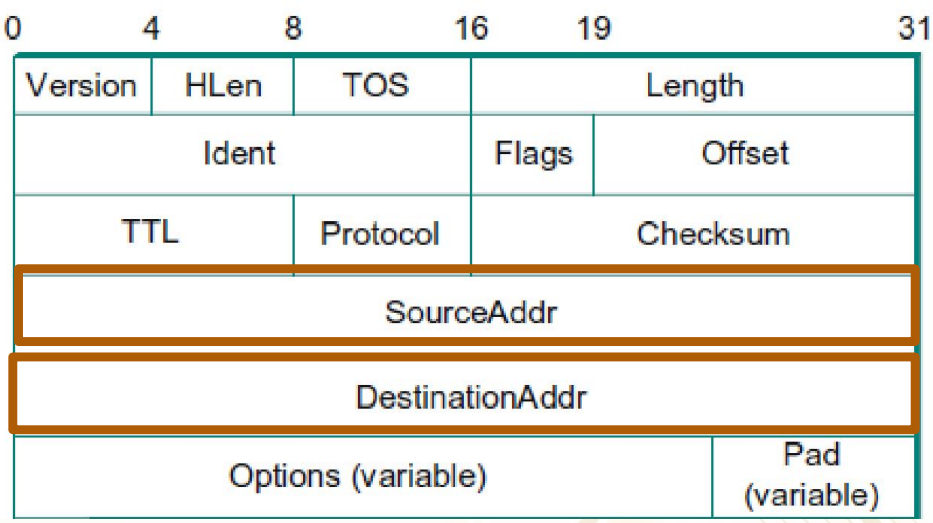


- **Checksum (16 bits):** It is calculated by considering the entire IP header as a sequence of 16-bit words,
- **Adding** them up using **ones complement arithmetic**, and taking the **ones complement** of the **result**
  - **Ref: Checksum algorithm** studied in the **Session 2C**
- Thus, if any bit in the header is corrupted in transit, the checksum computed will not give a correct result, upon receipt of the packet
  - If the checksum fails the entire IP packet is discarded by the receiver

IPv4 Header Format - 5

RV UNIVERSITY
Go. change the world

- **Source IP Addr (32 bits):** The Source I
  Address of the Host which has sent this
  IP packet
- IPv4 address is 32 bits wide
  - Typical IP addresses are given in the dott
    dotation
  - **8.8.8.8** (Google DNS server)

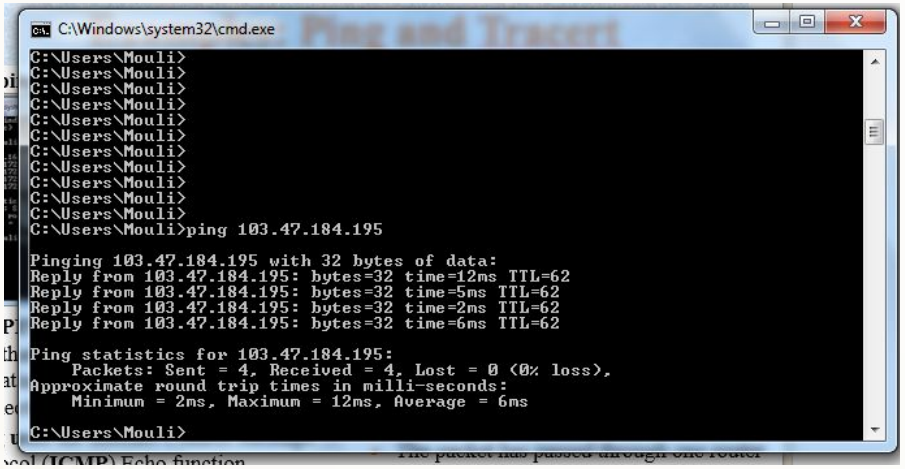


- **Destination IP Address (32 bits):** It is the IP address of the destination host to which this packet is to be delivered to
- Every packet contains a full address of its intended destination so that forwarding decisions can be made at each router
- The source address is required to allow recipients to decide if they want to accept the packet and also to enable them to reply
- IP defines its own **global address space,** independent of whatever physical networks it runs over. **It is covered shortly …**

Examples: Ping and Tracert

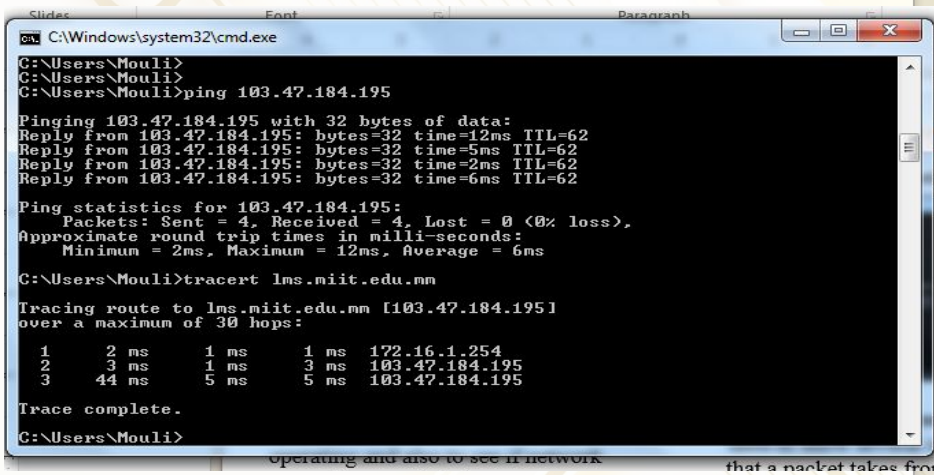
RV UNIVERSITY
Go, change the world
An Initiative of RV EDUCATIONAL INSTITUTIONS

ping: 103.47.184.195



- The **PING utility** is a system administrator's tool that is used to see if a computer is operating and also to see if network connections are intact.
- **Ping uses** the Internet Control Message Protocol (**ICMP**) Echo function
- From the **TTL** value, we can deduce the number of **routers visited** before **reaching** the **destination**
- Since **TTL** is **62**, **two routers** are **en-route**

tracert lms.miit.edu.mm



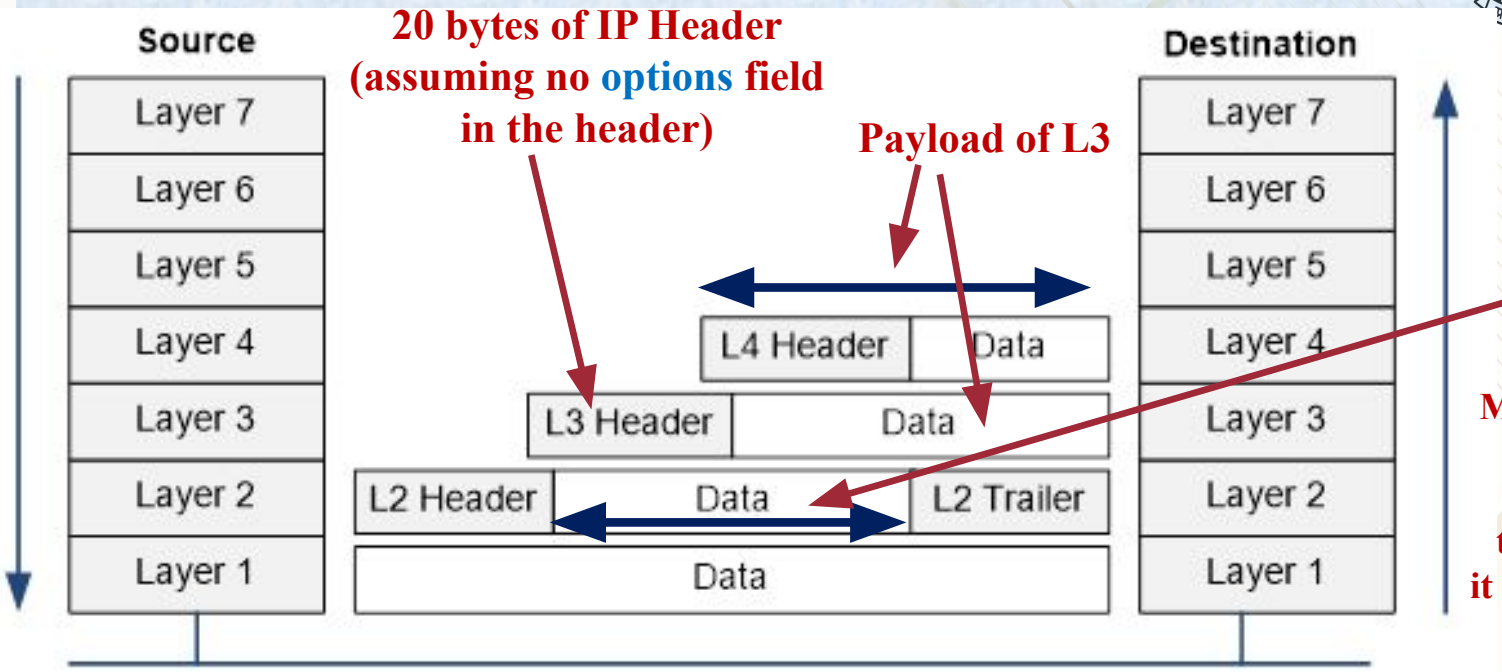
- The **tracert** (**trace route**) command is used to show several details about the path that a packet takes from the computer to whatever destination you specify
- The packet has passed through one router who's IP address is given above
- **172.16.1.254 (router** or **gateway) connecting to ISP**
- **Time** taken for the **packet** to **reach** the **destination** is **5 millseconds**

Ethernet: MTU: Maximum Transmission Unit

- The IEEE 802.3 specification limits the data portion of the 802.3 frame to a minimum of 46 and a maximum of 1500 bytes.
- The term maximum transmission unit (MTU) defines the maximum layer 3 packet (the layer above L2) that can be sent over a medium.
- Because the layer 3 packet rests inside the data portion of an Ethernet frame, 1500 bytes is the largest IP MTU allowed over an Ethernet.

Quiz 2: Payload and MTU

RV UNIVERSITY
Go, change the world
initiative of RV EDUCATIONAL INSTITUTIONS



- Does the IP datagram given to L2 to be transmitted over the physical link include the IP header also or only the data part of the IP layer?

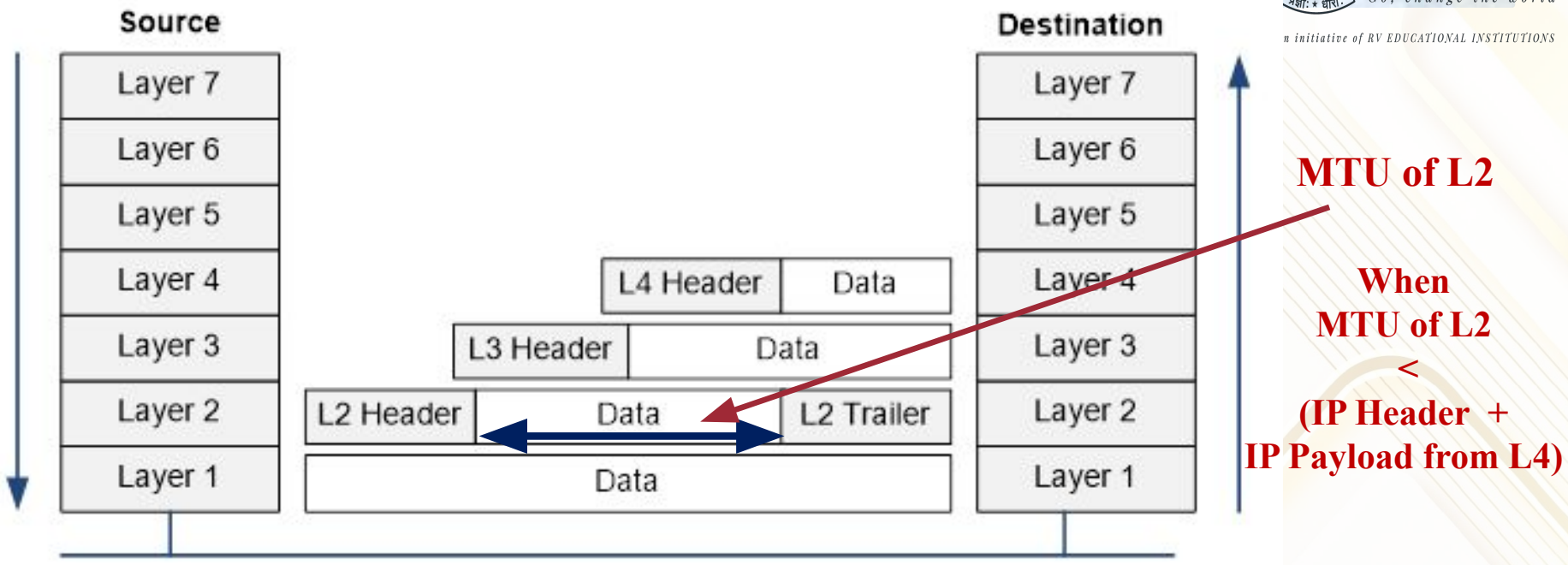
  ANS: It includes both the IP header and the payload from L3. Without the IP header, IP layer at the receiving end will not know what to do with that data.

- What happens when the size of IP datagram to be sent is larger than the MTU of the lower L2 level?

  ANS: It cannot be sent across the link unless the IP datagram is divided into smaller chunks of data, over multiple IP datagrams.

Quiz 3: When is fragmentation needed?

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS



- **IP datagram** has to be **fragmented before sending,** by the **host**:

A. When IP Header + IP Payload is larger than the MTU of local L2, to which the sending host is connected to

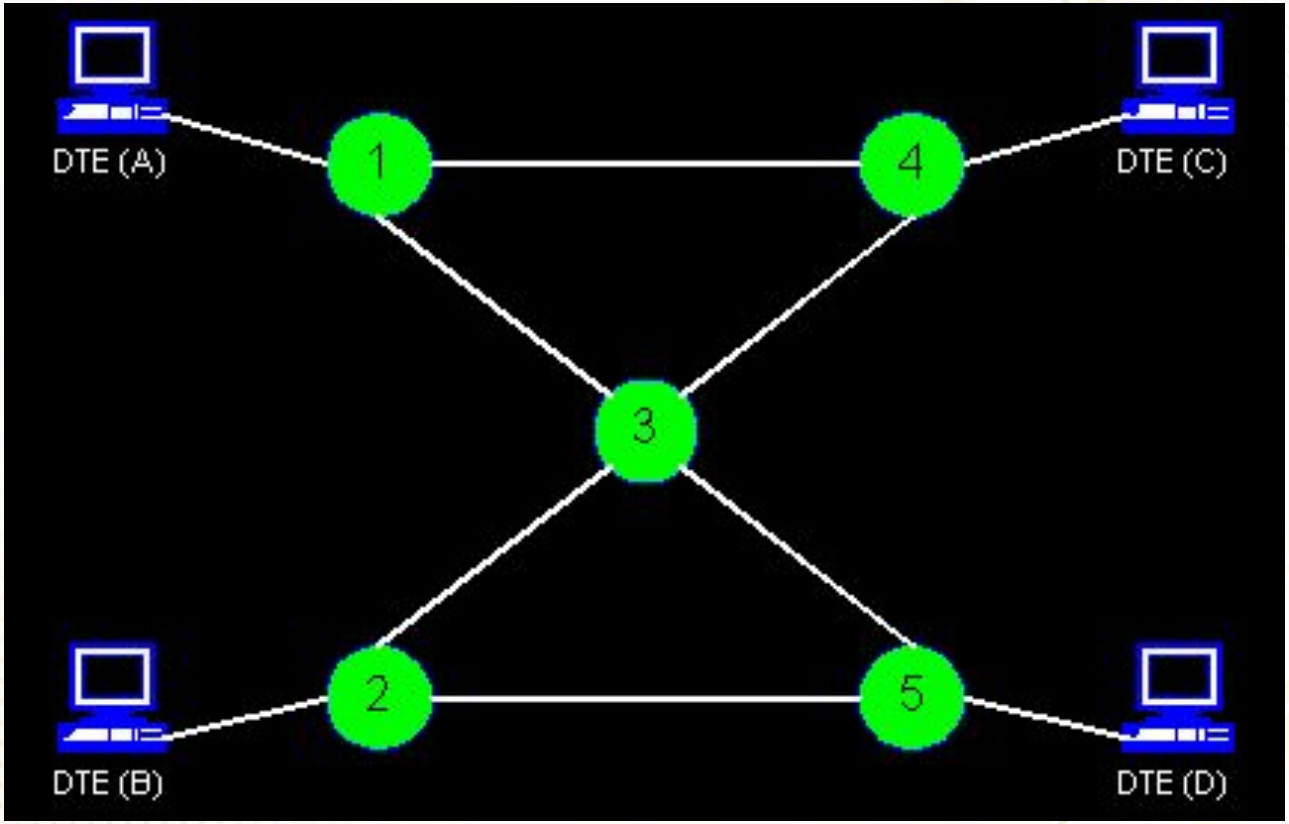
B. When the local MTU is larger than the IP datagram that needs to be transmitted

C. Both A and B are correct

D. None of the options are correct

ANS: Option A. Only when the IP datagram happens to be larger than MTU of the sender's L2

IP Fragmentation and Reassembly



Router

Host

C

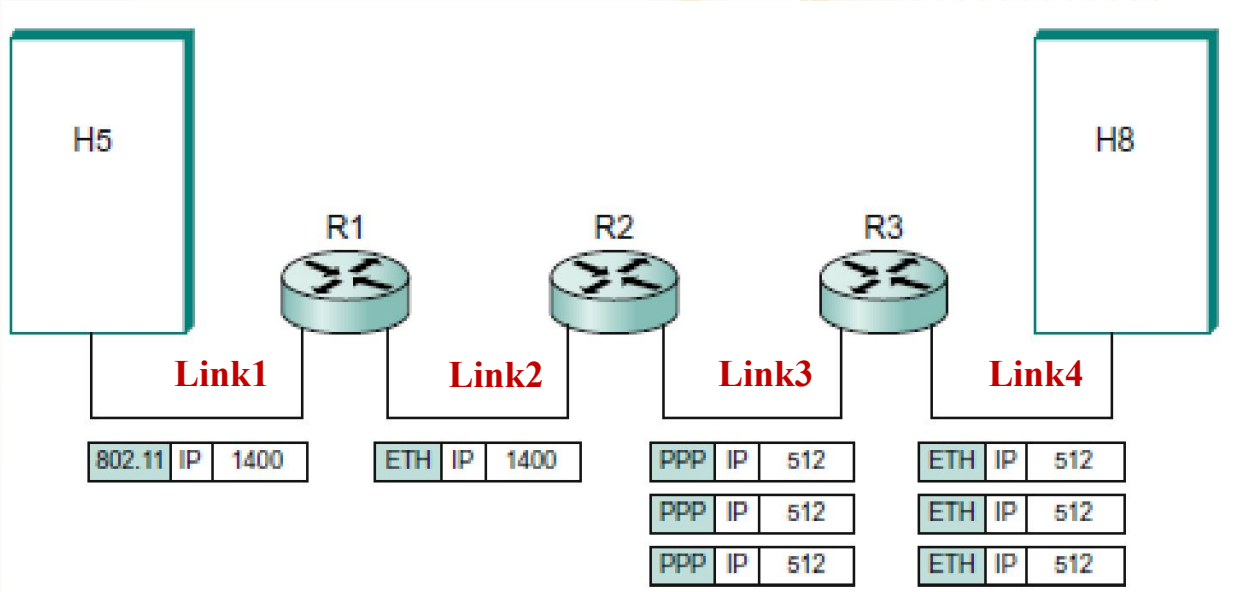
IP datagram being fragmented

Note: Loops formed by routers are handled by various IP routing protocols and also TTL field in IP header

- The out-of-order IP packets received by the host is reordered before passing them up to higher layer
- Why are they received out-of-order?

ANS: IP network is connectionless and IP datagrams can be routed through different paths with varying delays

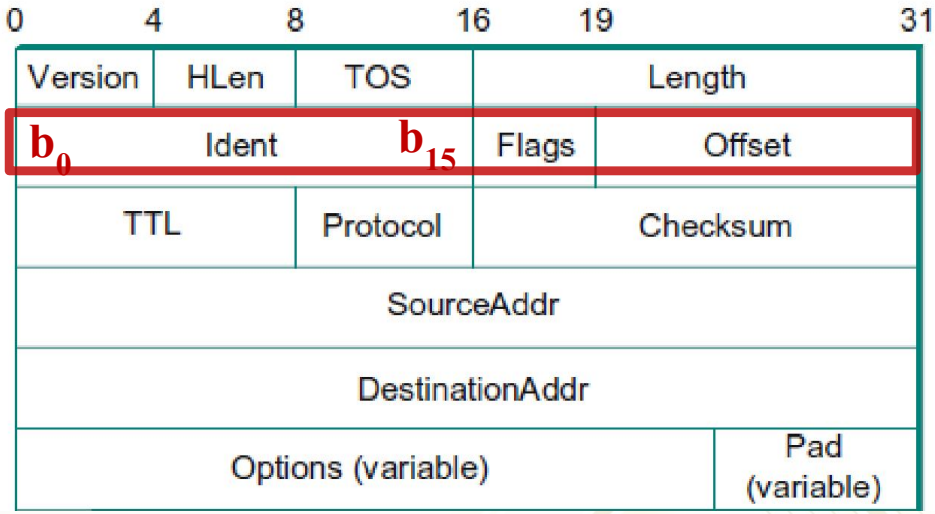
Where do Fragmentations happen?



- Fragmentation happens either at the sending host or in one of the routers enroute
- Once an IP Payload is fragmented, it is not reassembled on the way. Reassembly happens only at the receiving host
- Every fragmented IP data is also appended with the IP header before passing down to L2

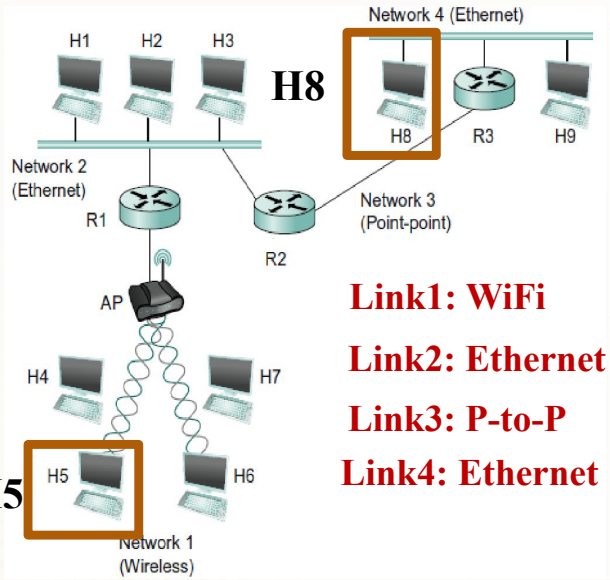
F & R related Fields in IPv4 Header

- **Ident (16 bits)**: **Identifier**:
  - The field which identifies the multiple IP datagrams belonging to a particular orginal IP payload from L4 which got fragmented by the sender
  - Or at any of the routers in the path of the IP datagram



- **Flags (3 bits)**: This is to pass on various information about a particular fragment of the original payload which got fragmented.
- **M flag** (**bit 18**) of the second word, when set, indicates that there are more datagrams to follow this current datagram
  - When it is cleared, it indicates that this datagram is the last datagram of the fragmented original datagram
- **Offset** (**13 bits**): It stores the offset of data bytes in terms of **8 bytes**

Example: Fragmentation & Reassembly - 1

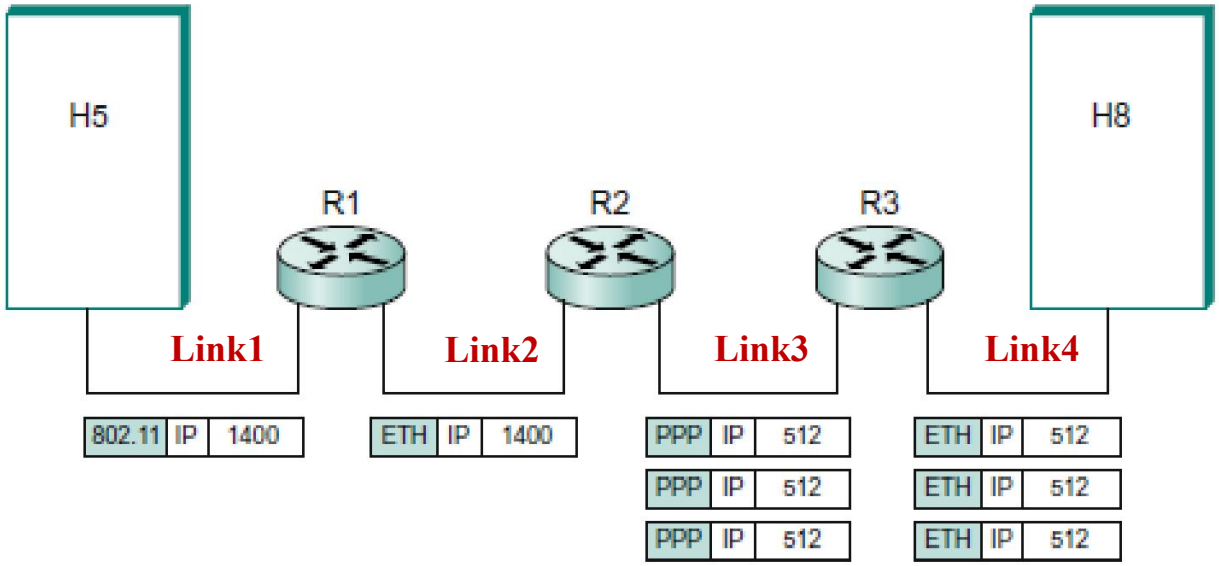


Link1: WiFi

Link2: Ethernet

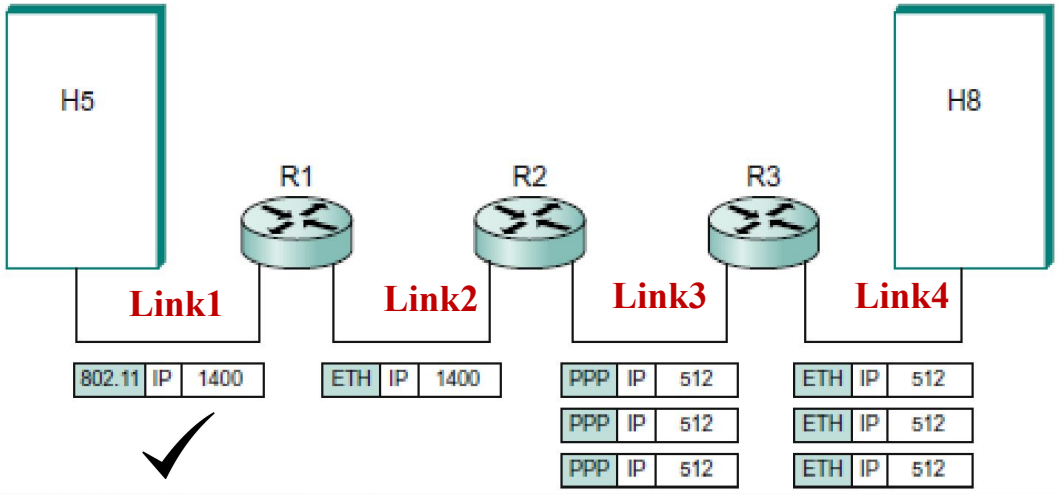
Link3: P-to-P

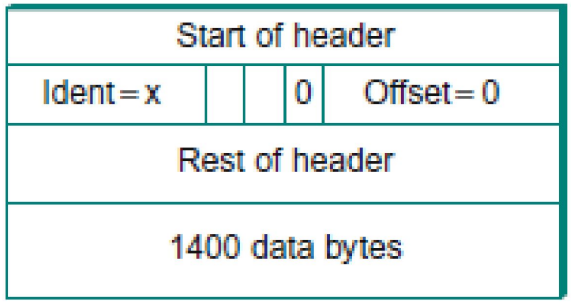
Link4: Ethernet



- Assume that initially the data part of the IP datagram is **1400** bytes at the Sender end (Host H5)
- Remember, the MTUs of Ethernet and WiFi are more than the payload size of L2 (20 + 1400) assuming IP header size is 20 bytes
- This data size of 1400 bytes can be accommodated without any fragmentation while passing it through the link till the Router R1

Example: Fragmentation & Reassembly - 2

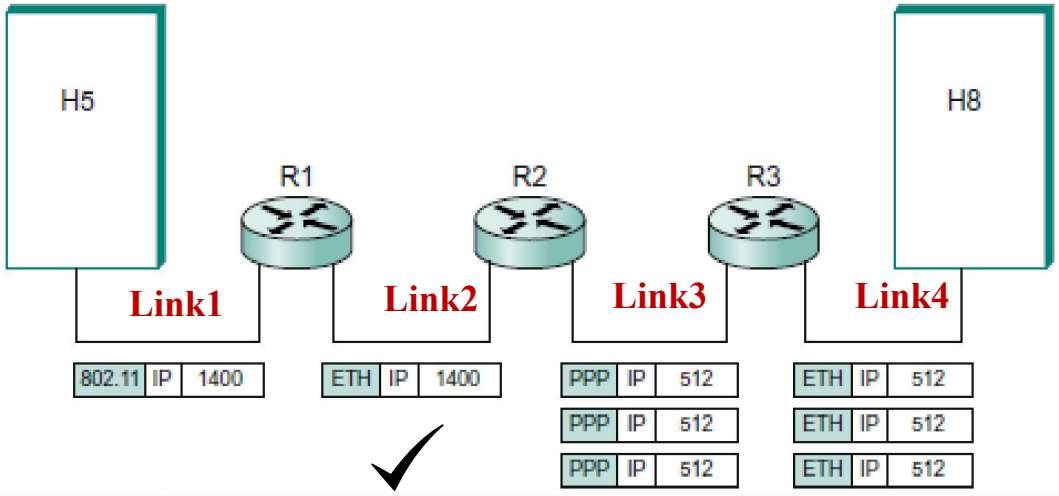




Payload of Link1

- The **IP header fields** while it is **sent over** the link **L1** is given above
- There is no fragmentation is done over the Link 1. The identifier is some **unique value** (**x**) though there is no fragmentation currently
- The **offset** is made **equal to zero** and the **M bit** in the **flags** field is also made equal to **zero**
- This indicates that this IP datagram is carrying the data which was not fragmented and this has the complete payload (1400 bytes) of L4 above

Example: Fragmentation & Reassembly - 3

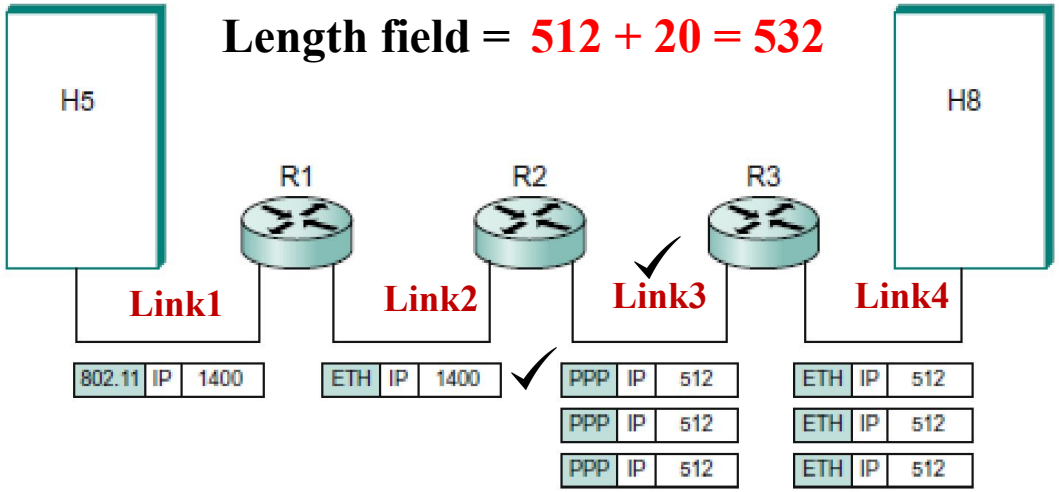


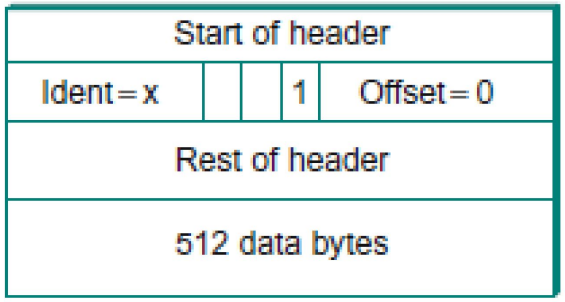
Start of header				
Ident = x			0	Offset = 0
Rest of header				
1400 data bytes				

Payload of Link2

- The **IP header fields** while it is **sent over** the link **L2** is given above
- L2 is also an Ethernet type and its MTU (1500 bytes) is greater than the Payload size 1400 bytes
- So, there is no fragmentation needed while sending this data over L2 too
- The IP header fields are same as what was seen over the Link1
  - Remember, while the same IP contents are sent over the Link2, the L2 layer header contents will be different having different Link2 MAC addresses

Example: Fragmentation & Reassembly – 4

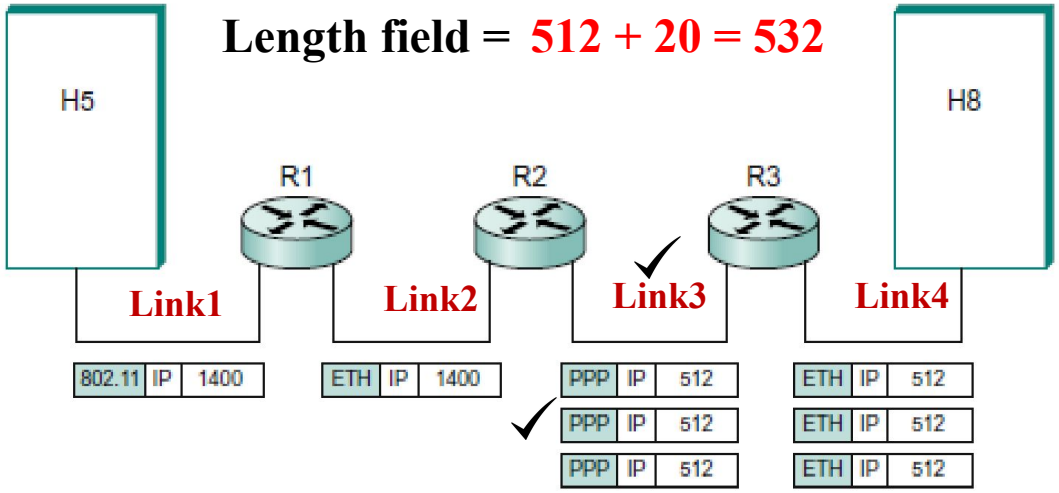


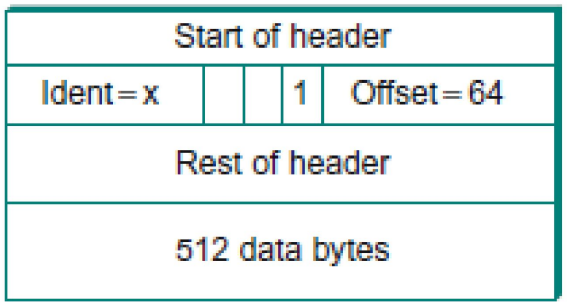


First fragment of the Original IP Datagram: Payload of Link3

- Assuming the MTU of the Link3 (P-to-P) is 532 bytes, the IP datagram has to be fragmented by the Router R2 before sending them over the Link3
- With the IP header taking 20 bytes, the useful data that can be sent through every fragment is only 512 data bytes
- The **offset** field is set to **zero** to indicate that the data contained in, is the first fragment of the data, of the original IP datagram
  - **M field** is also to be set to indicate that some more fragments of this data is on other IP datagrams

Example: Fragmentation & Reassembly – 5

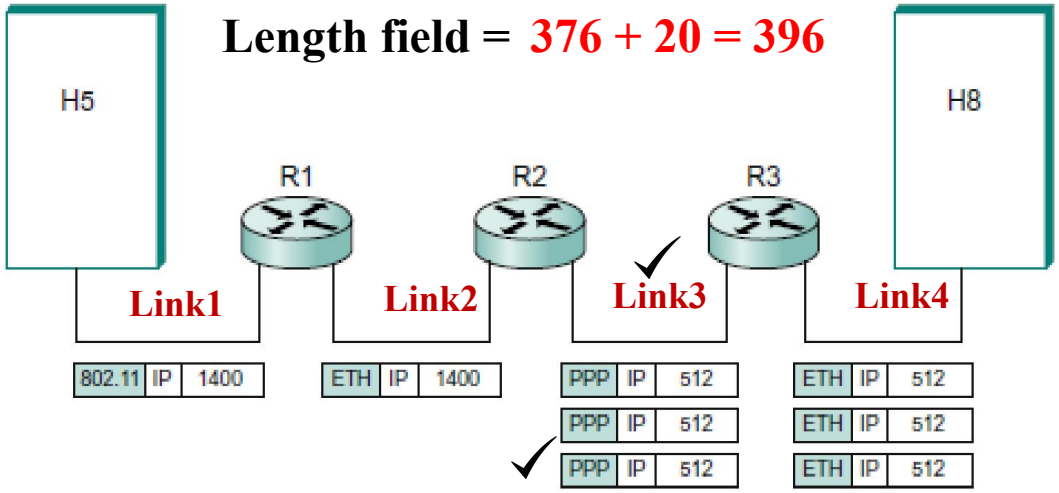




Second fragment of the Original IP Datagram: Payload of Link3

- The same unique identifier value is maintained which was sent by the sender originally
- The offset value is changed to 64 which is a count of 8 bytes, that means the offset in bytes is 64 * 8 = 512 bytes
- Because already 512 bytes have been sent through the first fragment (offset from 0 to 511)
- The second set of 512 bytes of data of the original IP data is being sent now

Example: Fragmentation & Reassembly – 6



Start of header				
Ident = x			0	Offset = 128
Rest of header				
376 data bytes				

Third fragment of the Original IP Datagram: Payload of Link3

- The same unique identifier value is maintained which was sent by the sender originally
- The offset value is changed to 128 which is a count of 8 bytes, that means the offset in bytes is 128 * 8 = 1024 bytes
- Because already 1024 bytes have been sent through the first and the second fragments (offset from 0 to 1023) already
- The third set of last **376 bytes** of data of the original IP data is being sent now, since this is the **last fragment** of the data, **M** is **zero**

Additional Points - 1: Fragmentation & Reassembly

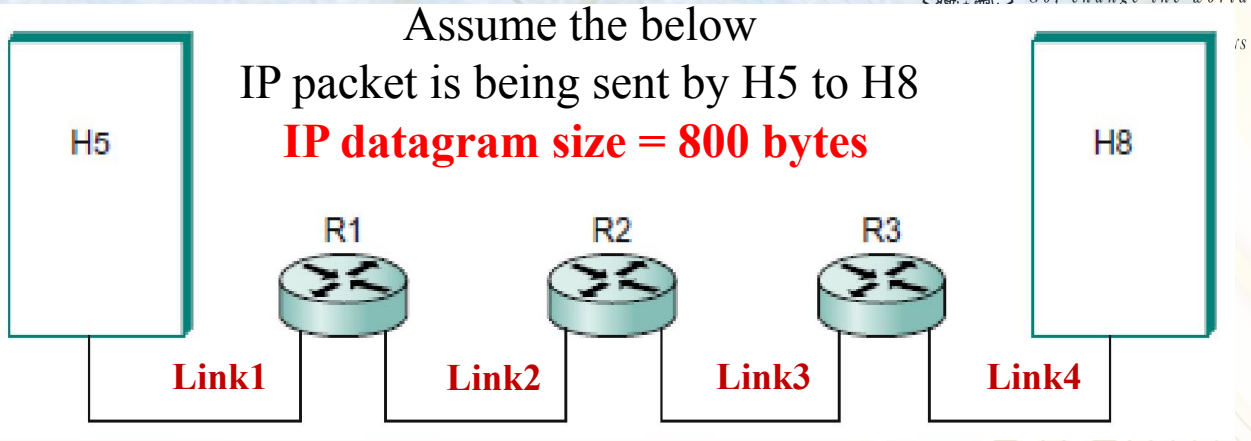
- Observe that the fragmentation process is done in such a way that it could be repeated if a fragment arrived at another network with an even smaller MTU.
- Fragmentation produces smaller, valid IP datagrams that can be readily reassembled into the original datagram upon receipt, independent of the order of their arrival.
- Reassembly is done at the receiving host and not at each router
  - Which means, after segmentation due to a lower MTU link, even if there is a link with higher MTU is encountered, the intermediate router do not perform reassembly
  - Once the IP datagrams are fragmented they are reassembled only at the host of receiving end
  - The fragmented IP datagrams may get further fragmented due to lower MTU links on the way, but never reassembled at the routers
  - The reason for this design decision is not to overload the routers with this complex task of reassembly for multiple flows going through it

Additional Points - 2: Fragmentation & Reassembly

- IP reassembly is a complex process.
- For example, if a single fragment is lost, the receiver will still attempt to reassemble the datagram, and it will eventually give up and have to garbage-collect the resources that were used to perform the failed reassembly.
- When a single fragment is either last or received with errors, all the fragments of that set is discarded,
  - No attempt is done by the IP layer to ask for retransmission, because it is a best-effort and no guarantee connectionless protocol
- For this reason, among others, IP fragmentation is generally considered a good thing to avoid.
- Hosts are now strongly encouraged to perform “path MTU discovery,”
- A process by which fragmentation is avoided by sending packets that are small enough to traverse the link with the smallest MTU in the path from sender to receiver.

Quiz 1: Fragmentation & Reassembly

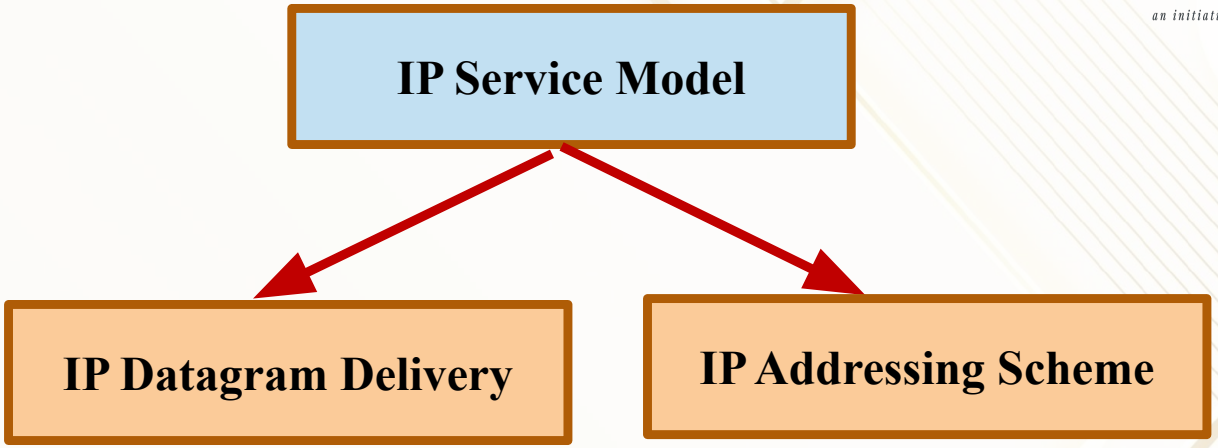
Links	MTU (bytes)
Link1	1500
Link2	200
Link3	1000
Link4	2000



1. Does the host H5 perform F & R on the above IP packet or not? Give the reason.
   - **ANS: No. The MTU of Link1 to which H5 is connected to, is more than the IP datagram size**
2. Does R1 do F & R on the same packet? If yes, how many fragments generated?
   - **ANS: Yes, four fragments of 200 bytes each because the MTU of Link2 is 200 bytes.**
3. How many frames pass through Link3 and Link4 carrying the same IP datagram?
   - **ANS: On both the Link3 and Link4, the same four frames (carrying the fragments) pass through. Though their MTUs are higher, reassembly is not done by the intermediate routers. Once fragmented, the IP packets get reassembled only on the host at receiving end (here, at H8).**
4. Suppose, host H5 peforms "Path MTU discovery", what happens?
   1. **H5 will perform F & R to the lowest MTU enroute. Four fragments of 200 bytes generated.**

Two Parts of IP Service Model - recap

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS



✓ Done (Sessions 6A to 6C)

Let us see this now … Session 7x series

- **IP Datagram** (**connectionless**) model of **data delivery**.
  - This service model is sometimes called **best effort** because, although IP makes every effort to deliver datagrams, it makes no guarantees.
- **IP addressing scheme,** which provides a way to identify all hosts in the internetwork,

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

IP Addresses

Why MAC addresses are not used for routing?

- A MAC address is an unique identifier of every network interface.
  - They are also called **Physical Addresses**
- It is a **48-bit number** (12 hexadecimal characters). They can either be written in either of these formats
  - **22-C0-90**-94-9C-07 or **22:C0:90:**94:9C:07
  - **22-C0-90**: Identifies the manufacturer of this NW interface
  - MAC addresses have two parts, the first 24 bits give the manufacturer details
  - And the next 24 bits are the serial number of the **network interfaces** manufactured by that company
- The first 24 bits identify the manufacturer—but this provides **no useful information** to **routing protocols** since this **structure** has nothing to do with the **network topology** they are in
  - Though **MAC addresses** are **globally unique**, they are **flat**
  - So, MAC addresses cannot be used for routing packets across the internetwork

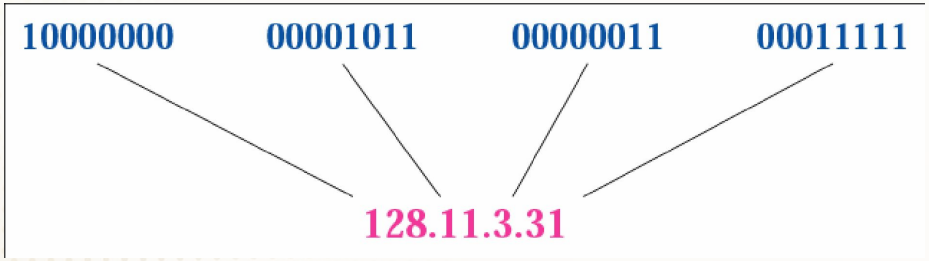
IP Addresses: Design Requirements

- We need another type of addresses to identify each host on the internetwork to route packets to them. IP addresses help us do that.
- If we want to be able to send data to any host on any network, there needs to be a way of identifying all the hosts uniquely
- Thus, we need a **global addressing scheme**— one in which no two hosts have the same address
- **Global uniqueness** is the **first property** that should be provided by the IP addressing scheme
- **Second property** is **hierarchical structure** of IP addresses
- They are made up of several parts that correspond to some sort of hierarchy in the internetwork
- IP addresses consist of two parts, usually referred to as a **network part** and a **host part**

IP Addresses: Notation

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- An IPv4 address is a 32-bit address that identifies a Host connected to the Internet, uniquely.
- The address space of **IPv4** is 2^{32} or **4,294,967,296**.
- IP addresses are normally written in a Dotted-Decimal (without leading zeros) notation

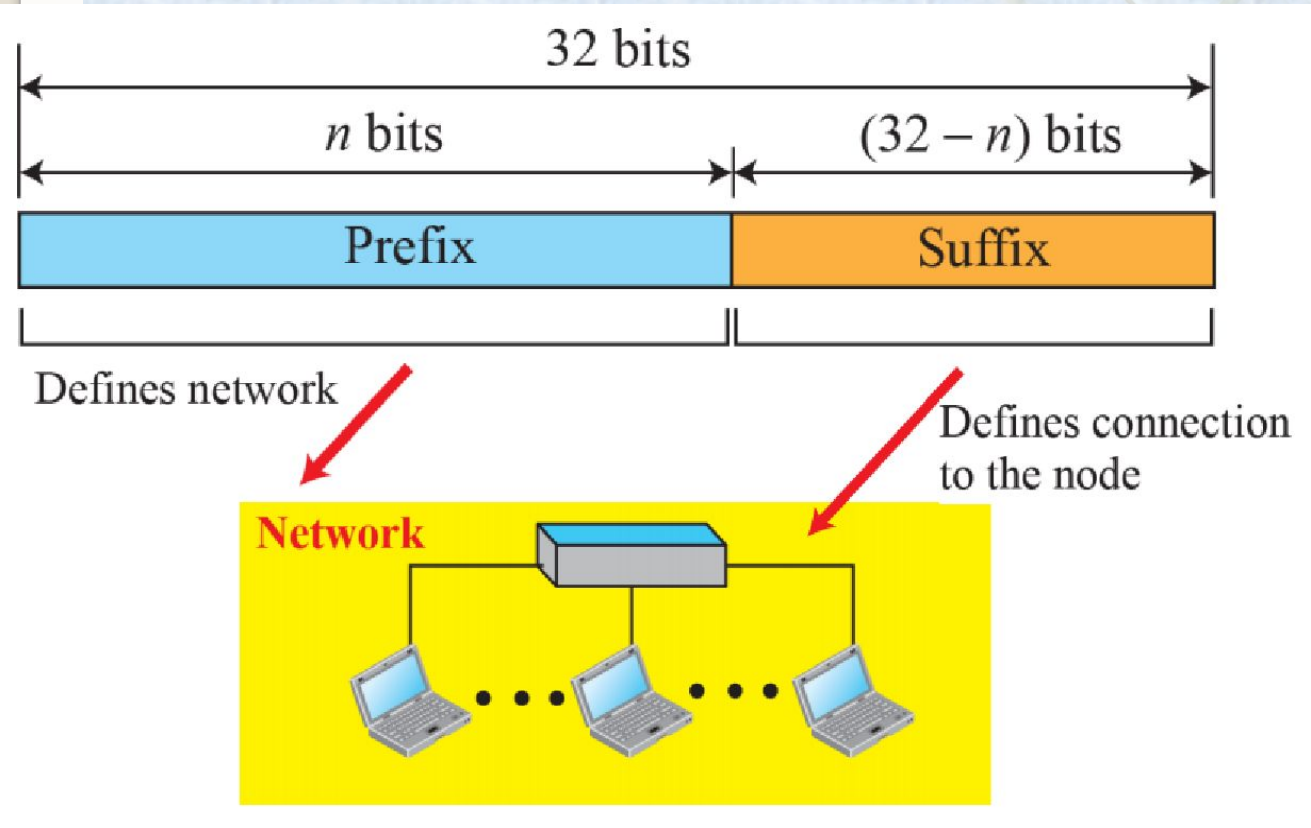


Note: **IPv6** uses **128-bit IP addresses**.

Since IPv4 addresses ran out, IPv6 standard came out.

Major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world united to redefine the global Internet and permanently enable IPv6 for their products and services on **6 June 2012**

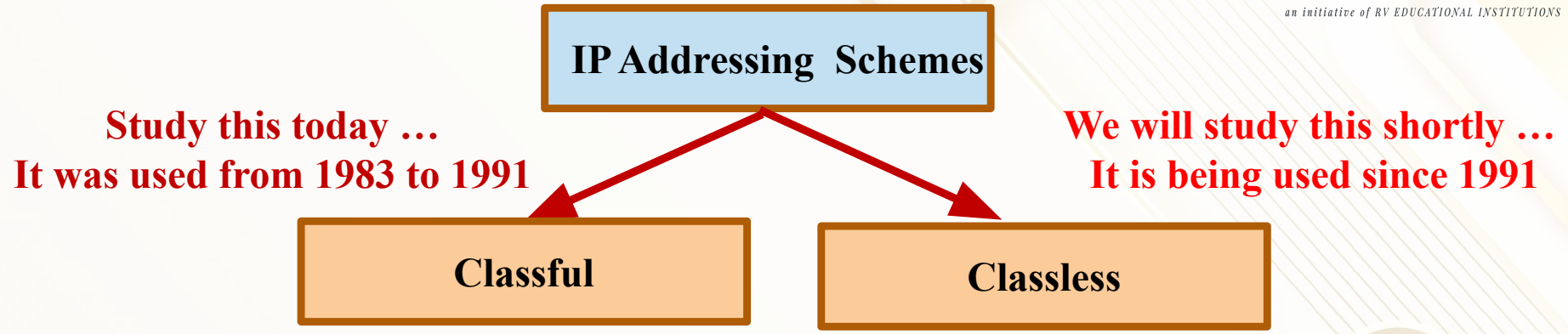
IPv4 Address Format



- 32 bits are split into two parts
  - **Network ID** and **Host ID**
  - **Prefix**: **Network ID**
  - **Suffix**: **Host ID**
- Network ID identifies the network where the Host is
- Host ID defines the node/host on that network

Two Types of IP Addressing Schemes

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS



- **Classful**: The **IP address space** (all possible IP values) is **divided** into **five classes**: **A, B, C, D,** and **E.**
- **Classless**: Instead of having five distinct address classes (Class A to E), classless addressing scheme allows an arbitrary number of classes based on the requirements

Notes: **a)** IP addresses are assigned by an international body called **ICANN**: Internet Corporation for Assigned Names and Numbers

b) Block of IP addresses with unique Net IDs are assigned to organizations or ISPs by ICANN. The individual organizations decide the allocation of specific Host IDs to the hosts on their network.

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

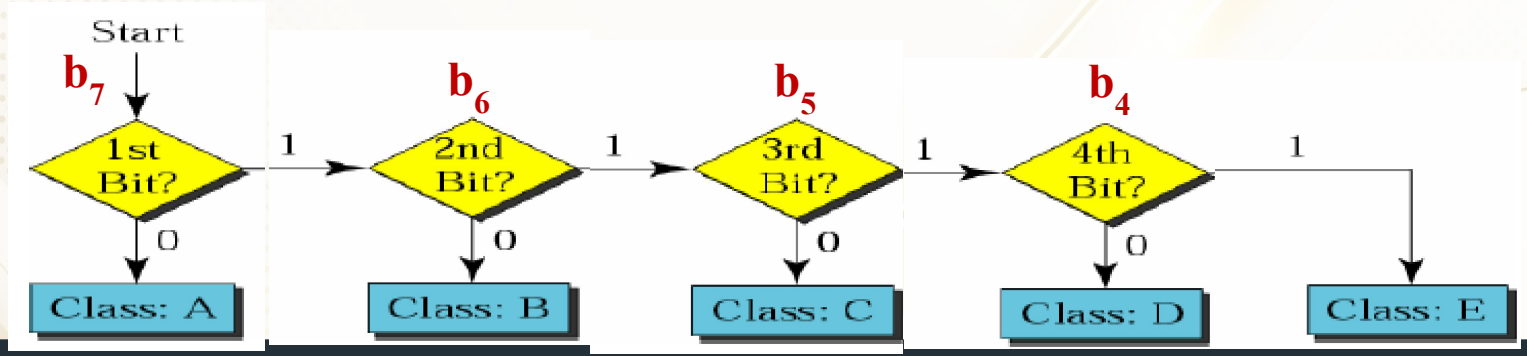
Classful IP Addressing Scheme

Classful: Classes A, B, C, D and E

- The MSB of IP address decides the class an IP address belongs

First Byte

values		First byte (b_7 … b_0)	Second byte	Third byte	Fourth byte
0 - 127	Class A	0			
128-191	Class B	10			
192-223	Class C	110			
224-239	Class D	1110			
240-255	Class E	1111			



Quiz 2: Number of Addresses of each Class type

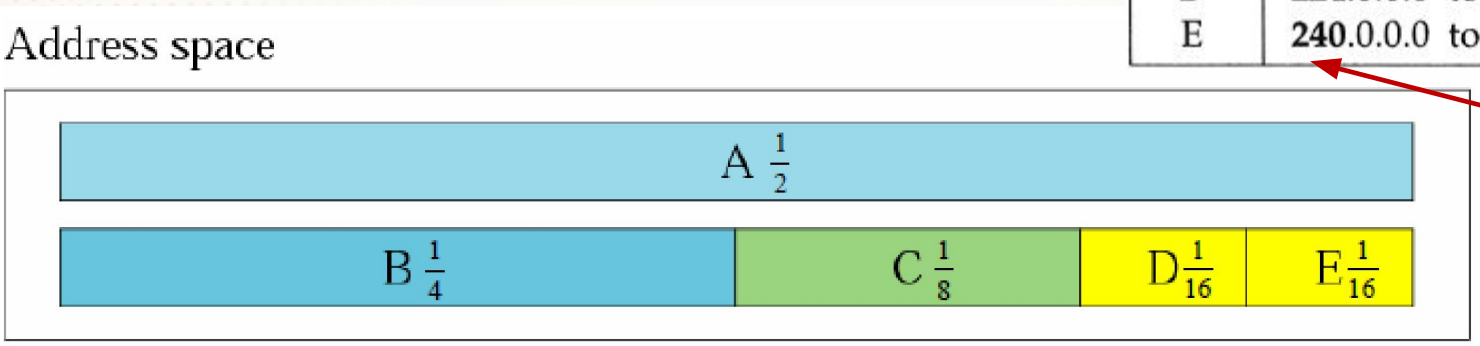
Class	No. of addresses
Class A	2^{31}
Class B	$2^{31}/\ 2 = 2^{30}$
Class C	$2^{30}/\ 2 = 2^{29}$
Class D	$2^{29}/\ 2 = 2^{28}$
Class E	$2^{29}/\ 2 = 2^{28}$

	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10			
Class C	110			
Class D	1110			
Class E	1111			

- How many IP addresses of each class be there? **Compare the sizes of each Network class**

Class A > Class B > Class C > Class D = Class E

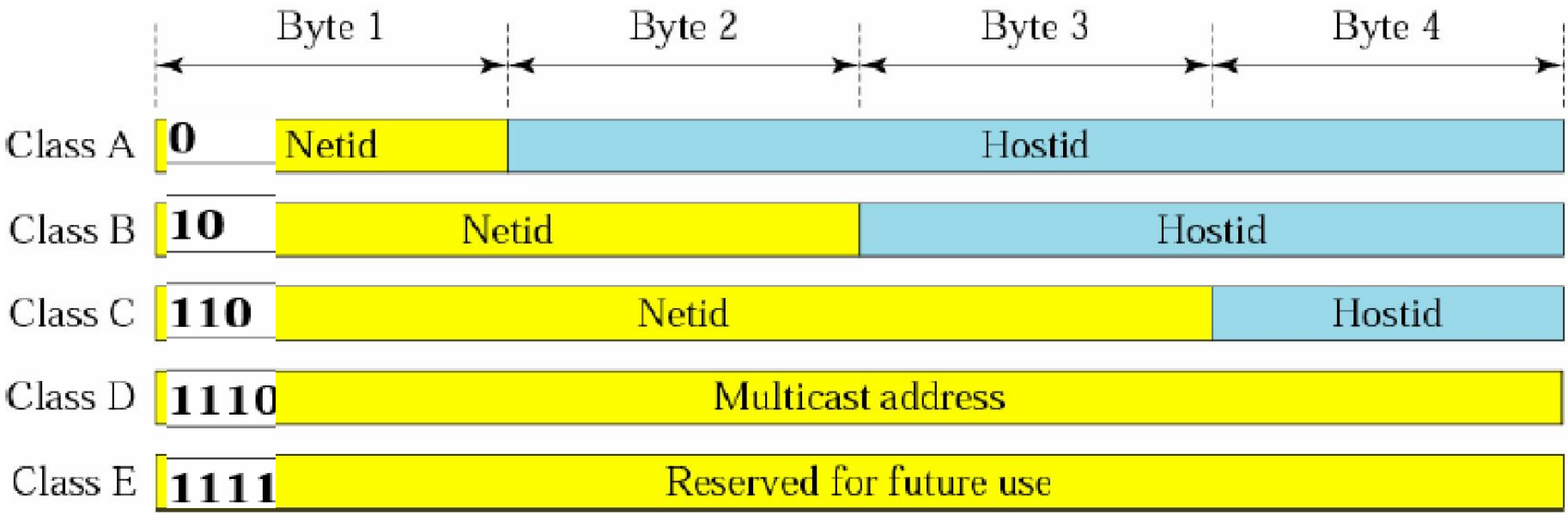
Class	Range
A	0.0.0.0 to 127.255.255.255
B	128.0.0.0 to 191.255.255.255
C	192.0.0.0 to 223.255.255.255
D	224.0.0.0 to 239.255.255.255
E	240.0.0.0 to 255.255.255.255



First Byte

128 □ 0x80
192 □ 0xC0
224 □ 0xE0
240 □ 0xF0

Quiz 3: Classes and its Net IDs and Host IDs



- **Only Class A, B** and **C** addresses are **sub-divided**
- **Exercise**: How many different **NetIDs** and **HostIDs** are there in each of the **classes A, B** and **C**?

	Netid's	Hostid's
Class A	• 2^(8-1) = 128	• 2^24 = 16,777,216
Class B	• 2^(16-2) = 16,384	• 2^16 = 65,536
Class C	• 2^(24-3) = 2,097,152	• 2^8 = 256

Note: Do not try to fix the net ID part of the IP addresses as per above pattern, because classful scheme is no longer used, except for some specific IP addresses.

Range of IP Addresses of Each Class

PV UNIVERSITY
Go, change the world

First Byte

128 □ 0x80
192 □ 0xC0
224 □ 0xE0
240 □ 0xF0

1. An **IP address** with **all zeros** is used by a device to refer to itself when it doesn't know its own IP address

2. **Host IDs** with **all zeros** and **all ones** are **reserved in all the classes**. They are not assigned to hosts on any class of networks. Used for multicast

3. So, the valid Host IDs of each class of addresses are always two less than the range of values available in each class.

More details on Classes

RV UNIVERSITY
Go, change the world
ve of RV EDUCATIONAL INSTITUTIONS

Classes of Addresses

The maximum **network size** is determined by the class of the address:

- **Class A** -- large
- **Class B** -- medium
- **Class C** -- small

Note: **Network size** refers to the **number of hosts** on the **network**

First Four Bits Of Address	Table Index (in decimal)	Class of Address
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Advantage of Classful Addressing: Given an Classful IP address, prefix can be found Immediately, no extra information is needed!!!

Intended Uses of Each Class of Addresses

RV UNIVERSITY
Go, change the world

IP Address Class	Fraction of Total IP Address Space	Number Of Network ID Bits	Number Of Host ID Bits	Intended Use
Class A	1/2	8	24	Unicast addressing for very large organizations with hundreds of thousands or millions of hosts to connect to the Internet.
Class B	1/4	16	16	Unicast addressing for medium-to-large organizations with many hundreds to thousands of hosts to connect to the Internet.
Class C	1/8	24	8	Unicast addressing for smaller organizations with no more than about 250 hosts to connect to the Internet.
Class D	1/16	n/a	n/a	IP multicasting.
Class E	1/16	n/a	n/a	Reserved for “experimental use”.

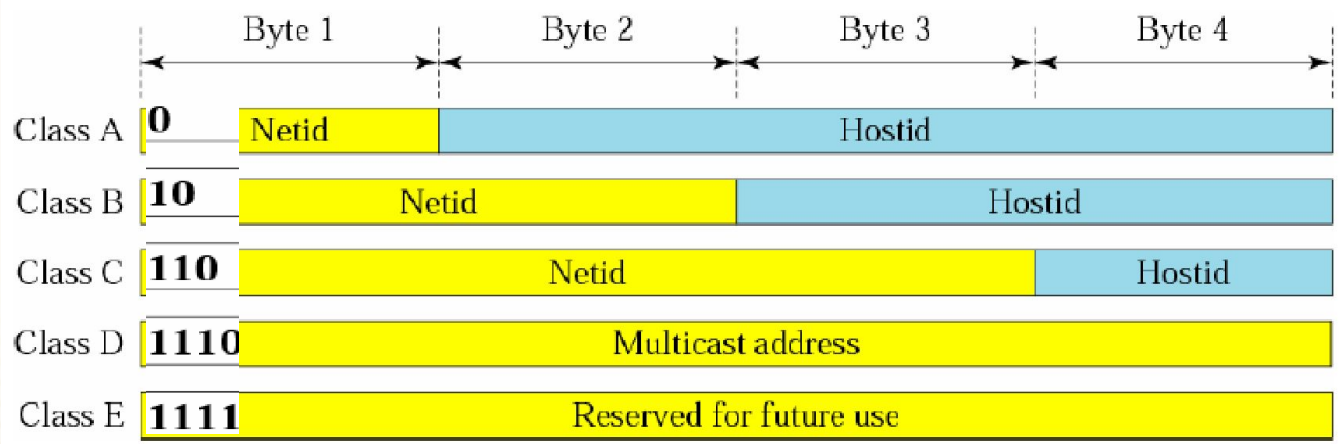
Disadvantages of Classful Addressing

- **Lack of Internal Address Flexibility**
  - Big organizations are assigned large, "monolithic" blocks of addresses that normally don't match well the structure of their underlying internal networks.
- **Inefficient Use of Address Space**
  - The existence of only three block sizes (classes A, B and C) leads to waste of limited IP address space.
  - Because, not all the host IDs of an allocated class of IP address may be used by an organization
- **Proliferation of Router Table Entries**
  - As the Internet grows, more and more entries are required for routers to handle the routing of IP datagrams,
  - This causes performance problems for routers.

Quiz 1: Identify the Classes of Addresses (Classful)

Q1. Identify the **Class** of the **IP Addressing (classful) Scheme** to be **chosen** if the **number of hosts** likely to be in the **network** is:

The **Net ID** and **Host ID** of **classes** are:



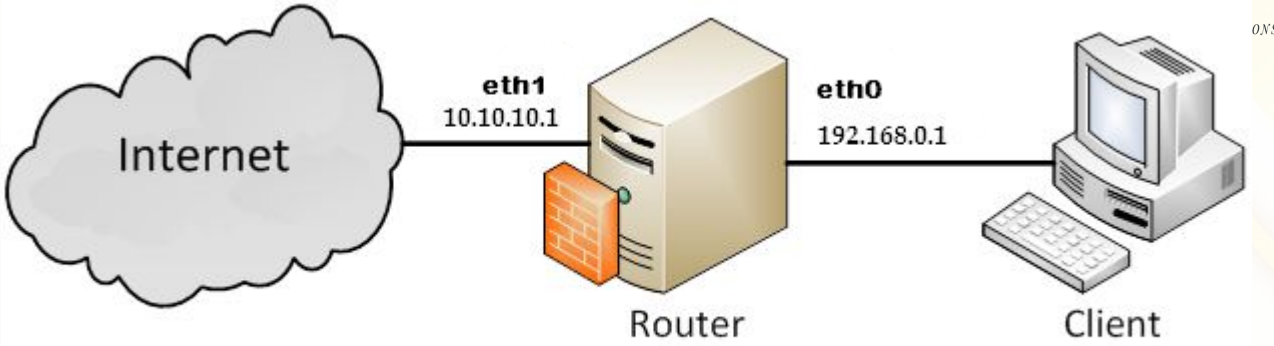
No. of Hosts	IP Class (classful)
200	Class C
20,000	Class B
2,00,000	Class A

1. How many Class C networks can there be in the world?
   - **How is the Class C address identified?** **ANS**: Given above in the picture
   - **The remaining bits available for Net ID, leaving out the pattern 110 (3 bits out of 24 bits), then the number of class C networks could be (2^{21}) □ 2,097,152**
2. How many **Class B networks** can there be in the world?
   - **No. of Class B networks could be (2^{14}) □16,384**

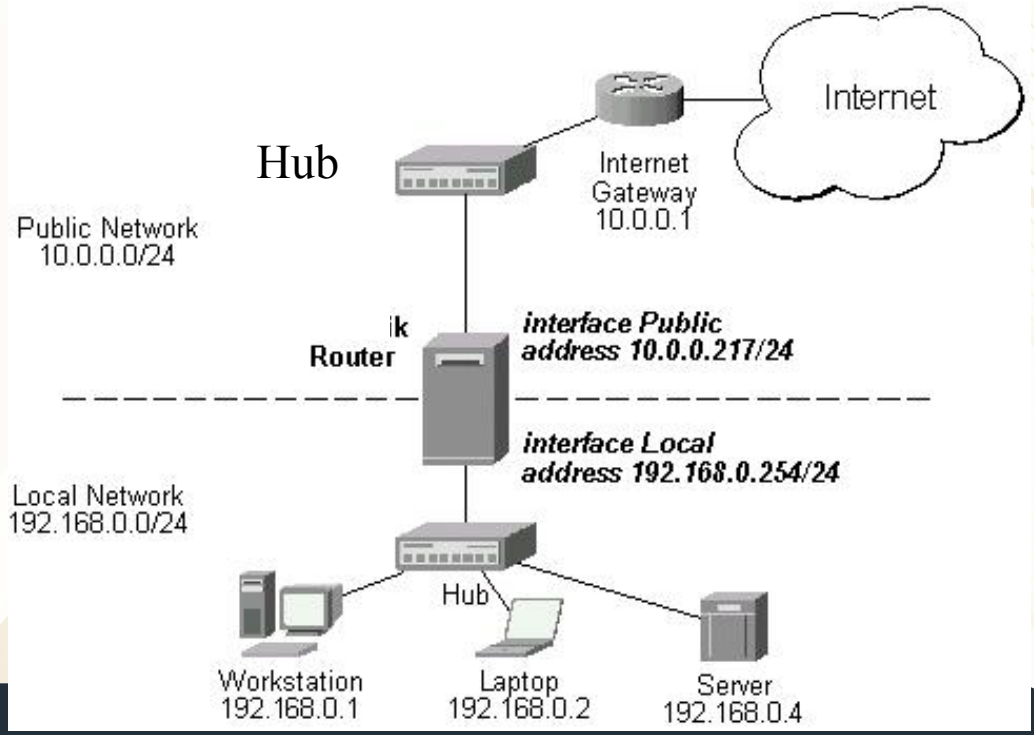
Homework: Find the total number of hosts/networks in each type of classes

Note; All zeros and all 1s for Host ID are reserved.

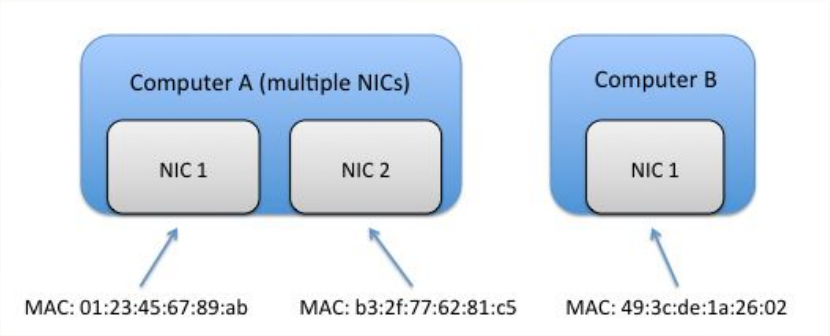
Example IP Routers: Connected to Two Networks



- **IP routers** are to be connected at least to **two or more different networks** to enable it to route IP datagrams
- They run **IP protocol**.
- Router has a MAC address on each of the networks it is connected to
- Now, how does a router get the IP datagram from the source machine or host? Let us see …

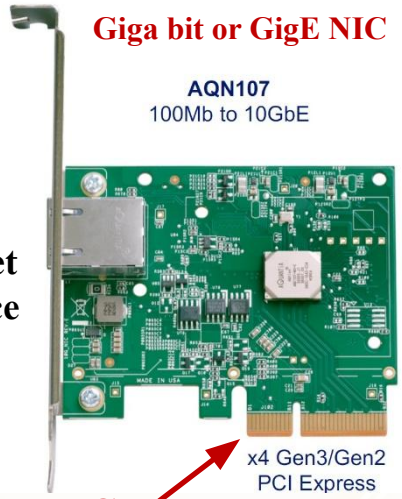


Network Interface Cards (NIC) in a Router



Notice that they have **different MAC addresses** on those **networks**

RJ45 Ethernet Interface

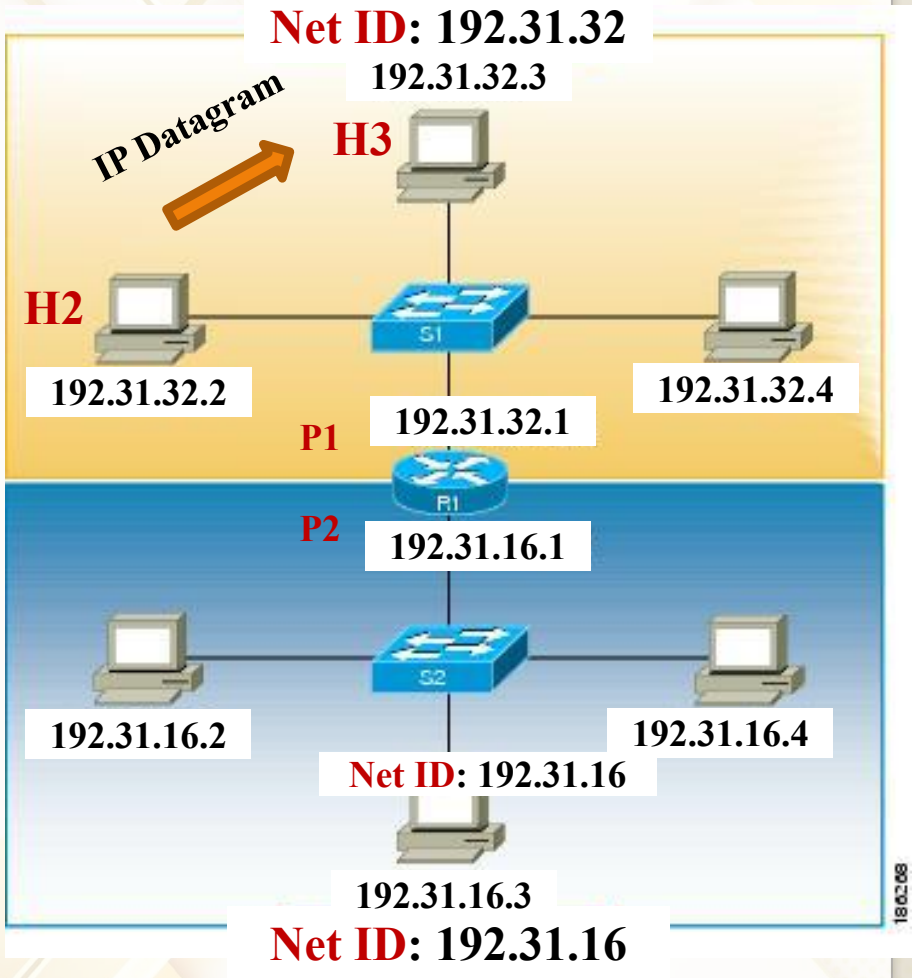


- For a router to be on two networks, it needs to have two network interface cards in them
- A PC with two interface cards, running IP routing protocol, can be considered as a router
- Which is capable of sending IP datagrams on any one of the network interfaces it has, based on the routing or forwarding table entries
- Having two network interfaces is the minimum configuration for a router, there can be more, based the number of ports it has and no. of different networks connected to them

IP Datagram Forwarding within the LAN contd.

RV UNIVERSITY
Go, change the world

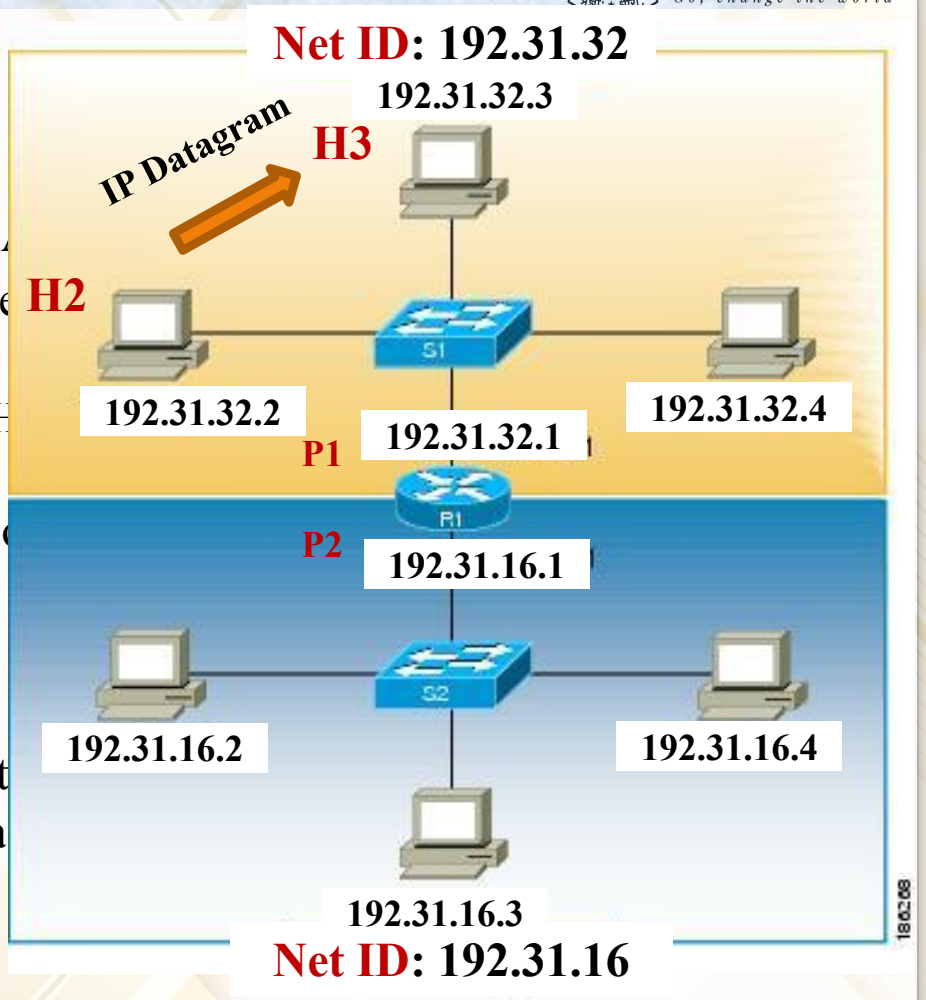
- LAN or the same network means the hosts on that network are all connected to the same physical broadcast medium
- Any L2 message on it will be received by all the hosts on it
- For H2 to send the IP datagram over the L2 layer, it should know the MAC address of H3
- The protocol used is **ARP** (Address Resolution Protocol)
- H2 uses ARP to get the MAC address of the destination host (H3) on the same network



Let us see .. What is **ARP**

IP Datagram Forwarding within the LAN

- There are two **Class C** networks connected by router
- First, let us see how an **IP datagram** is **exchanged** between two **Hosts** on the **same L**
- Assume, H2 receives data from the layer above be sent to H3
  - **Assume** H2 knows the IP addresses of its own (H and of H3
- First, H2 should check whether the host H3 is the same network or not, from the H3's IP address
- How can it find that?
- If the Net ID of H3's IP address is same as Net of H2's own IP address, then both are in the **sa LAN or same network**



What else should H2 know to send the IP datagram to H3? **Let us see ..**

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

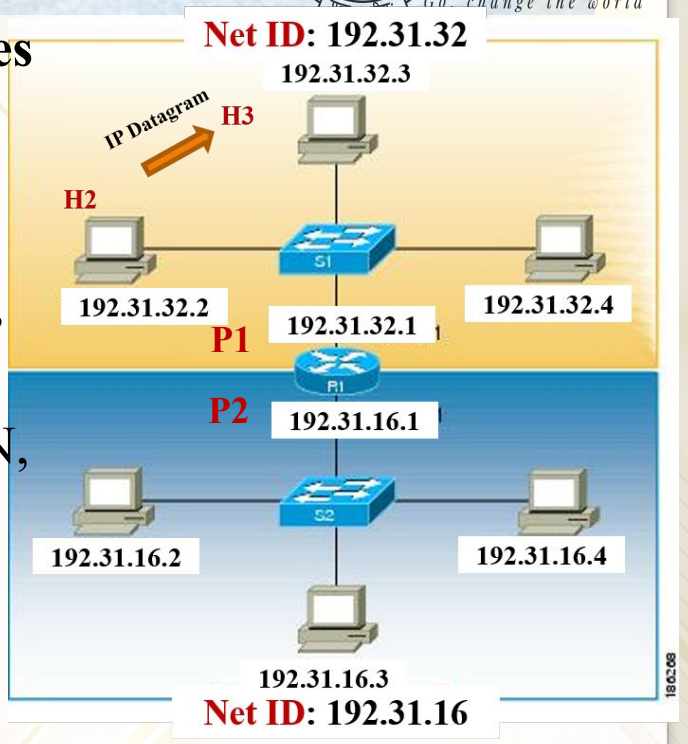
Address Resolution Protocol (ARP)

Ref1 read section on ARP:

ARP: How does it work?

RV UNIVERSITY
Go, change the world

- Every host maintains a table which **maps IP addresses** of the hosts in the LAN network and their **MAC addresses,** called **ARP cache**
- It is called ARP Cache because the mappings can change because the **IP addresses allotted** to the hosts are **dynamic. We will study this shortly**.
- H2 sends an **ARP Query** as a broadcast over the LAN, with target IP as H3's. H2 also shares its own IP and MAC addresses in the message.
- All the hosts on the LAN receives the **ARP query** including H3. Other hosts can also learn about H2.
- When H3 sees its IP address as the **target IP** in the query, **H3 responds** back with **its MAC address**, in a **ARP response** message to H2
- H2 **updates** its **ARP cache** with the value of H3's MAC address and sends the IP packet over LAN

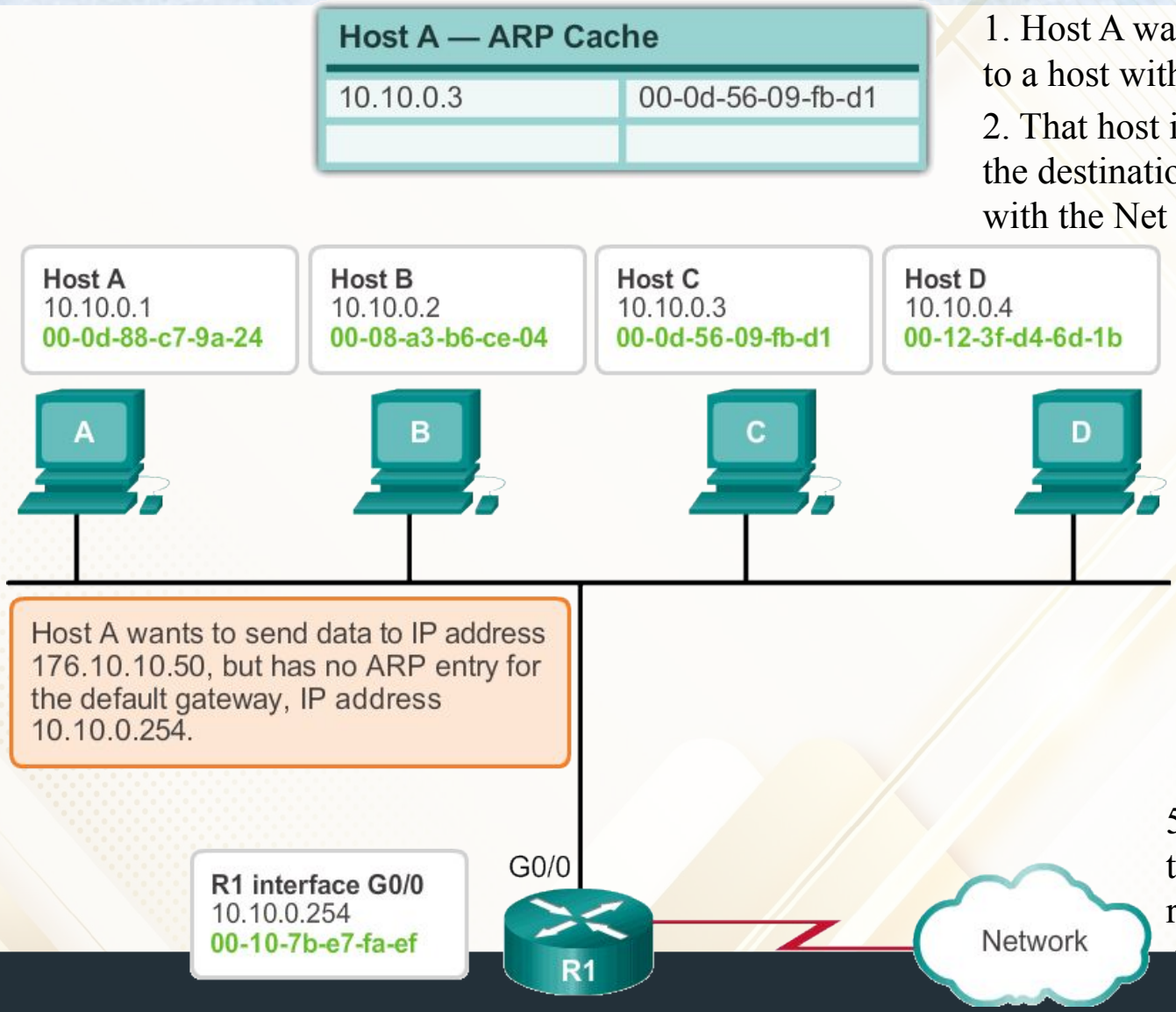


While H2 learns about H3's MAC address, H3 also updates its ARP cache with H2's MAC address, because when H3 receives IP packet from H2 it may have to reply back to it

Additional Points on ARP

- Since the mapping between IP address and MAC address can change over time, the ARP cache entries in each host need to be timed out periodically or removed
  - This happens in the order of every 15 minutes.
- Whenever there is an ARP query broadcast message, all the hosts in the network receive it
- Only the host whose IP address matches the target IP address of the query, responds with its own MAC address
- Other hosts in the network, may refresh the entry in their ARP cache, if they do have an entry for the ARP query sender's IP address
  - This delays the timeout for the removal of that entry from the ARP cache
- Entries created by ARP query are called **dynamic**. There are other statically created entries too in the ARP cache

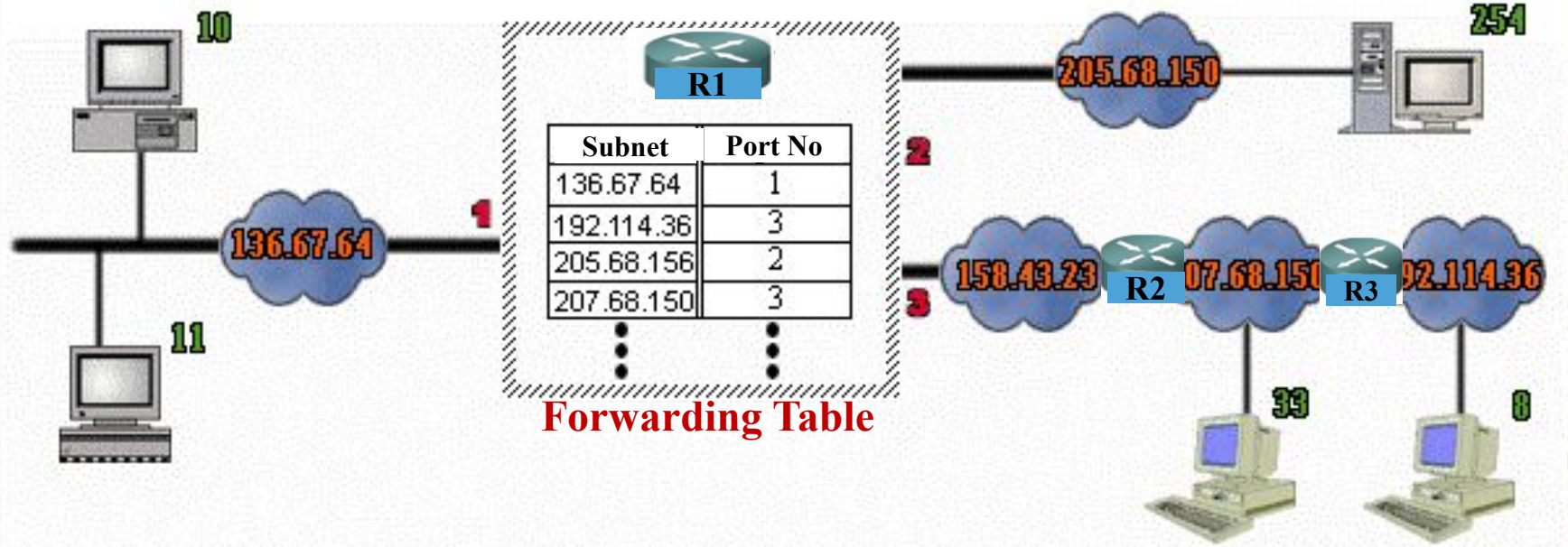
Example: ARP Query and Response with Router



1. Host A wants to send an IP packet to a host with IP 176.10.10.50.
2. That host is not on the same network, the destination Net ID is not matching with the Net ID of LAN, where Host A is part of.
3. Host A needs to send that IP packet to the default Gateway which Will route that packet to the destination IP.
4. Host A needs to know the MAC address of the router to send the IP packet to it
5. Host A uses ARP to find the MAC address of the router which is also in the same Network (10.10.0.254)

Quiz 1: Inside an IP Router

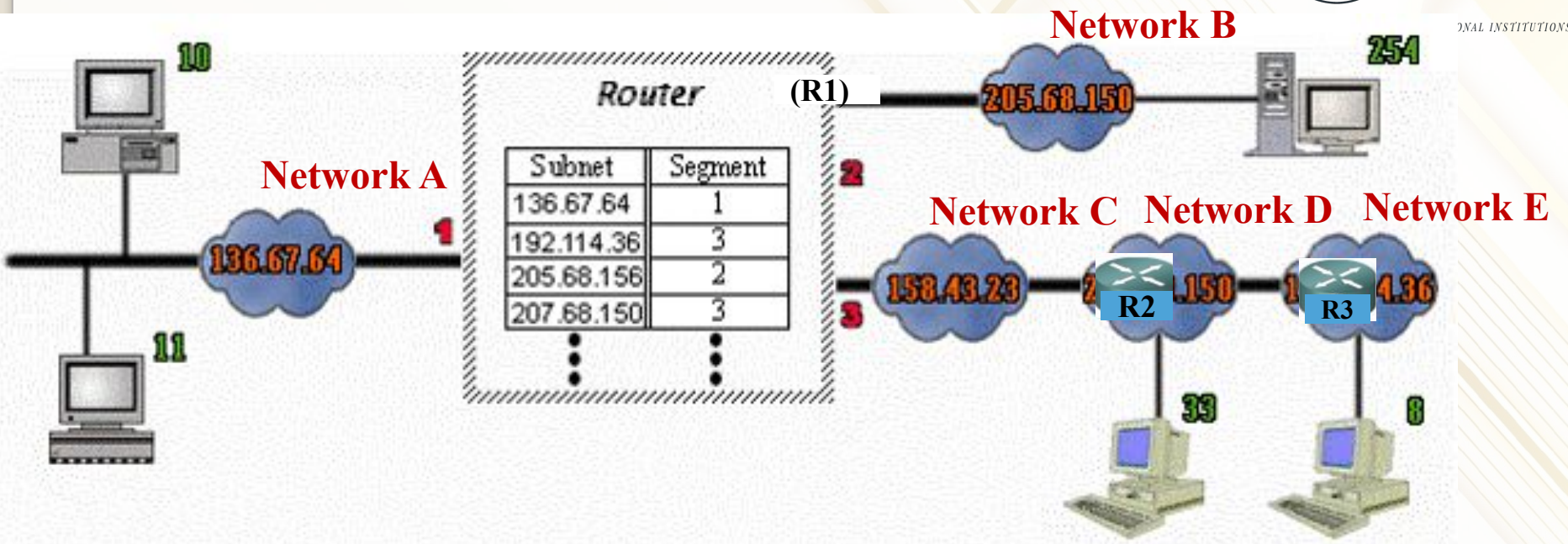
Note: You are **yet to learn** about **Subnet**. It is an extension to **Net ID**, it will be **covered soon**.



- How many LAN networks are there? **5 LANs**
- How many routers are required to connect them all? **Router 1 (R1) is already shown, apart from R1, 2 more are needed. R2 and R3**

- How many ports does R1 have? **3 ports and R1 is connected 3 LANs**
- How many ports are there in R2 and R3? **2 ports each**

Quiz 2: Find the Hop Distances



Hop Distances	Network A	Network B	Network C	Network D	Network E
Network A	0	1	1	2	3
Network B	1	0	1	2	3
Network C	1	1	0	1	2
Network D	2	2	1	0	1
Network E	3	3	2	1	0

Special IP addresses

RV UNIVERSITY
Go, change the world

Special IP Addresses	Description
0.0.0.0	Refers to the **default route**. This route is to simplify routing tables used by IP.
127.0.0.0	Reserved for **Loopback**. The Address 127.0.0.1 is often used to refer to the **local host**. Using this Address, applications can address a local host as if it were a remote host.
IP Address with all **host bits** set to "**0**" **192.168..72.0 (class C)**	Refers to the actual network itself. For example, network 192.168.72.0 (Class C) can be used to identify network 192.168.72. This type of notation is often used within routing tables.
IP Address with all **node bits** set to "**1**" (Subnet / Network Broadcast) e.g: **192.168.72.255**	IP Addresses with all **node bits** set to "**1**" are local network broadcast addresses and must **NOT** be used. Some examples: **125.255.255.255** (**Class A**) , **190.30.255.255** (**Class B**), **203.31.218.255** (**Class C**).
IP Address with **all bits** set to "1" (Network Broadcast) e.g **255.255.255.255**	The IP Address with all bits set to "1" is a broadcast address and must **NOT** be used. These are destined for all nodes on a network, no matter what IP Address they might have.

Host IP allocation

Host IP address allocation: Requirements

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Each host on a network needs to get an IP address for it to be able to communicate with other machines on the network
- What are the **requirements** to be taken care of while **allocating IP addresses to hosts**

1. Each host needs to have a **globally unique** IP address, no duplicate allocation
2. The **network hierarchy** needs to be taken care of. That means all the hosts on a particular LAN need to have their **Net IDs** same as that of the network they are part of.
3. If the IP addressing scheme being followed is **classful**, **correct class addresses** are to be allotted
4. **Invalid Host IDs** and **IP addresses** should **not** be **allotted**

Host IP address allocation:
Issues with Manual Configuration

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- If **network administrators** go around to configure the IP addresses manually on all machines, the **issues** would be:

1. **Time consuming** task
2. A host cannot be on the network as soon as it is switched on. It **needs to wait** for the network administrator to configure its IP address before it can start communicating over the network
3. **Error-prone**. Human error is possible, with so many hosts are to be configured, each with unique IP addresses.
   - Duplicate IP addresses will make the hosts to misbehave
4. When the machines fail and reboot, they need to be configured again.
5. Manual configuration is **not scalable** when the network is spread over different sites and buildings.
6. IP addresses cannot be reclaimed easily when the machines shutdown or go offline

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Dynamic Host Configuration Protocol (DHCP)

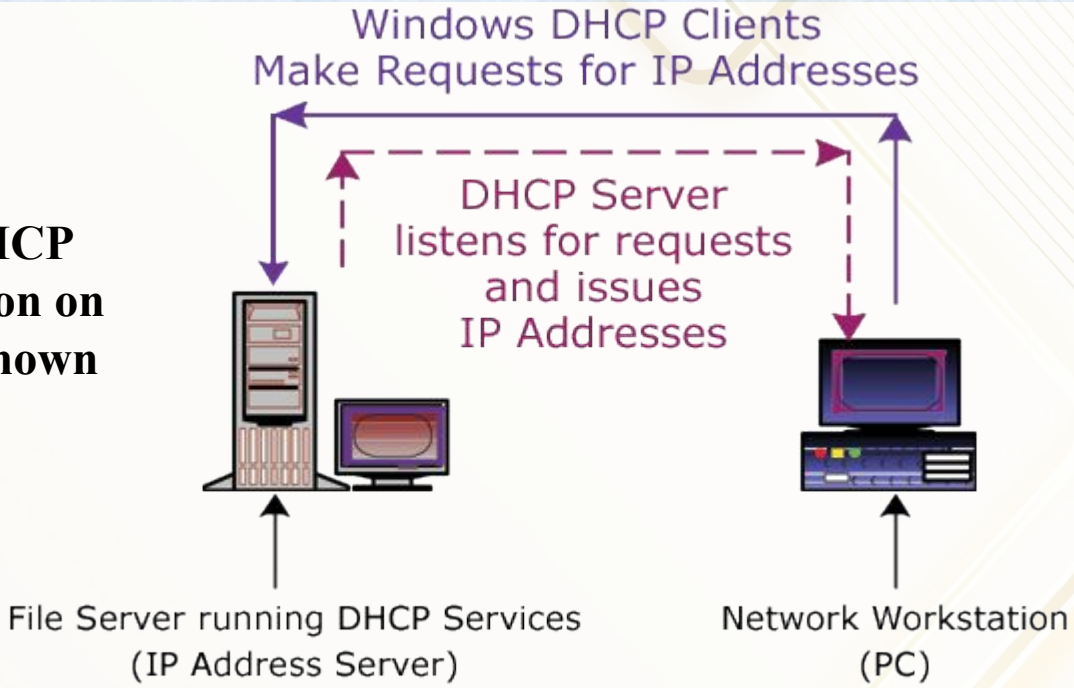
Read Ref 1: Section on DHCP:

Host IP address allocation: Solution

DHCP

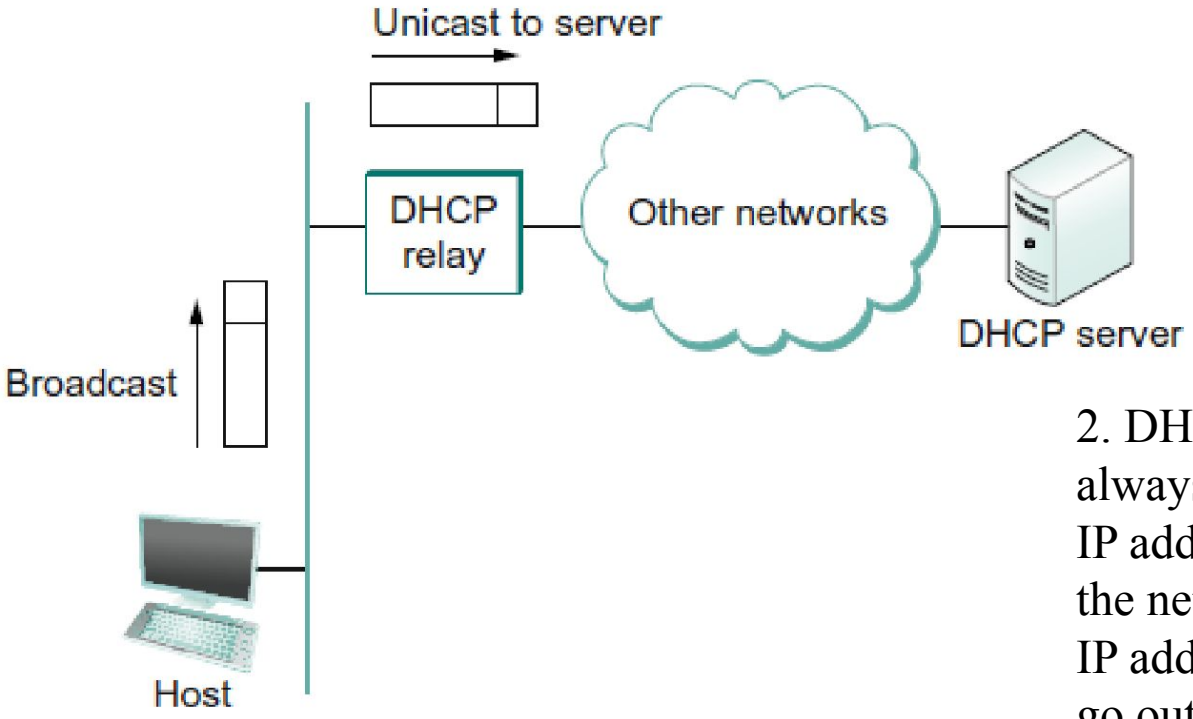
RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Example DHCP Implementation on Windows is shown



- Dynamic Host Configuration Protocol (DHCP) is a **client/server protocol** that automatically provides an Internet Protocol (IP) host with its **IP address**, and
  - Other related **configuration information** such as the **subnet mask (for classless scheme)** and
  - **Default gateway** or **default router's IP address**.
- This protocol is initiated by the host while booting up, for joining the network it is physically connected to

DHCP: Network Configuration



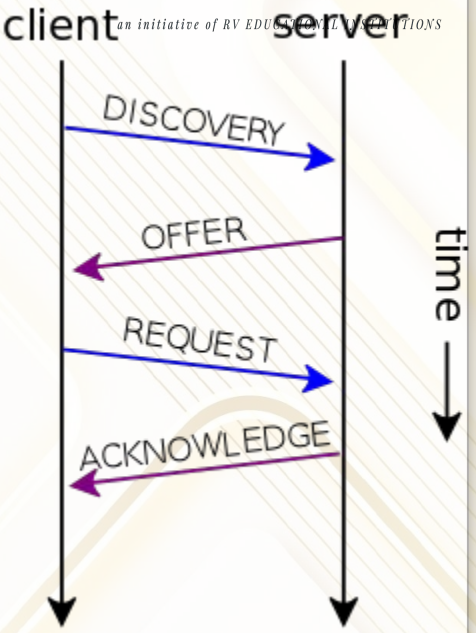
1. The network Administrator is responsible for providing the DHCP server with the **pool of IP addresses** for it choose from

2. DHCP server must be running always to take care of allocating IP addresses to the hosts joining the network. Reclaiming the IP addresses when the hosts go out the network

- This shows the configuration of a network with **DHCP server** and a **relay agent** to implement DHCP for IP address allocation
- Each LAN network has one such configuration to allot IP addresses to different hosts in its network based on the available IP addresses it has received from ICANN

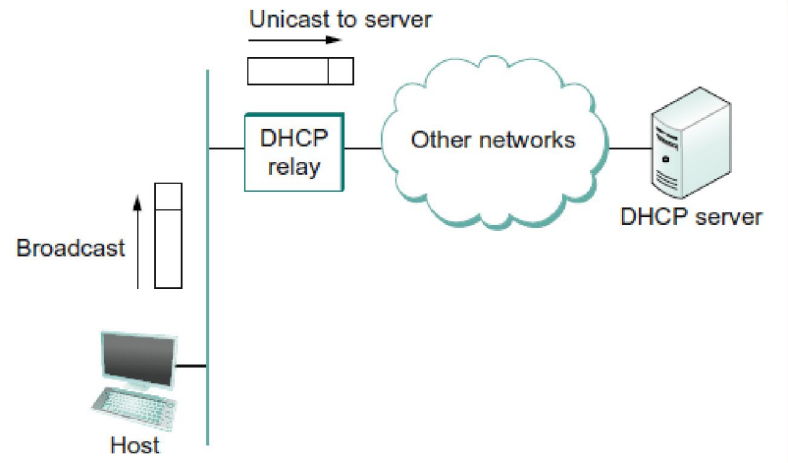
DHCP Server Discovery

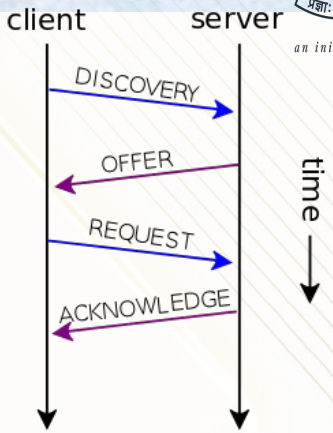
- Since the **goal of DHCP** is to **minimize** the amount of **manual configuration** required for a host to function
- It would rather defeat the purpose if each host had to be configured with the **IP address of a DHCP server**.
- Thus, the **first problem** faced by DHCP is that of **DHCP server discovery**



- To contact a DHCP server, a newly booted or attached host sends a **DHCPDISCOVER** message to a special IP address (255.255.255.255) that is an IP broadcast address
  - Which needs to be sent over an Ethernet Broadcast frame for all the hosts and routers in the network to receive this message including the DHCP Server
- Routers do not forward such packets onto other networks, preventing broadcast to the entire Internet

DHCP: Relay Agent





- The server would then reply to the host that generated the discovery message
  - All the other nodes would ignore it
- However, it is not really desirable to require one DHCP server on every network,
  - Because this still creates a potentially large number of servers that need to be correctly and consistently configured
- Thus, DHCP uses the concept of a ***relay agent***.
- There is at least one relay agent on each network, configured with just one piece of information, the **IP address of DHCP Server**

DHCP Lease of IP Address

- In the case where DHCP dynamically assigns IP addresses to hosts, it is clear that hosts cannot keep addresses indefinitely
- As this would eventually cause the server to exhaust its address pool.
- At the same time, a host cannot be depended upon to give back its address, since it might have crashed, been unplugged from the network, or been turned off.
- Thus, DHCP allows addresses to be leased for some period of time.
- The **DHCP lease** is how long a device reserves an IP address on its network without a renewal request from it
- Once the lease expires, the server is free to return that address to its pool.
- A host with a leased address clearly needs to renew the lease periodically if in fact it is still connected to the network and functioning correctly.
- In a home router, the lease time is set for about 24 hours
  - Some ISPs set 8 hour leases, some may set it for even for a week!

Quiz 1: DHCP and IP Protocol Suite

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Answer the questions below:

- **Q1:** What is the **correct order of execution** of **these events** or **running of protocols** in a **host** which has just **booted up?** Note that they need to **run without** any **errors**:
  - A. PING
  - B. DHCP
  - C. ARP
  - D. NIC HW initialization

  ANS: D □ B □ C □ A

- **Q2:** Suppose **DHCP server** is **down** in a network, then hosts on the network:
  - A. Can communicate over the network without any problems, though DHCP Server discovery would have failed.
  - B. The hosts cannot receive any IP packets from other networks but it can continue to communicate with other hosts on its network over IP
  - C. The hosts can send Ethernet frames and broadcasts but they cannot communicate over IP layer

    ANS: C

    Note: Without having it own IP address, a host cannot communicate over IP layer at all.
  - D. None of the given options are correct

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Internet Control Message Protocol (ICMP)

Read the Section on ICMP:

ICMP: Introduction

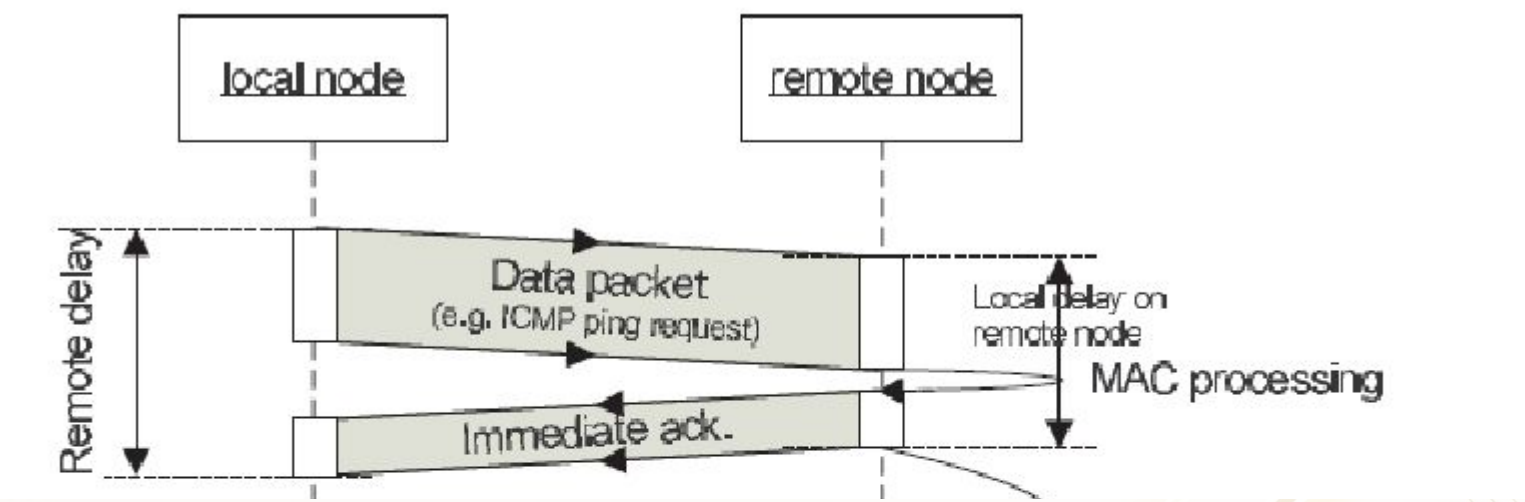
- ICMP defines a collection of **error messages** that are **sent back** to the **source host** whenever a **router** or **host** is **unable to process** an **IP datagram** successfully.
- **ICMP** defines **error messages** indicating that
  - The **destination host is unreachable** (perhaps due to a link failure), or
  - The **reassembly process failed,**
  - The TTL had reached 0,
  - The IP header checksum failed, and so on.
- Since IP protocol is unreliable, these ICMP messages help the **sending host** to take **corrective actions** based on these error messages

ICMP: Control Messages

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

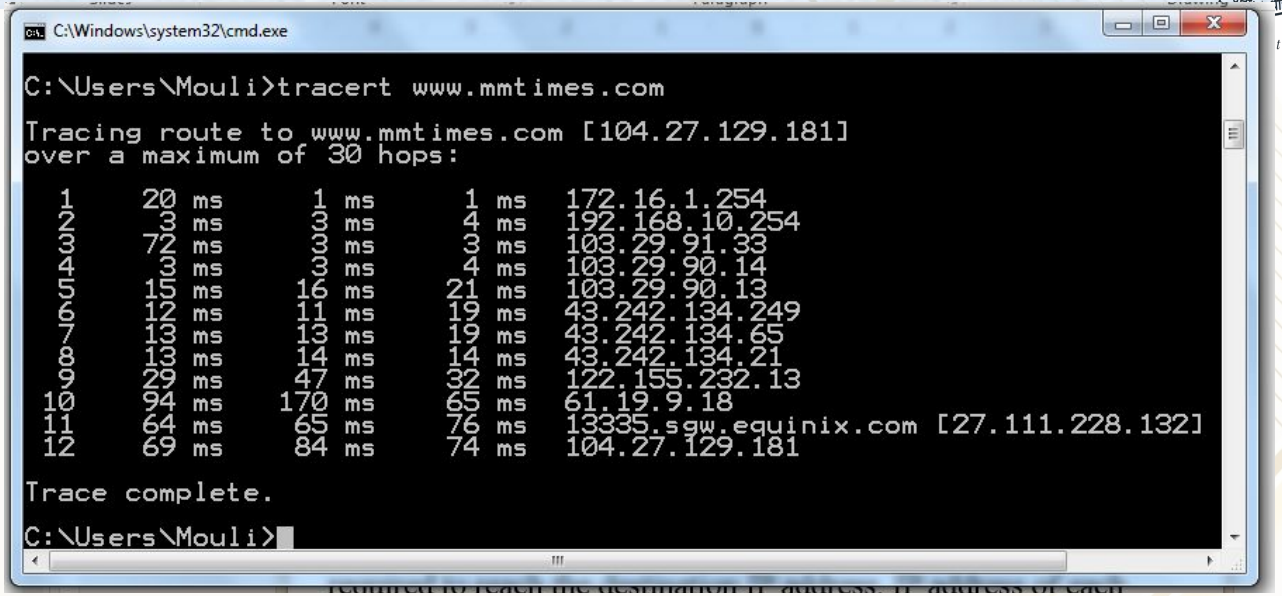
- ICMP also defines a handful of **control messages** that a **router** can **send back** to a **source host**.
- One of the most useful control messages, called an **ICMP-Redirect**, tells the source host that there is a **better route** to the **destination**.
- ICMP-Redirects are used in the following situation.
- Suppose a host is connected to a network that has **two routers** attached to it, called **R1** and **R2**, where the **host** uses **R1** as its **default router.**
- Should R1 ever receive a datagram from the host, where based on its **forwarding table** it knows that **R2** would have been a **better choice** for a particular destination address,
- **R1** sends an ICMP-Redirect back to the host, instructing it to use R2 for all future datagrams addressed to that destination.
- The host then adds this new route to its forwarding table

ICMP: Ping in Action



- **Ping** is a computer network administration software utility used to test the reachability of a host on an Internet Protocol (IP) network
- It measures the **round-trip time** for **messages** sent from the **originating host** to a **destination computer** that are echoed back to the source
- Ping uses **ICMP protocol** to communicate over IP layer

ICMP: Tracert in Action



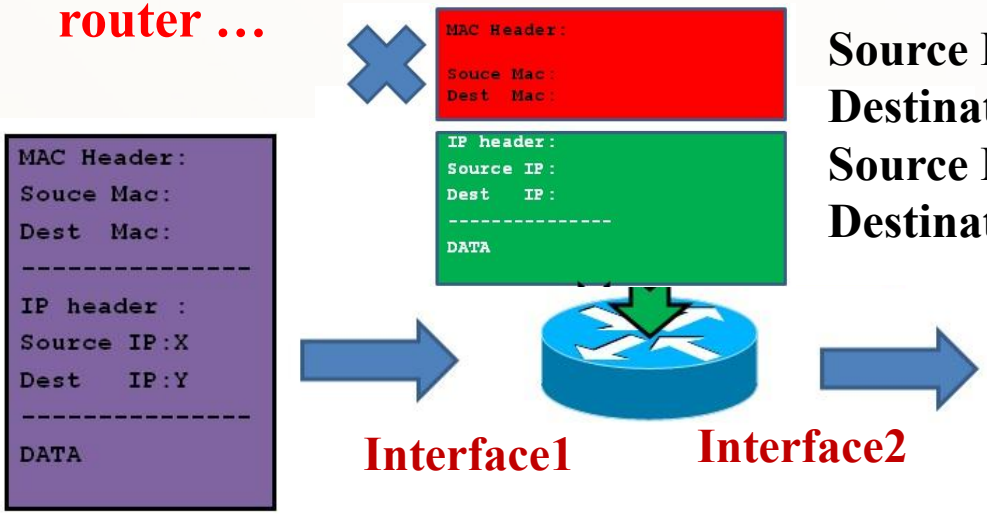
- A **traceroute** is a **network tool** used to **show the route** taken by packets across an IP network using ICMP.
- The Traceroute tool will shows each hop sequentially, and total hops required to reach the destination IP address. IP address of each router is hop is also shown on each line
- Traceroute sends out **three packets**. Each column corresponds to the time is took to get one packet back (**round-trip-time**)

What happens inside a Router?

Ref1 read section on Subnetting:

1. What happens inside a Router?

- What happens inside a router on receiving a frame on one of its interface, before it forwards on one of its other interfaces?
- **Let us understand closely, every step of processing that happens within a router …**



Source IP: x — **IP of Source Host**
Destination IP: y — **IP of Destination Host**
Source MAC: — **MAC addr of Host**
Destination MAC: — **MAC addr of Interface1**

Let us assume this is the **first hop router**
From the source: Source host's **Default Router**

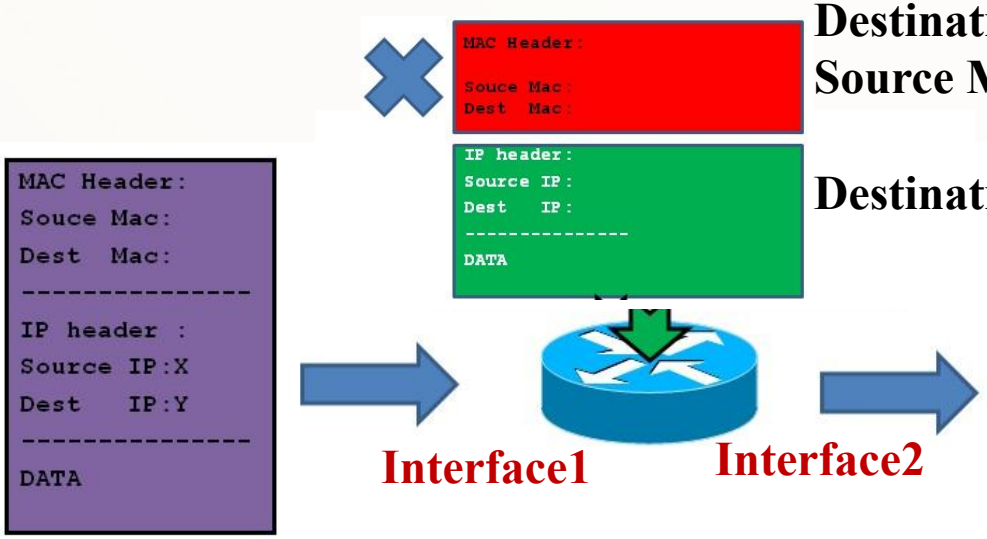
Processing steps at Router

1. L2 of R1 receives the frame
2. If erroneous, rejects the frame
3. Looks at destination MAC to see if it is it's own MAC
4. If not, it ignores the frame
5. If yes, it accepts the frames and passes it to L3 (IP layer) within the router (another task or a function) running. At this moment the **L2 frame is removed from the packet**.
6. L3 looks at the destination IP
7. If the dest IP address is matching with one of its interfaces, it is meant for one of the hosts on that network to which the router is directly connected to, through an interface.

2. What happens inside a Router?

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Let us continue …



Source IP: IP of Source Host

Destination IP: IP of Destination Host

Source MAC: MAC addr of this router's interface 2 through which frame is going to be sent out

Destination MAC: Diff MAC addr based on routing decision

9. If the TTL becomes zero, it does not forward it further. It builds A ICMP error echo reply message to the original source IP host, if it is ICMP packet. (not for all IP packets)

10. It now, prepares the L2 frame for ICMP, with the destination MAC address of the source machine which is on the network through which it came. sends that ICMP back to the Src host.

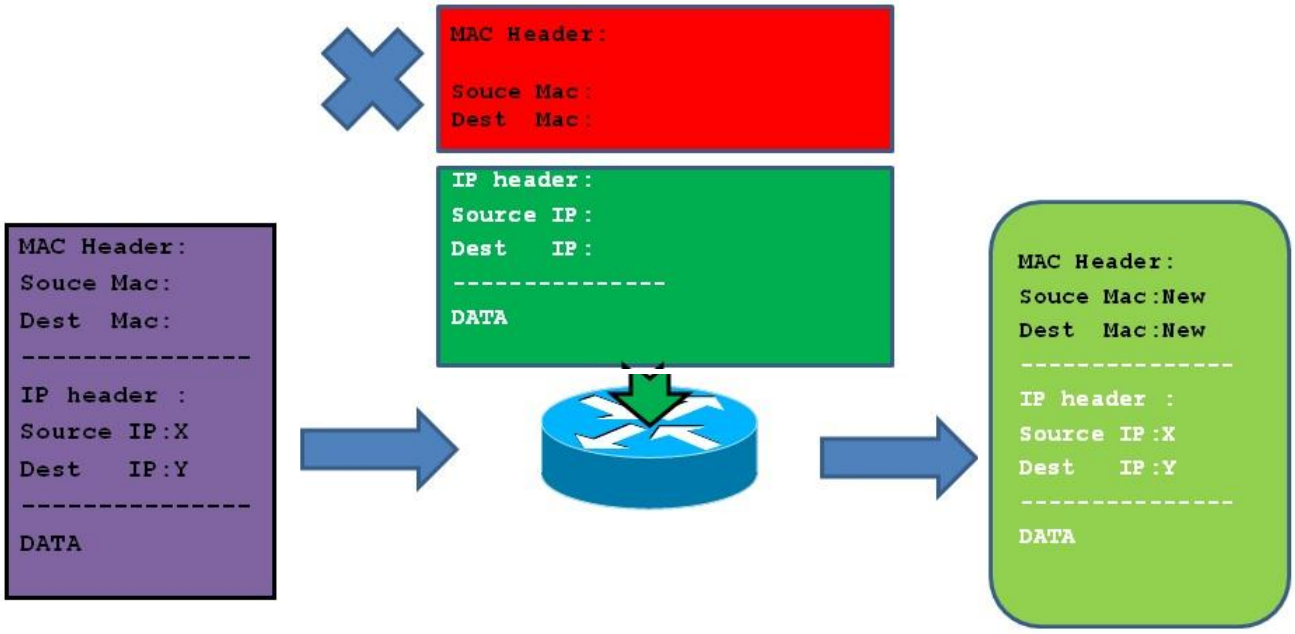
Let us assume this is the **first hop router**

From the source: Source host's **Default Router**

11. Note that router does not modify the Source and destination IP address in the IP header. But it decrements TTL by one.

12. If IP pkt is not dropped and the destination IP on the network connected to say, Interface 2, the following happens router builds L2 header with the source MAC as its own Interface 2 and the destination host's MAC as destination MAC, keeps the IP Packet as payload of L2, sends on the network through the Interface2

3. What happens inside a Router?



Note that router does not modify the source and destination IP addresses of the packet generated by the original source host.

13. If the destination IP host is not on Network where Interface2 is connected to, then the IP packet has to travel further to reach the destination.

14. Router, based on the routing table entry, IP packet is sent to either the next hop Router to which this router is connected to, through one of its interfaces. If there is no entry found in the table specific to the destination IP address, it needs to be sent to default router on one of itIts interfaces.

15, whatever be the next router, it knows its IP address, it uses ARP, if it does not know the MAC addr of that router, it builds L2 packets and sends it on the relevant interface.

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Subnetting

Ref1 read section on Subnetting:

The problems with Classful Addressing

(1. Inefficiency in Address Assignment)

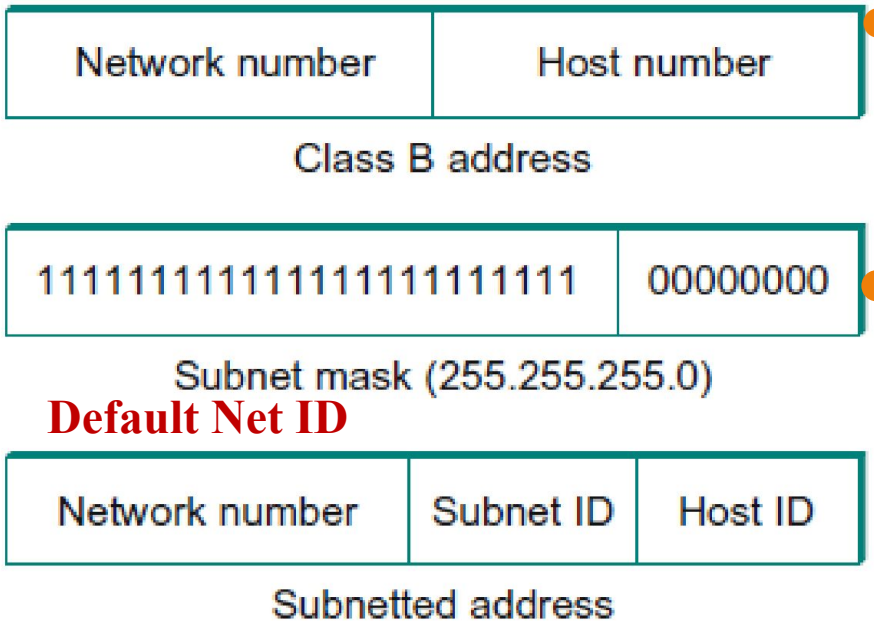
- The original intent of IP addresses (classful) was that the **network part** would **uniquely identify** exactly one **physical network**.
- It turns out that this approach has a **couple of drawbacks.**
- Imagine a **large campus** that has **lots of internal (small) networks** and decides to **connect** to the **Internet**.
- For **every network**, no matter how small, the site **needs** at least one **class C network address**.
- Even worse, for **any network** with **more than 254 hosts,** they need a **class B address**
- But there are only a **finite number** of **network numbers**, and there are **far fewer class B** addresses **than class Cs**.
- **Class B** addresses tend to be in particularly **high demand** because you never know if your network might **expand beyond 254 nodes**
  - The **problem** we observe here is **address assignment inefficiency**

The problems with Classful Addressing ... Contd.

(2. Increased no. of entries in the Routing Table)

- Assigning one network number per physical network, therefore, uses up the IP address space potentially much faster than we would like.
- While we would need to connect over 4 billion (2^{32}) hosts to use up all the valid addresses, we only need to connect 2^{14} (about 16,000) class B networks before that part of the address space runs out.
  - Therefore, we would like to **find** some **way** to **use** the **network numbers more efficiently**
- Assigning many network numbers has **another drawback** that becomes apparent when you think about **routing table entries**
- Each router needs to have an entry in its table to route the packets towards, each unique Net ID, i.e., every physical network in Internet
- Thus, the **more network numbers** there are **in use**, the **bigger** the **forwarding tables get**
  - **Bigger routing tables** increases **costs of routers**, **more memory** and **increased search time**, thus needing **powerful processors**

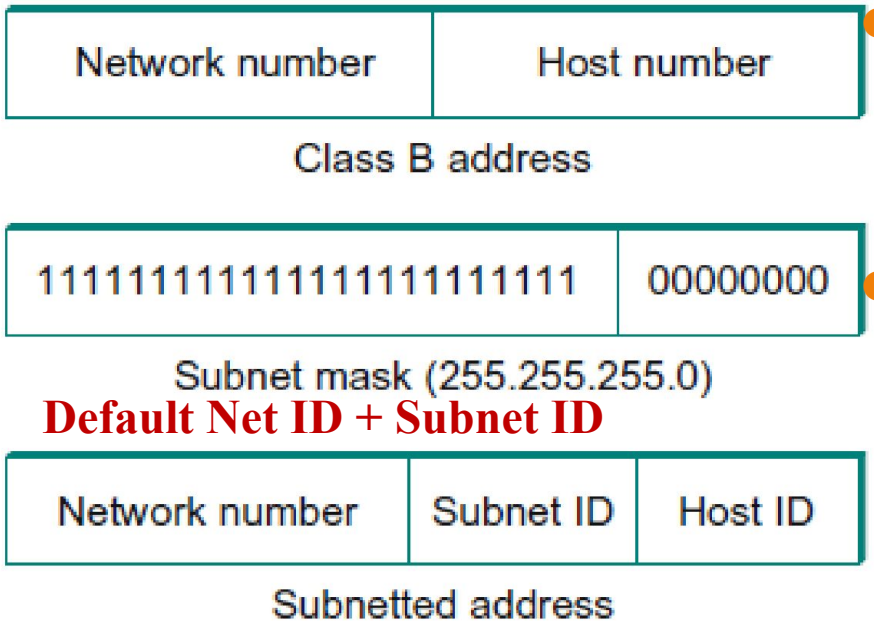
Solution: Subnetting: Subnet ID



- In the **subnet addressing system**, the **two-tier, network** and **host** division of the IP address is made into
- **Three-tier system** by **taking some number of bits** from the **host ID's** of **Class A, B, or C addresses** and **using them** for a **subnet** identifier (**subnet ID**).

- The Net ID part of the classful addresses is called **default Net ID**
- For example, for a class A, the **default Net ID** is 8 bits wide, similarly for Class B, 16 bits wide, Class C, 24 bits, and so on.
- In subnet addressing, a part of the host ID (from the MSB side of host ID) is taken away for identifying **subnets** and leaving only the remaining bits for Host IDs

Subnets: Physical Networks



- Now, each **physical network** is **identified** with a new **unique Net ID** which is a **combination** of **default Net ID + Subnet ID**
- All the subnets of an organization will have the same default Net ID but a new unique Net ID by having different Subnet IDs

Note that Subnet ID Is local and understood within the organization. Outside, it is all single network as per Default NetID

- Several things need to be done to make this work.
- First, the **subnets** should be **close to each other**, **physically**.
- This is because at a distant point in the **Internet**, they will all look like a **single network,** having **only one default net ID** among them
- This means that a routers in the Internet will only be able to select one route to reach any of the subnets, so they had better all be in the same general direction –

Advantage: only one entry for all subnets!!!

Quiz 1: Identify the Class of the IP address

- Class of the IP address 110.11.11.11 is:

A. Class A

B. Class B

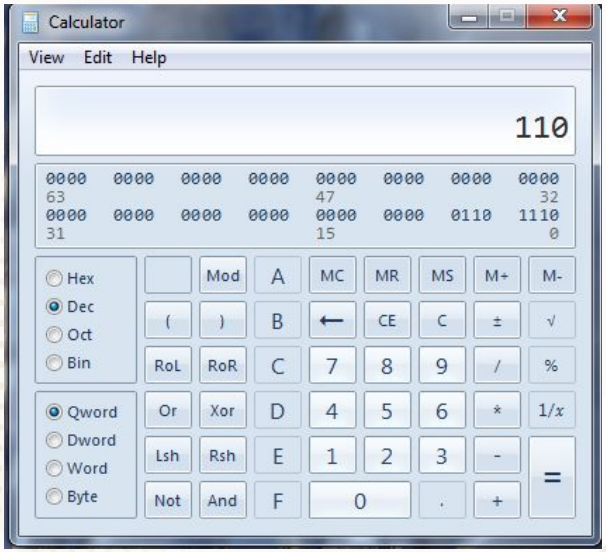
C. Class C

D. None of the given options are correct

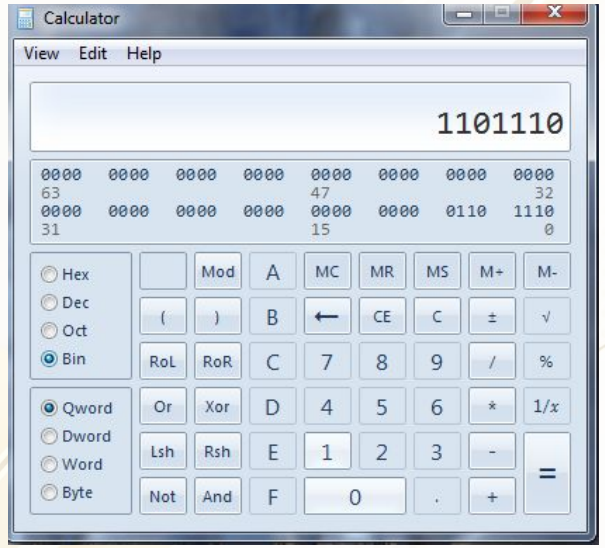
Ans: A

Note that the Binary representation on the calculator is of 7 bits, the 8 bit value is 0110 0101 □ Class A Moreover the decimal Value 110, is less than 128, so this IP address is Class A and not Class C!!!

Clue:



Decimal Form



Binary Form

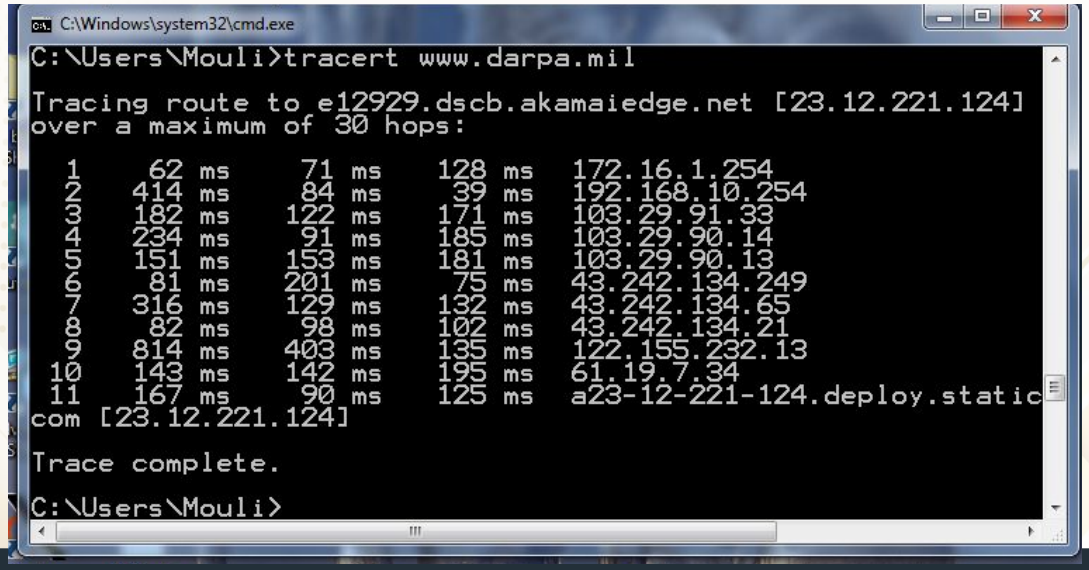
Remember the IP addresses are given as dotted decimal numbers, never in binary form.

Quiz 2: Default Router

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- From the output of **tracert** command below, identify the **default router** of the **source host**:

A. 23.12.221.124
B. 172.16.1.254
C. 192.168.10.254
D. None of the given options are correct



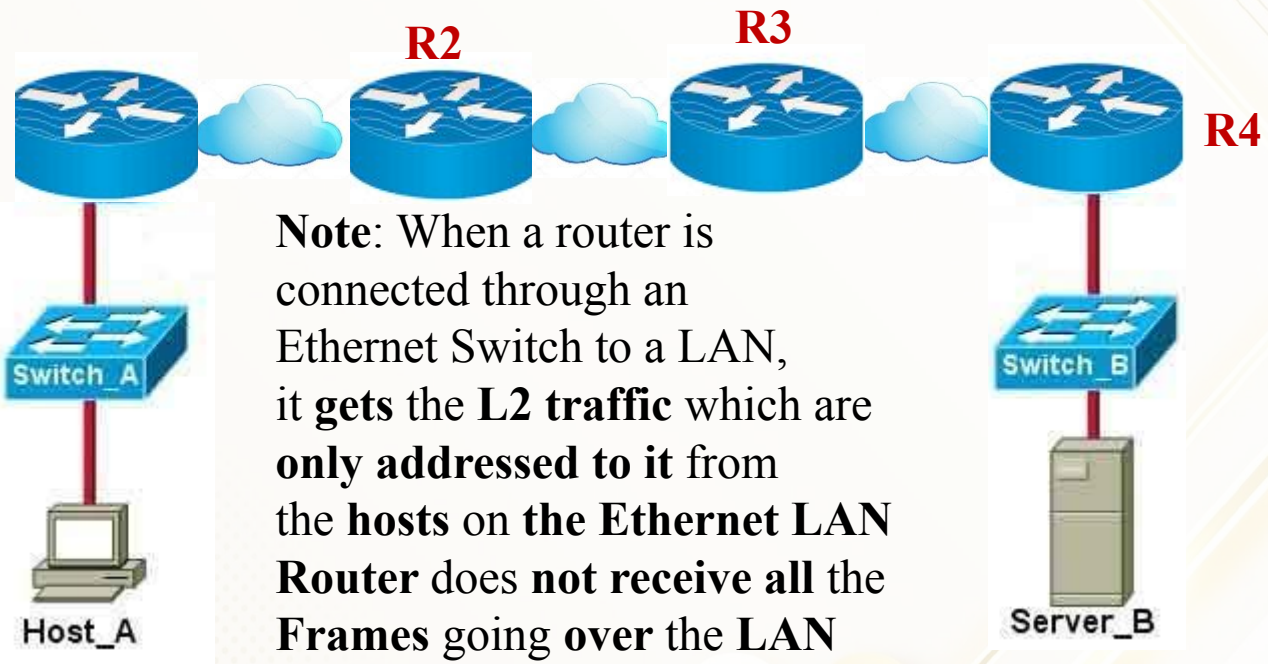
Ans: B

The **first hop router** in the **tracert** command corresponds to the **default router** of the sending host (**source**) which is **172.16.1.254**
The IP address **23.12.221.124** is the destination **IP address** of web server hosting the web site**: www.darpa.mil**

Ref: what is .mil domain name?
DARPA: Defense Advanced Research Project Agency, **where** the **Internet was born**.

Quiz 3: MAC addresses through Tracert

- Can you get the intermediate router's MAC addresses with the help of **Tracert** command and by using **Wireshark** at the **source host**?



Note: When a router is connected through an Ethernet Switch to a LAN, it **gets** the **L2 traffic** which are **only addressed to it** from the **hosts** on **the Ethernet LAN Router** does **not receive all** the **Frames** going **over** the **LAN**

It is possible, only when Wireshark is run on all the intermediate networks to sniff the replies coming from each router back to Host A or the IP pkt going from HostA to each router.

tracert 172.22.33.34 **IP: 172.22.33.34**

Ans: Not possible with tracert. Because when the replies come from each router, the source and destination MAC addresses keep changing on every hop. Finally when the reply reaches the host A, the L2 frame will only have R1's MAC as the source MAC address, and the Host A's MAC address as the Destination MAC address.

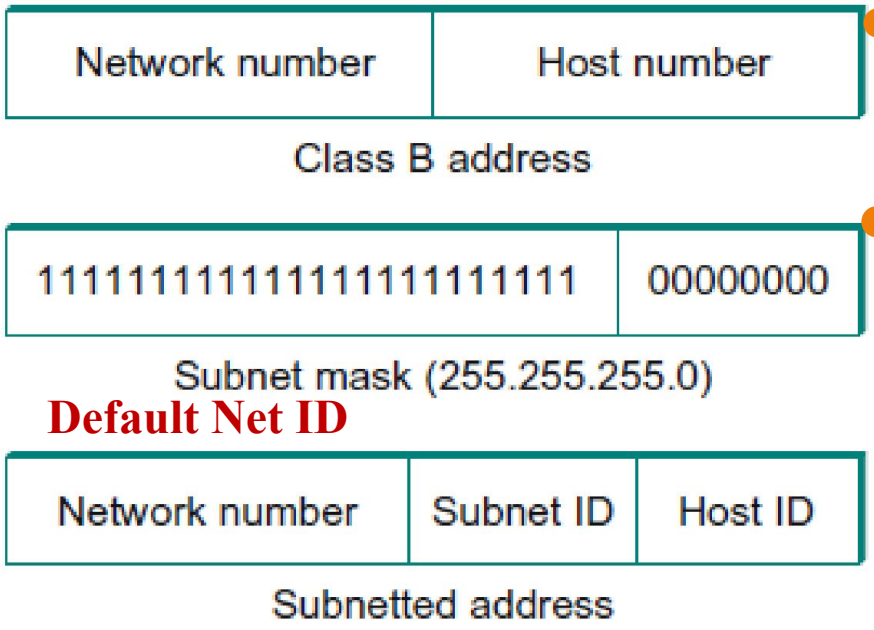
Quiz 4: Different IP addresses for the same Website

- tracert www.yyy.com □ IP address. 133.232.44.55
- tracert www.yyy.com □ IP address: 231.67.5.43
- What do you understand when the same website has different IP addresses?

ANS:

- A Website can have multiple IP addresses when it is **hosted** at **multiple locations**.
- A website can be hosted at different locations on different web servers for **load balancing** or **redundancy**. Or
- To serve the web pages with less latency, based on user's location.
- The DNS (Domain Name System) which is a server maintaining the IP addresses of various domain names (website addresses) maintain different IP addresses based on its location and gives those IP addresses when the browser queries them.

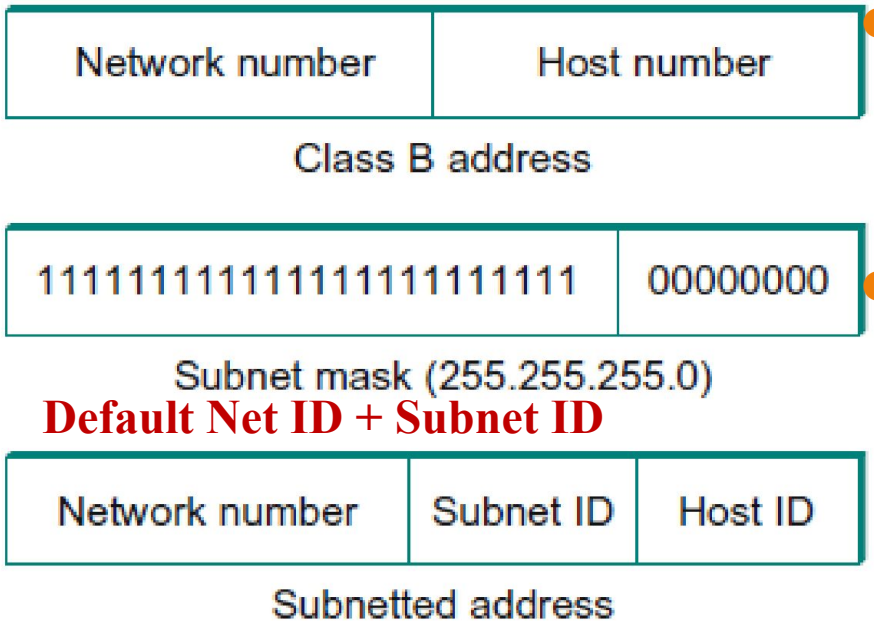
Solution: Subnetting: Subnet ID -recap



- In the **subnet addressing system**, the **two-tier, network** and **host** division of the IP address is made into
- **Three-tier system** by **taking some number of bits** from the **host ID's** of **Class A, B, or C addresses** and **using them** for a **subnet** identifier (**subnet ID**).

- The Net ID part of the classful addresses is called **default Net ID**
- For example, for a class A, the **default Net ID** is 8 bits wide, similarly for Class B, 16 bits wide, Class C, 24 bits, and so on.
- In subnet addressing, a part of the host ID (from the MSB side of host ID) is taken away for identifying **subnets** and leaving only the remaining bits for Host IDs

Subnets: Physical Networks – recap



- Now, each **physical network** is **identified** with a new **unique Net ID** which is a **combination** of **default Net ID + Subnet ID**
- All the subnets of an organization will have the same default Net ID but a new unique Net ID by having different Subnet IDs

Note that Subnet ID is local and understood within the organization. Outside, it is all single Network as per Default NetID

- Several things need to be done to make this work.
- First, the **subnets** should be **close to each other**, **physically**.
- This is because at a distant point in the **Internet**, they will all look like a **single network,** having **only one default net ID** among them
- This means that a routers in the Internet will only be able to select one route to reach any of the subnets, so they had better all be in the same general direction –

Advantage: only one entry for all subnets!!!

Example1: Subnets in an Organization

RV UNIVERSITY
Go, change the world

Network number	Host number

Class B address

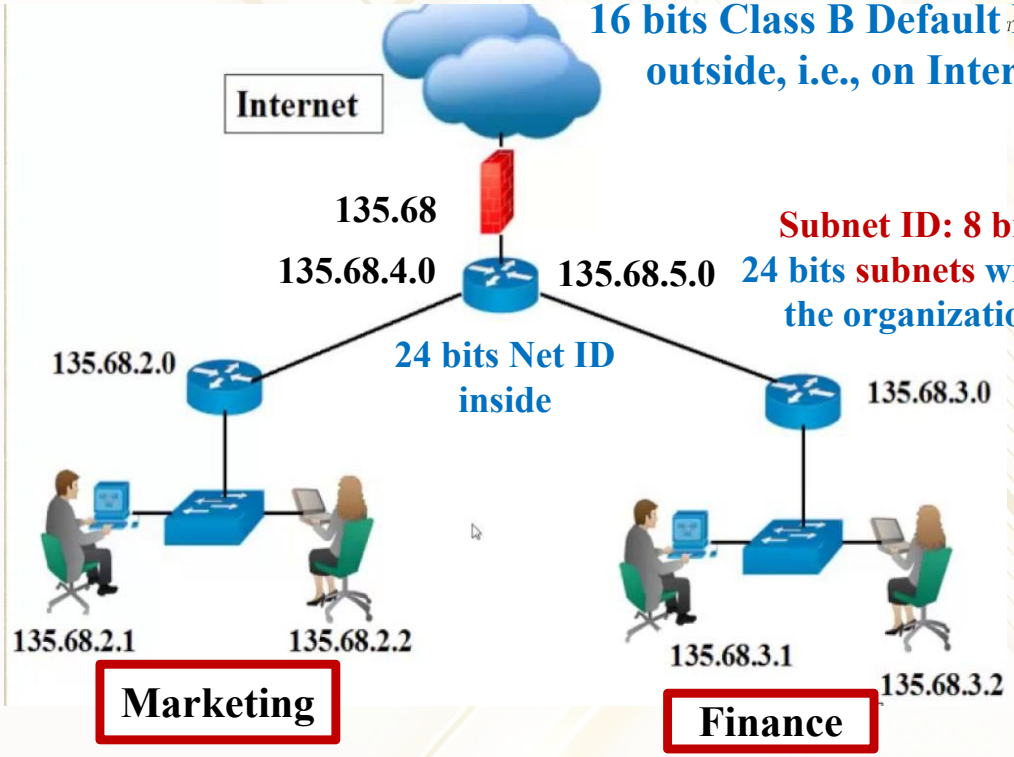
11111111111111111111111	00000000

Subnet mask (255.255.255.0)

Default Net ID + Subnet ID

Network number	Subnet ID	Host ID

Subnetted address



1. What is the **class of IP addresses used here?** **e.g.: 135.68.2.1**

135 □ 0x87 □ 0b10000111

Ans: Class B

- **Default Net ID** of this **organization's network is:** **135.68 (first 16 bits)**
- No. of **physical networks** or **Subnets**: **4**
- Are those **networks** have **different new Net IDs**? **Yes (24 bits)**
- What are the **subnets** here? **135.68.2.0 and 135.68.3.0**
  135.68.4.0 and 135.68.5.0

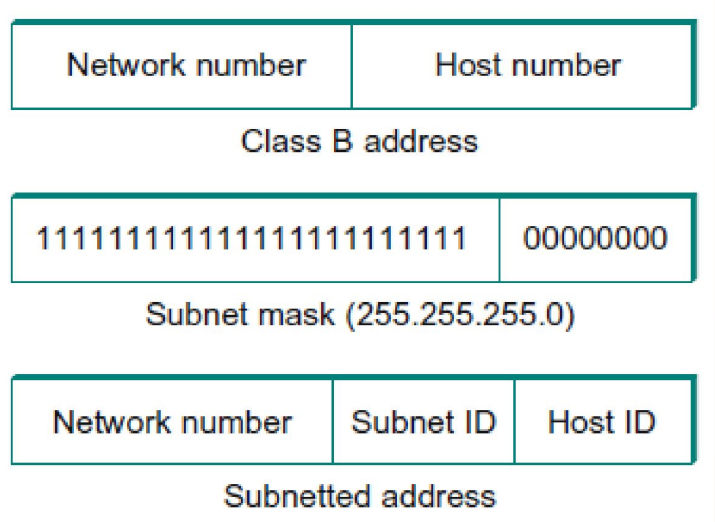
Note: **Routers** within the organization need to be made **aware** of **subnetting**.

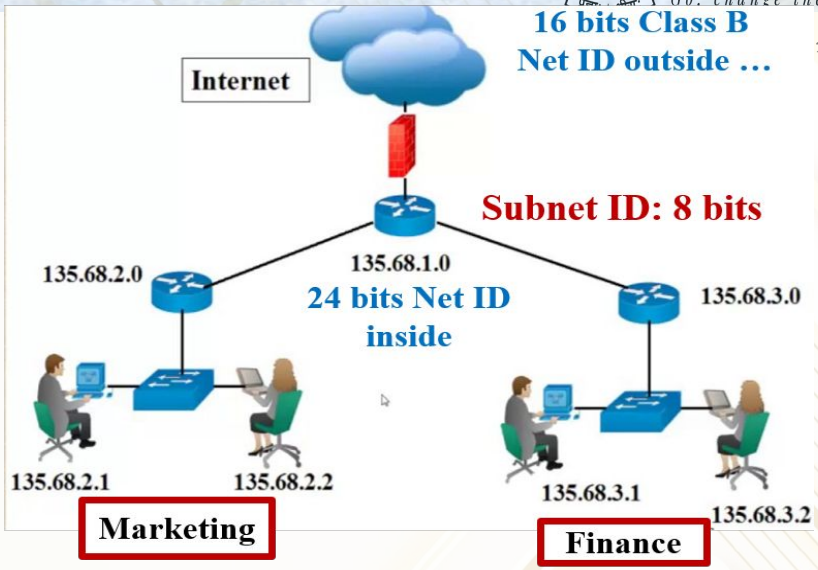
Host ID: Only 8 bits

Subnets have its host ID part all zeros.

Subnetting: Subnet Mask

Subnet Mask here is: 255.255.255.0



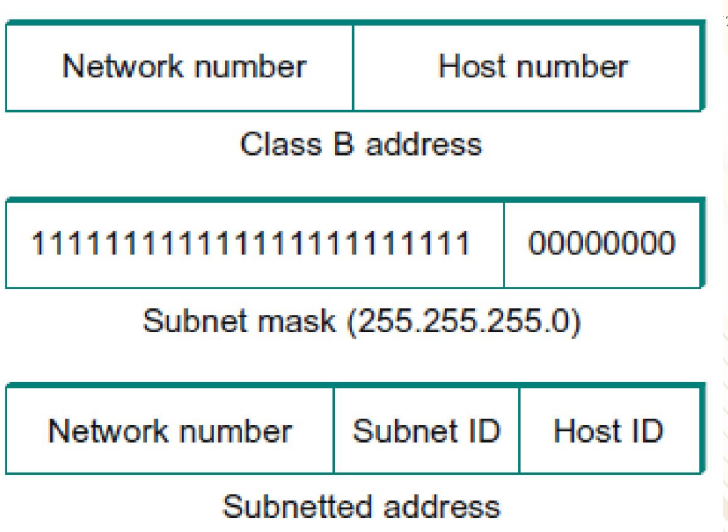


- Now, the requirement that each physical network needs to have an **unique Net ID as per its classful addressing scheme**, is **removed**.
- Here, **both** the **physical networks** have the **same class B default Net IDs**
- Then, routers within the organization need to be made aware that the **Net ID** to be considered for routing decision is not as per classful addressing scheme. It should also **include** the **Subnet ID,** to identify **unique subnet**s.
- A **mask** of **24 bits** (**subnet mask, all 1's**) is to be applied to find if an **IP address** belongs to a **physical network** or a **subnet,** to be **precise**

Subnet Mask: Explained

RV UNIVERSITY
Go, change the world

- **Subnetting** provides a first step to **reducing total number of network numbers** that are **assigned**.
- The **idea** is to take a **single IP network number** and **allocate** the IP addresses with **that network number** to **several physical networks**, which are now **referred** to as **subnets**



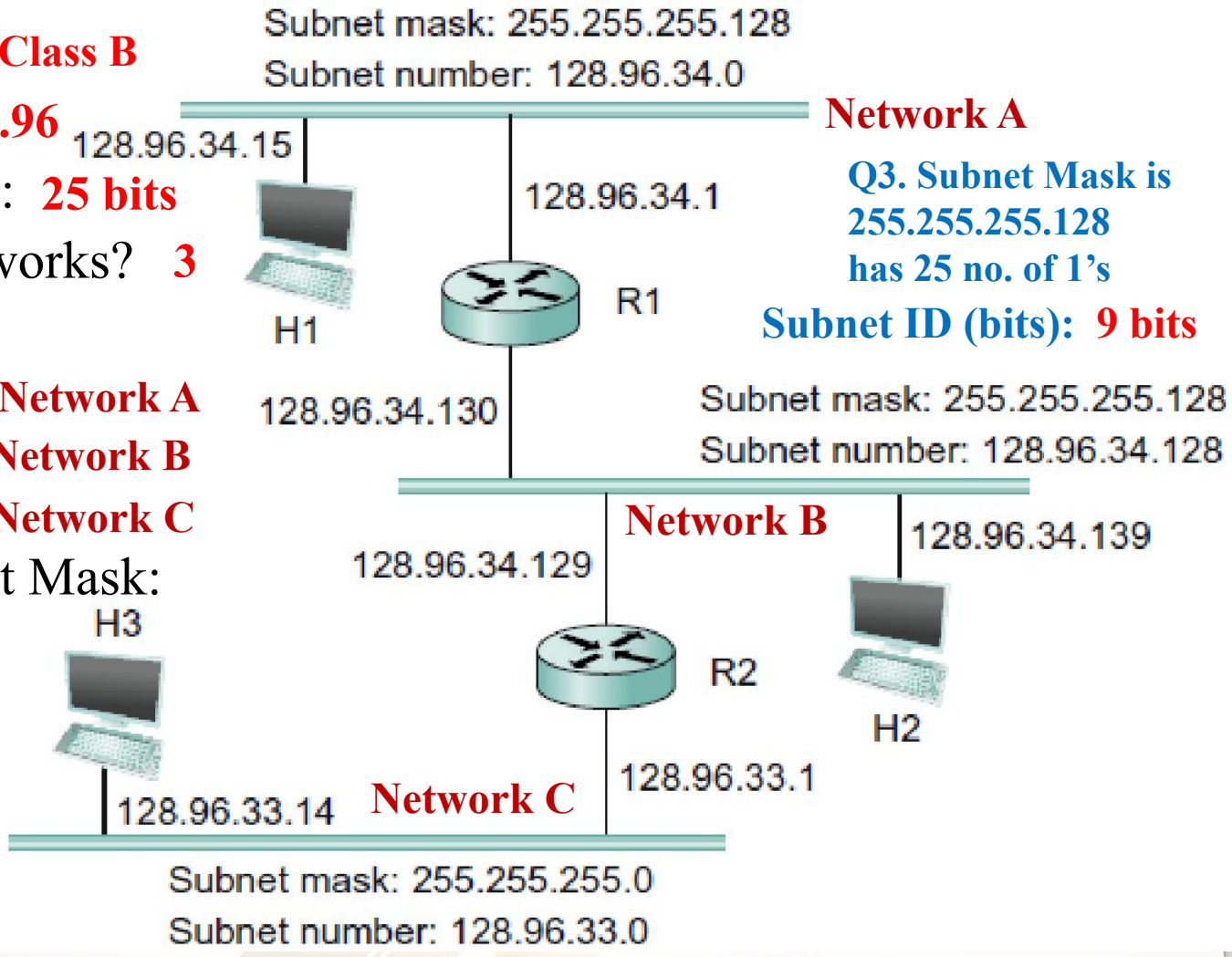
- The mechanism by which a **single network number (135.68)** can be **shared** among **multiple physical networks** involves **configuring** all the nodes on each **subnet** with a **subnet mask**.
- The subnet mask enables us to introduce a **subnet number**; all hosts on the same physical network will have the same subnet number,
- Which means that hosts may be on different physical networks but share a same default network number (135.68)

Example 2: Subnet Configuration

RV UNIVERSITY
Go, change the world

1. Class: 128 □ 0x80 □ Class B
2. Default Net ID: 128.96
3. Subnet Mask (bits?): 25 bits
4. No. of Physical networks? 3
5. Subnet Masks are:
   - A. 255.255.255.128 - Network A
   - B. 255.255.255.128 - Network B
   - C. 255.255.255.0 - Network C
6. IP addr **AND** Subnet Mask: (Subnet numbers)
   - A. 128.96.34.0
   - B. 128.96.34.128
   - C. 128.96.33.0

Each Physical Network is a subnet



Q3. Subnet Mask is 255.255.255.128 has 25 no. of 1's

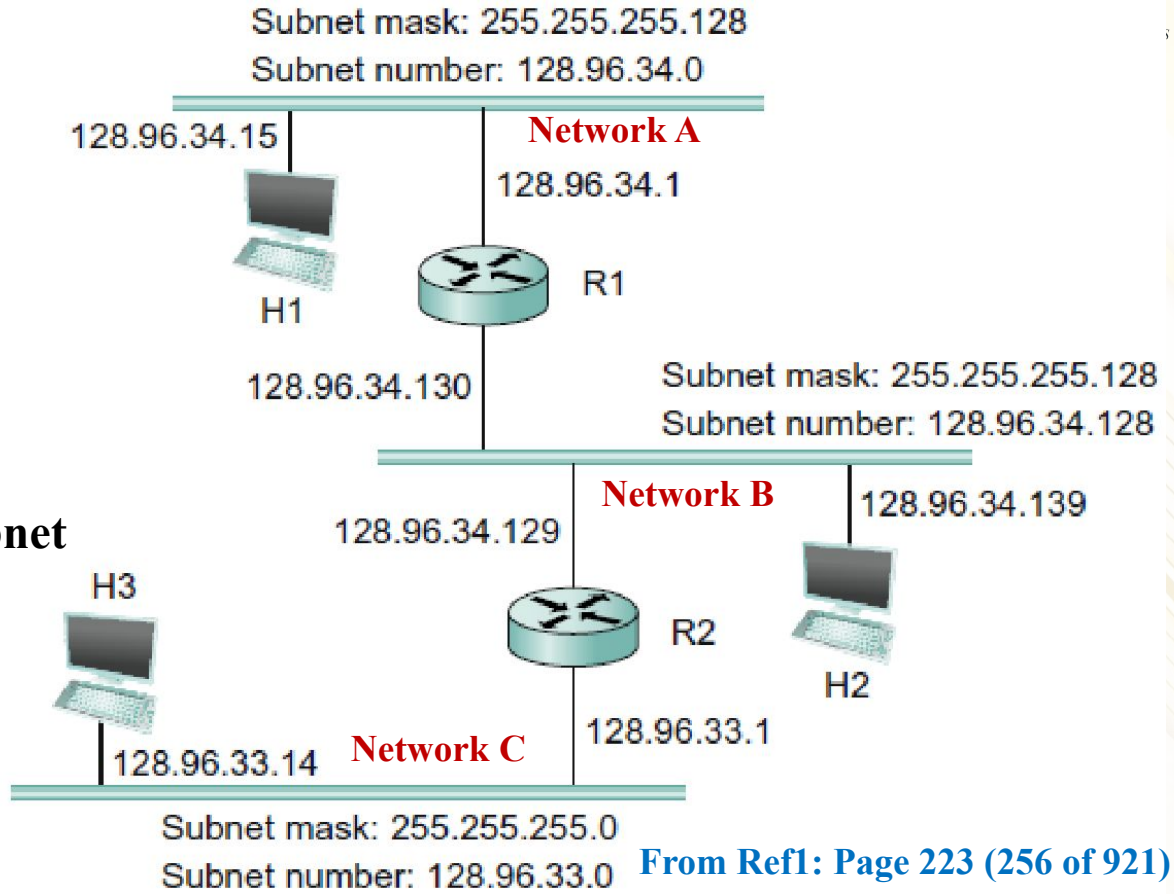
Subnet ID (bits): 9 bits

Quiz 4: Validate the IP Addresses of Hosts

RV UNIVERSITY
Go, change the world

1. Host **H1: 128.96.34.15** o
   Network A
2. Host **H2: 128.96.34.139** (
   Network B
3. Host **H3: 128.96.33.14** o
   Network C

Note: For an **IP address** on a **subnet** to be **valid**, the **bit AND** of the **IP Addr** and **Subnet Mask** should yield the **subnet ID** of the **subnet** the **IP address** is **part of.**



From Ref1: Page 223 (256 of 921)

ANS: **1. H1: 128.96.34.15 AND 255.255.255.128 □ 128.96.34.0**

2. H2: 128.96.34.139 AND 255.255.255.128 □ 128.96.34.128

3. H3: 128.96.33.14 AND 255.255.255.0 □ 128.96.33.0

Homework:
Check the validity of IP addresses of all router Interfaces on the subnets.

Subnet Address: Prefix Notation

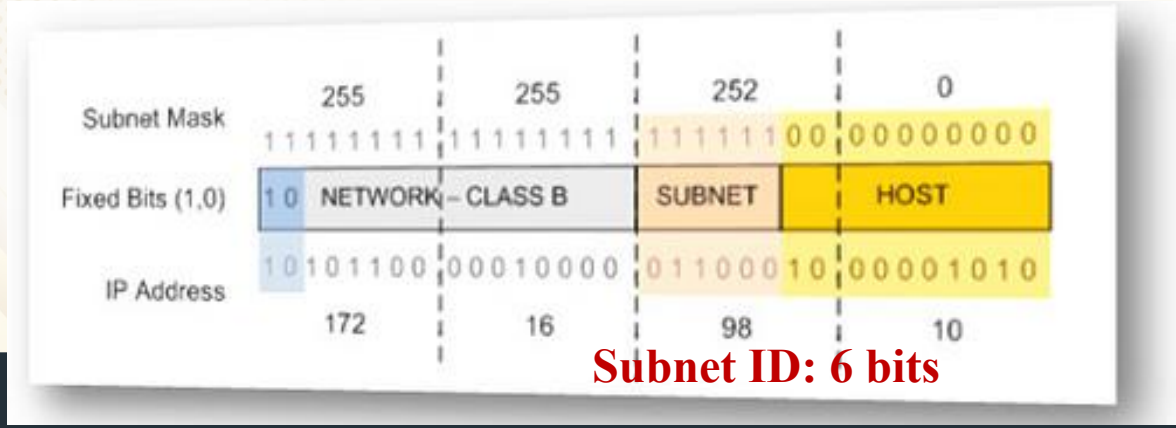
RV UNIVERSITY

Prefix and Subnet mask

Network Address	Subnet 1	Host Number	128.42.0.0/24
Network Address	Subnet 2	Host Number	128.42.1.0/24
Network Address	Subnet 3	Host Number	128.42.2.0/24
Network Address	Subnet 4	Host Number	128.42.3.0/24

Subnet Numbers

- The **class** of this address is: 128 □ 0x80 □ 0b10000000: **Class B**
- **Here, /x** gives the **number of bits** of **subnet mask** of the **subnets**
- **/24** means, the **subnet mask** is **255.255.255 (twenty four 1's)**



Subnet ID: 6 bits

Write the IP address in the Prefix notation:

Ans: 172.16.98.10/22

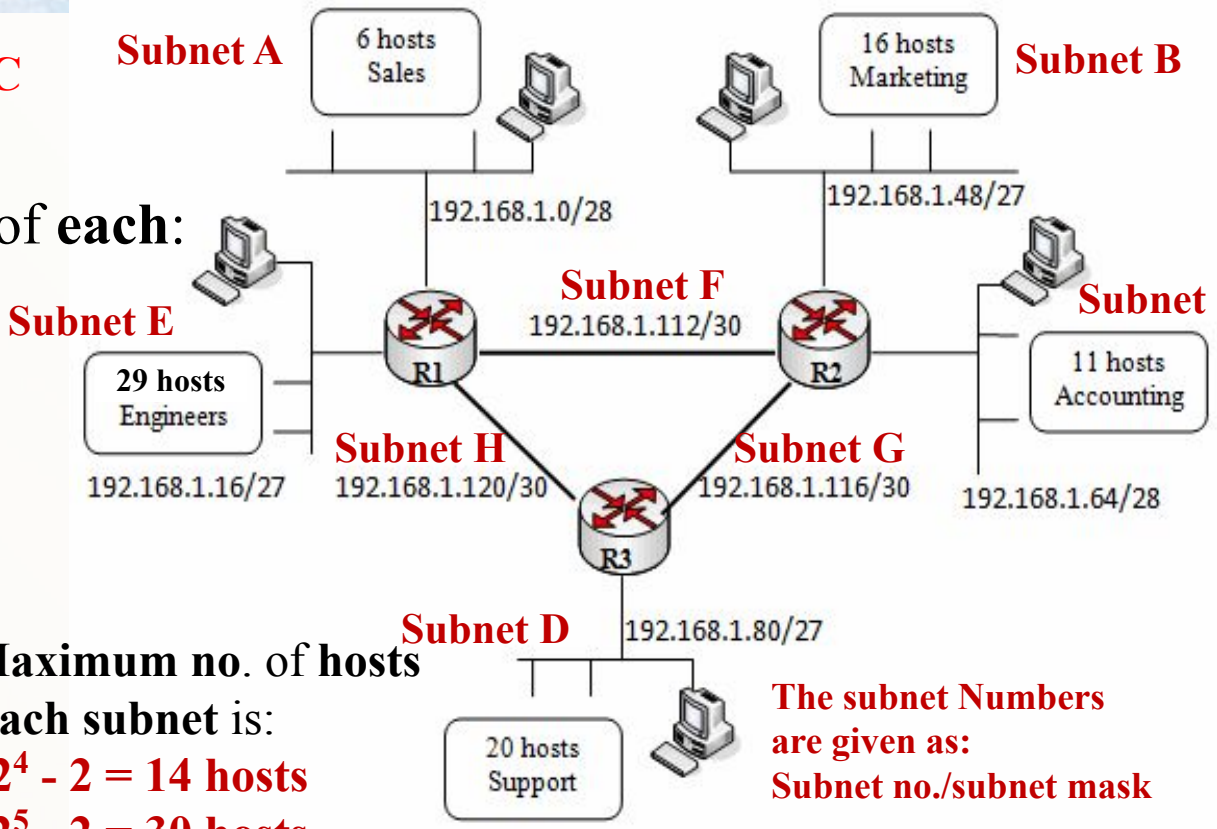
How many hosts can be in this Subnet?

Ans: $2^{10} - 2 = 1024 - 2 = 1022$

Quiz 5: Answer the Questions on these Subnets

1. Class: 192 □ 0xC0: Class C
2. No. of subnets: 5 + 3 = 8
3. **Give** the **subnet masks** of **each**:
   - A. 255.255.255.240
   - B. 255.255.255.224
   - C. 255.255.255.240
   - D. 255.255.255.224
   - E. 255.255.255.224
   - F. 255.255.255.252
   - G. 255.255.255.252
   - H. 255.255.255.252

Binary: Decimal values
0x1100 0000: 192
0x1110 0000: 224
0x1111 0000: 240
0x1111 1100: 252



2. Maximum no. of **hosts** on **each subnet** is:

- A. $2^4 - 2 = 14$ hosts
- B. $2^5 - 2 = 30$ hosts
- C. 14 hosts
- D. 30 hosts
- E. 30 hosts
- F. $2^2 - 2 = 2$ hosts
- G. and H. 2 hosts each (two router interfaces)

The subnet Numbers are given as: Subnet no./subnet mask

3. **List** the **subnets** on which **no more hosts** can be **added**:

ANS: Subnets: E, F, G and H

Quiz 1: Building Subnets

Ref: Subnetting

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

0. Input: **IP address block**: 192.168.1.0 **1. Class:** 192 □ 0xC0 □ 0b1100 0000 □ **Class C**

2. Total no. of hosts that can be **added** here is: $2^8 - 2 = 254$

3. Requirement is to create **five physical LANs** or **Subnets**

4. How many **bits** are to be **taken off** from **Host ID** for **Subnet ID**?

$2^3 = 8$, so 3 bits

5. **Same IP address** in **prefix notation**:

192.168.1.0/27

6. Subnet mask: 255.255.255.224 [0xE0□224]

7. How many bits for Host ID? 5 bits

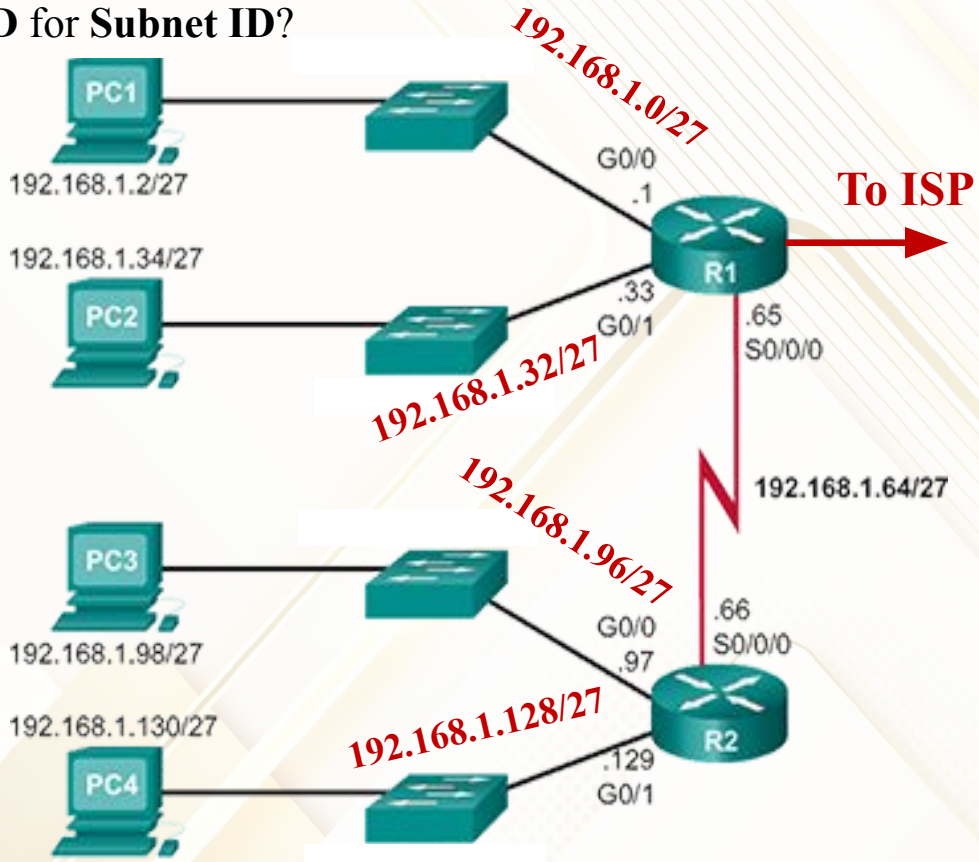
8. How **many more subnets** can be **added?**

3 more can be added

Note: Here both the routers are connected wirelessly using one of the subnets. (**Net 2**): **ref next page**

Note: **Refer** the **next slide** to **understand** how the **addresses** are **split across subnets**.

Note: Here **borrowing 2 bits** from **Host ID** only **four subnets** can be **created**.



Note: IP address Block means one valid default Net ID of a particular Class. Normally organizations are allotted one or more classful addresses. It is used internally by creating subnets based on the needs.

Quiz 1: Building Subnets … contd.

RV UNIVERSITY
change the world
EDUCATIONAL INSTITUTIONS

[Ref: Subnetting]

Let us see the valid Subnets and how the addresses are split across

				3 bits SubnetID		5 bits Host ID	
Net 0	Network	192.	168.	1.	000	0 0000	192.168.1.0
	First	192.	168.	1.	000	0 0001	192.168.1.1
	Last	192.	168.	1.	000	1 1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1 1111	192.168.1.31
Net 1	Network	192.	168.	1.	001	0 0000	192.168.1.32
	First	192.	168.	1.	001	0 0001	192.168.1.33
	Last	192.	168.	1.	001	1 1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1 1111	192.168.1.63
Net 2	Network	192.	168.	1.	010	0 0000	192.168.1.64
	First	192.	168.	1.	010	0 0001	192.168.1.65
	Last	192.	168.	1.	010	1 1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1 1111	192.168.1.95
Net 3	Network	192.	168.	1.	011	0 0000	192.168.1.96
	First	192.	168.	1.	011	0 0001	192.168.1.97
	Last	192.	168.	1.	011	1 1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1 1111	192.168.1.127
Net 4	Network	192.	168.	1.	100	0 0000	192.168.1.128
	First	192.	168.	1.	100	0 0001	192.168.1.129
	Last	192.	168.	1.	100	1 1110	192.168.1.158
	Broadcast	192.	168.	1.	100	1 1111	192.168.1.159
Net 5	Network	192.	168.	1.	101	0 0000	192.168.1.160
	First	192.	168.	1.	101	0 0001	192.168.1.161
	Last	192.	168.	1.	101	1 1110	192.168.1.190
	Broadcast	192.	168.	1.	101	1 1111	192.168.1.191
Net 6	Network	192.	168.	1.	110	0 0000	192.168.1.192
	First	192.	168.	1.	110	0 0001	192.168.1.193
	Last	192.	168.	1.	110	1 1110	192.168.1.222
	Broadcast	192.	168.	1.	110	1 1111	192.168.1.223
Net 7	Network	192.	168.	1.	111	0 0000	192.168.1.224
	First	192.	168.	1.	111	0 0001	192.168.1.225
	Last	192.	168.	1.	111	1 1110	192.168.1.254
	Broadcast	192.	168.	1.	111	1 1111	192.168.1.255

30 IP addresses

Note: The **routers** on the **subnets,** based on the subnet they are part of, treats a particular address as a **broadcast address for that subnet**, though the **default Host ID part is not all 1's**

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Classless Addressing: Supernetting

Classless Addressing: CIDR: Classless Inter-domain Routing

Ref1: Read the Section on CIDR

CIDR: Supernetting: Introduction

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Which **one** is **default mask?** 2

No. of 1's in default masks: 8 or 16 or 24

Which class is this **Default mask for?** Class C

1. Subnet Mask

1 | 11111111 11111111 11111111 111 00000

2. Default Mask

2 | 11111111 11111111 11111111 000 00000

3. Supernet Mask

3 | 11111111 11111111 11111000 000 00000

Net Masks are shown above

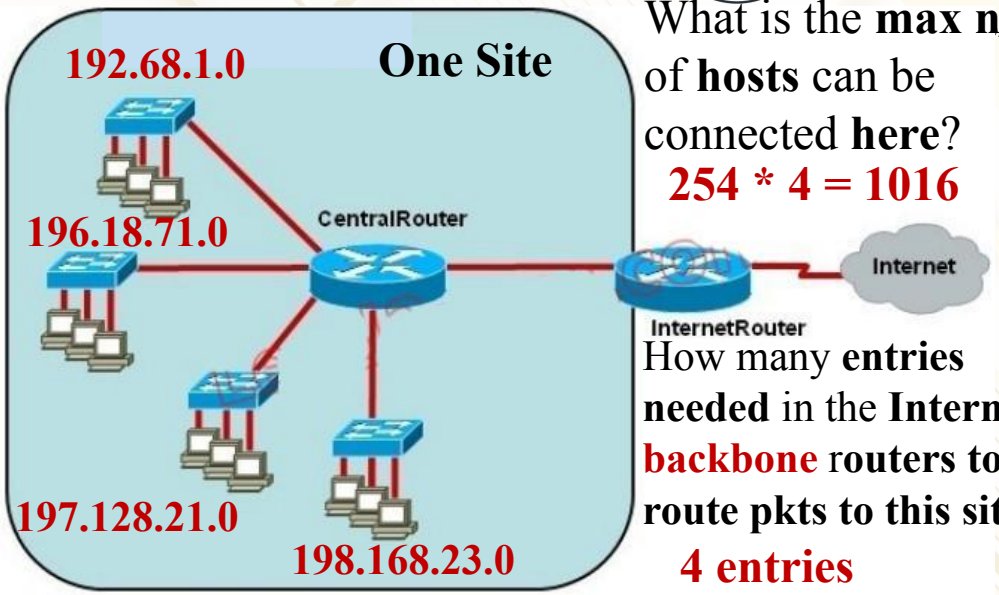
- **Subnetting** has a **counterpart**, sometimes called **supernetting**, but more often called **Classless Interdomain Routing** or **CIDR**, pronounced "cider."
- **CIDR** takes the subnetting idea to its **logical conclusion** by essentially **doing away** with **address classes altogether**.
- Why isn't subnetting alone sufficient?
- In essence, **subnetting** only allows us to **split** a **classful address** among **multiple subnets**, while **CIDR** allows us to **coalesce (join** or **group) several classful addresses** into a **single "supernet."**
- This **further tackles** the **address space inefficiency** and does so in a way that keeps the routing system from being overloaded.

Problem with allocation of Multiple Classful Addresses

(Without subnetting)

- Suppose a **site** needs IP addresses for **~1000 hosts**
- The **site** has **two options** to go for.

1. **Take one Class B address**. But, this will waste whole lot of addresses. So, **not efficient** and due to limited class B addresses, **not practical** either



What is the **max no** of **hosts** can be connected **here**?

254 * 4 = 1016

How many **entries needed** in the **Internet backbone routers to route pkts to this site**?

4 entries

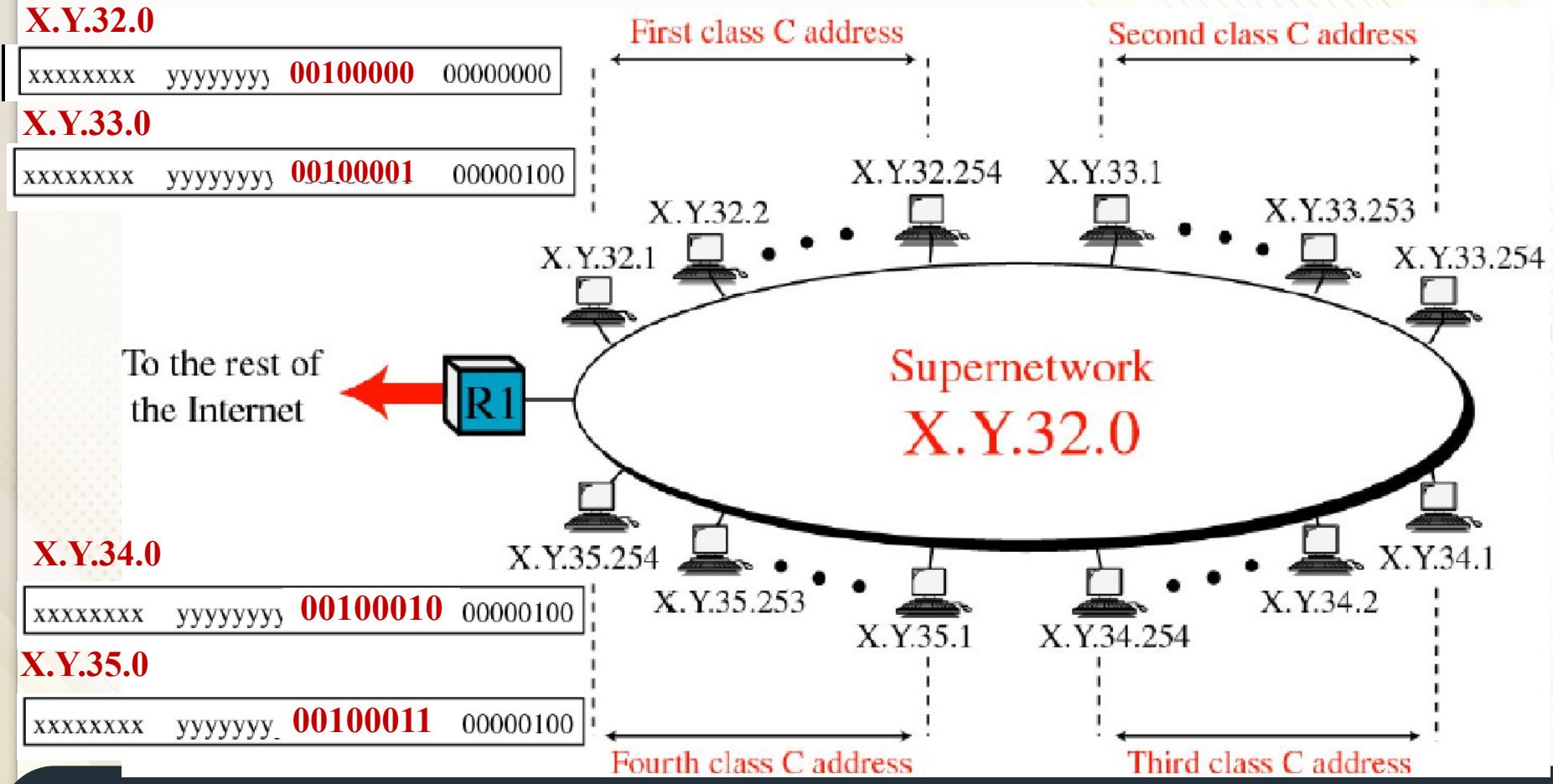
Note: Though the packets belonging to these **four Class C addresses** are all **routed** to the **same physical location**, there are **four separate entries** to be maintained by **all routers**.

2. Take **four Class C** addresses**, instead** of **one class B address.**
3. But this will require all the backbone routers (on Internet) to have **four entries** to route the traffic to this one site, physically located together. This **increases** the **entries** in **many routers** in the **Internet**

Backbone Routers: The routers in the Internet connected to different internetworks

Example 1: Four Consecutive Class C Addresses

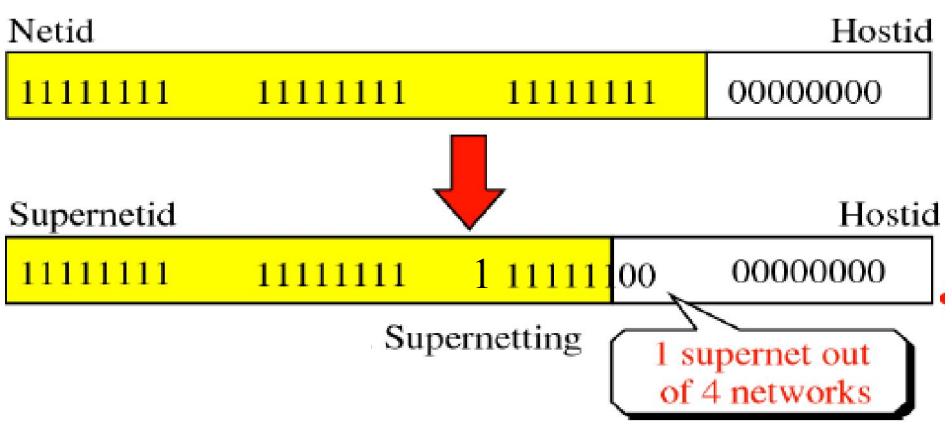
- Now, **instead** of getting **four different Class C addresses**, get **four consecutive Class C addresses** allotted to the site

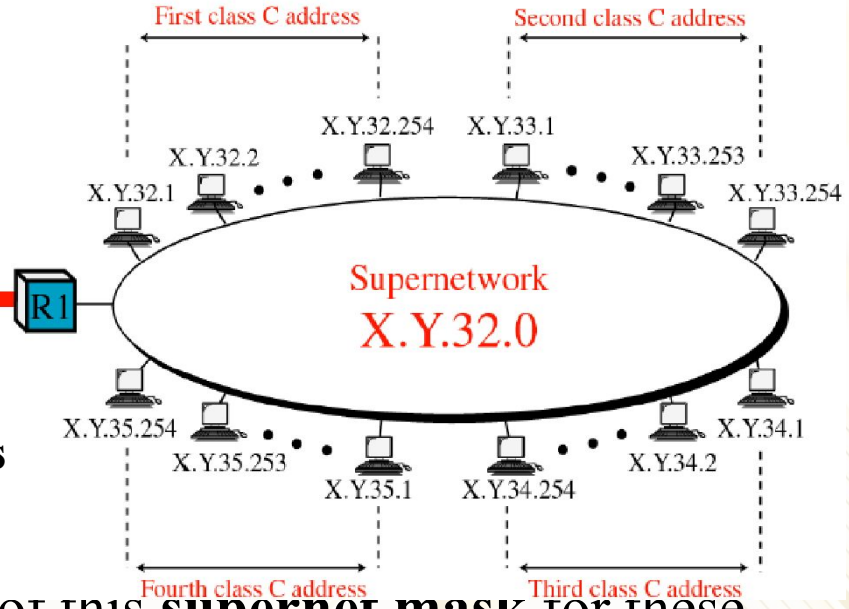


How **many bits** of **Net ID** are **common**, **among** these **four Class C addresses**? **Not 24, but 22!!**

Example 1: Supernetting: Supernet Mask

Supernet Mask here is: 255.255.252.0 **(252 □ 0xFC)**





Prefix notation is used to **represent** the **addresses**

X.Y.32.0/22

- If the backbone routers are made aware of this **supernet mask** for these range of IP addresses, then the **Internet routers** need **only one entry** in them for routing **all IP packets** to **this site**, not four different entries
- With the **supernetting** the Internet routers cannot apply the **default net mask** directly, they **need** the **supernet mask** to **identify** the **Net ID** part of the **addresses**, but it **solves both** the **problems**, **inefficiency in the addressing** scheme as well as **explosion of number of entries** in the **backbone routers**
  - But, one **additional requirement** is that **each IP address** need to **have** an **associated mask**

Example 1: Routing table with Supernet

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Default mask	Network address	Next hop address
255.255.255.0	X.Y.32.0	.....
255.255.255.0	X.Y.33.0	.....
255.255.255.0	X.Y.34.0	.....
255.255.255.0	X.Y.35.0	.....
.	.	.
.	.	.
.	.	.

a. Routing table without supernet mask

Default mask	Network address	Next hop address
255.255.252.0	X.Y.32.0	.....
.	.	.
.	.	.
.	.	.

b. Routing table with supernet mask

Network number: X.Y.32/22

- Though allocations of IP addresses are classful, since set of addresses are handled together by all the routers in the network, this is called classless or CIDR addressing scheme
- No longer, the Net ID can be derived from the first few bits of the IP addresses, to interpret the Net ID part of any address, net mask is needed
- Prefix notation is followed always.

Set of CIDR Notations

RV UNIVERSITY
Go, change the world
f RV EDUCATIONAL INSTITUTIONS

Max no. of Hosts

How many?

$(2^{31} - 1)$ hosts

CIDR Notation	Dotted Decimal	CIDR Notation	Dotted Decimal
/1	128.0.0.0	/17	255.255.128.0
/2	192.0.0.0	/18	255.255.192.0
/3	224.0.0.0	/19	255.255.224.0
/4	240.0.0.0	/20	255.255.240.0
/5	248.0.0.0	/21	255.255.248.0
/6	252.0.0.0	/22	255.255.252.0
/7	254.0.0.0	/23	255.255.254.0
Class A /8	255.0.0.0	/24	255.255.255.0 Class C
/9	255.128.0.0	/25	255.255.255.128
/10	255.192.0.0	/26	255.255.255.192
/11	255.224.0.0	/27	255.255.255.224
/12	255.240.0.0	/28	255.255.255.240
/13	255.248.0.0	/29	255.255.255.248
/14	255.252.0.0	/30	255.255.255.252
/15	255.254.0.0	/31	255.255.255.254
Class B /16	255.255.0.0	/32	255.255.255.255

Just Two Hosts

Normally used for WAN links with routers at both the ends

1. **Identify** the **mask values** which **correspond** to the **default Net Masks** of **standard classes**
2. **Identify** the **one** which has got the **maximum number of hosts** in it.
3. **Identify** the **one** which has got just **two usable host addresses** in it.

Special IP addresses – Recap

RV UNIVERSITY
Go, change the world

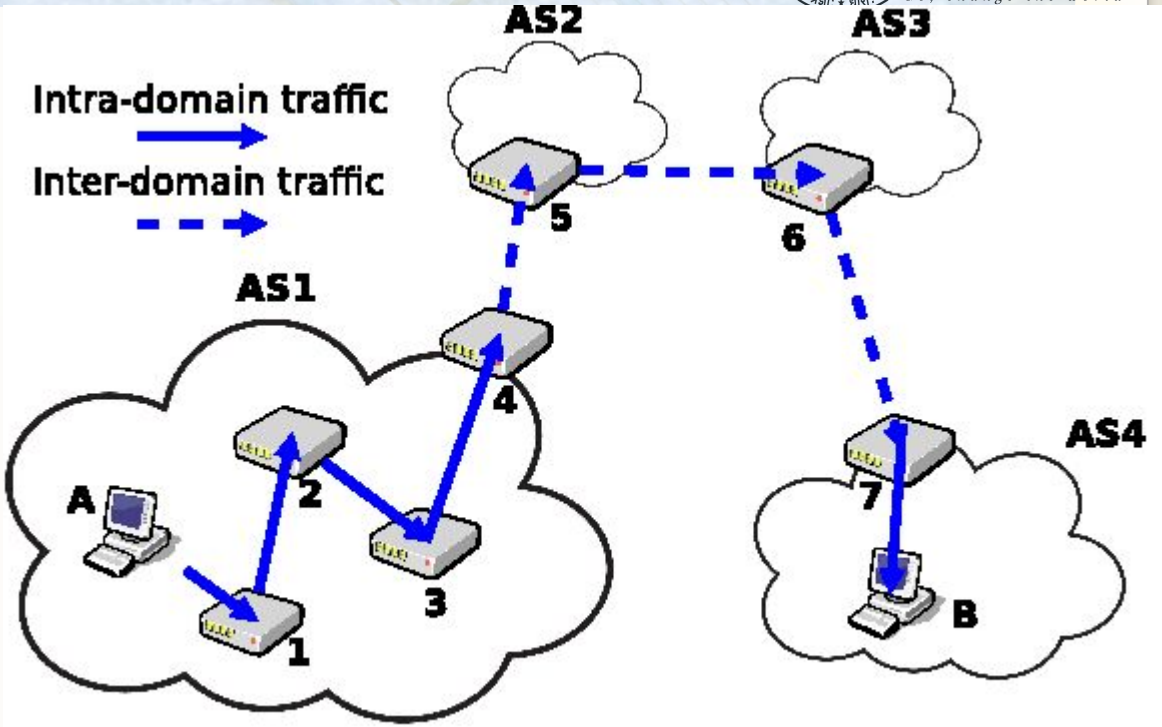
Special IP Addresses	Description
0.0.0.0	Refers to the **default route**. This route is to simplify routing tables used by IP. **Net mask of 0, all IP address match with this mask**
127.0.0.1	Reserved for **Loopback**. The Address 127.0.0.1 is often used to refer to the **local host**. Using this Address, applications can address a local host as if it were a remote host.
IP Address with all **host bits** set to "**0**" **192.168..72.0 (class C)**	Refers to the actual network itself. For example, network 192.168.72.0 (Class C) can be used to identify network 192.168.72. This type of notation is often used within routing tables.
IP Address with all **node bits** set to "**1**" (Subnet / Network Broadcast) e.g: **192.168.72.255**	IP Addresses with all **node bits** set to "**1**" are local network broadcast addresses. Some examples: **125.255.255.255** (**Class A**) , **190.30.255.255** (**Class B**), **203.31.218.255** (**Class C**).
IP Address with **all bits** set to "1" (Network Broadcast) e.g **255.255.255.255**	The IP Address with all bits set to "1" is a broadcast address and must **NOT** be used. These are destined for all nodes on a network, no matter what IP Address they might have.

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Domain and Autonomous System
&
Forwarding Vs Routing

Definitions: Domain and Autonomous System

- **Domain** is an **internetwork** in which **all** the **routers** are **under** the **same administrative control**
- **Example: University campus, Internet Service Provider (ISP)**



- **Domain** or **Autonomous System (AS)** is a network which is under the control of one organization, it may have one more subnets
- The routing of IP packets **within a domain** (**intra-domain**) and **between the domains** (**inter-domain**) are handled by different **routing protocols**

Note: Domain and AS mean the same

Quiz 1: AS Vs Subnet

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Choose all the correct options about the AS and Subnets below:

A. An AS can have many subnets in them
B. A subnet can have many AS in them
C. AS is a collection of internetworks in a physical area, within an organization or college premises or ISP network, which is under the administrative control of one entity
D. AS is normally larger in size than a subnet

ANSWER: A, C and D

Forwarding Vs Routing

- **Forwarding** consists of taking a packet, looking at its destination address, consulting a table, and **sending the packet** in a direction determined by that table.
  - We have seen several examples of forwarding
- **Routing** is the **process by which forwarding tables** are **built**.
- We also note that **forwarding** is a relatively **simple** and **well-defined process** performed **locally at a node**,
- Whereas **routing** depends on **complex distributed algorithms** that have continued to evolve throughout the history of networking
- **Routing protocols** help in **building** and **maintaining** the **forwarding tables** in the routers based on the **dynamic state** of **various routers** and **links** in the **internetwork**

Note: We will not be looking at **Routing protocols** in this course

Quiz 2: Forwarding Vs Routing

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- Choose all the correct options about Forwarding and Routing below:

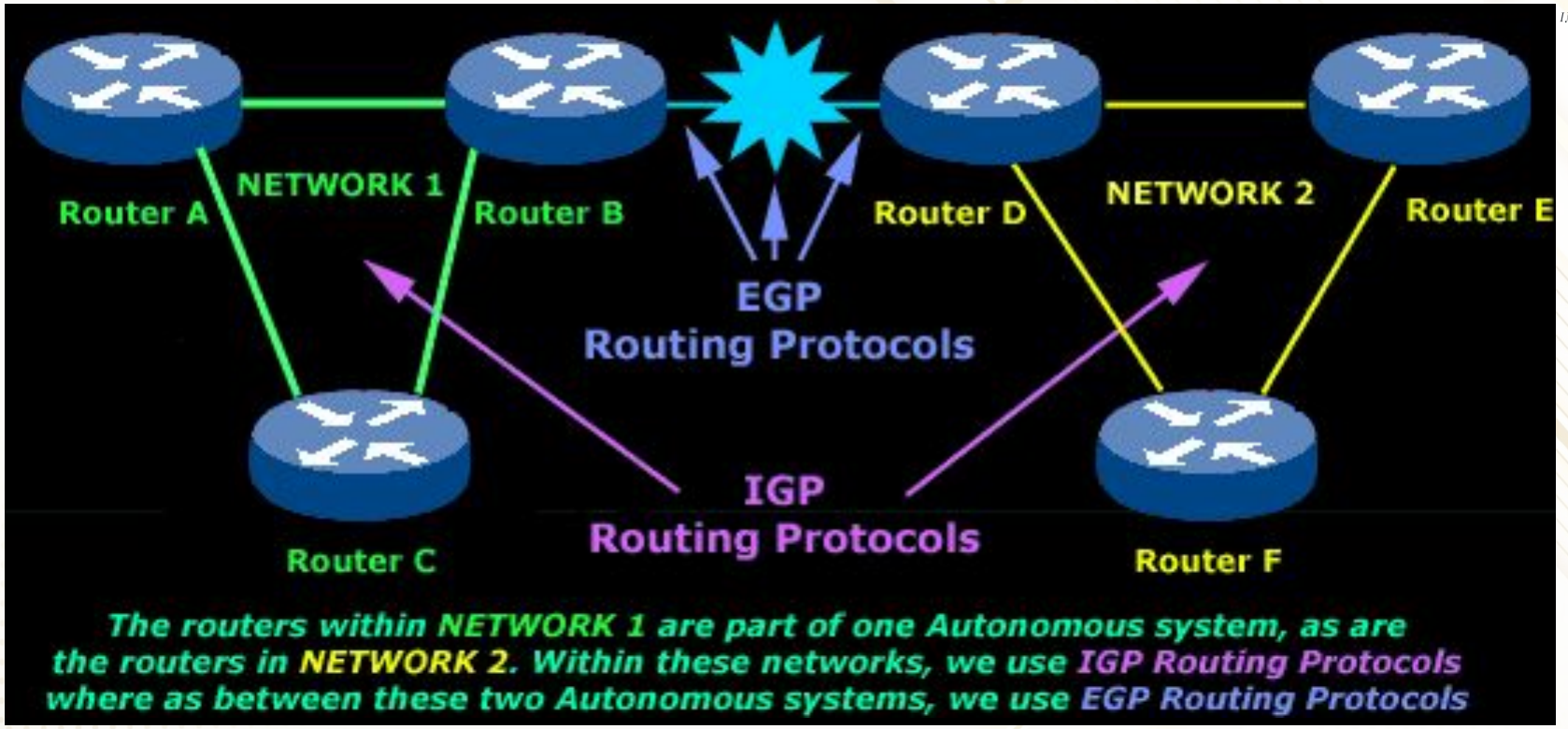
A. Routing protocols exchange information among its peer routers in the network, to periodically update the routing/forwarding tables
B. Forwarding decisions are made by the routers based on the forwarding table entries built by routing protocols
C. Routing protocols run only once when the routers are switched ON for the first time
D. Only the Host ID part of the IP addresses are used by the routers to take forwarding decisions

ANSWER: A and B

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Intra-domain and Inter-domain Routing Protocols

Intra-domain and Inter-domain Routing



Intradomain Routing is **done** by **Interior Gateways Protocols**
Interdomain Routing is **done** by **Exterior Gateway Protocols**

These protocols are run by routers by exchanging information among themselves periodically to build routes based on IP addresses and maintain routing tables within each router

Inter-domain and Intra-domain Routing Protocols

RV UNIVERSITY
Go, change the world

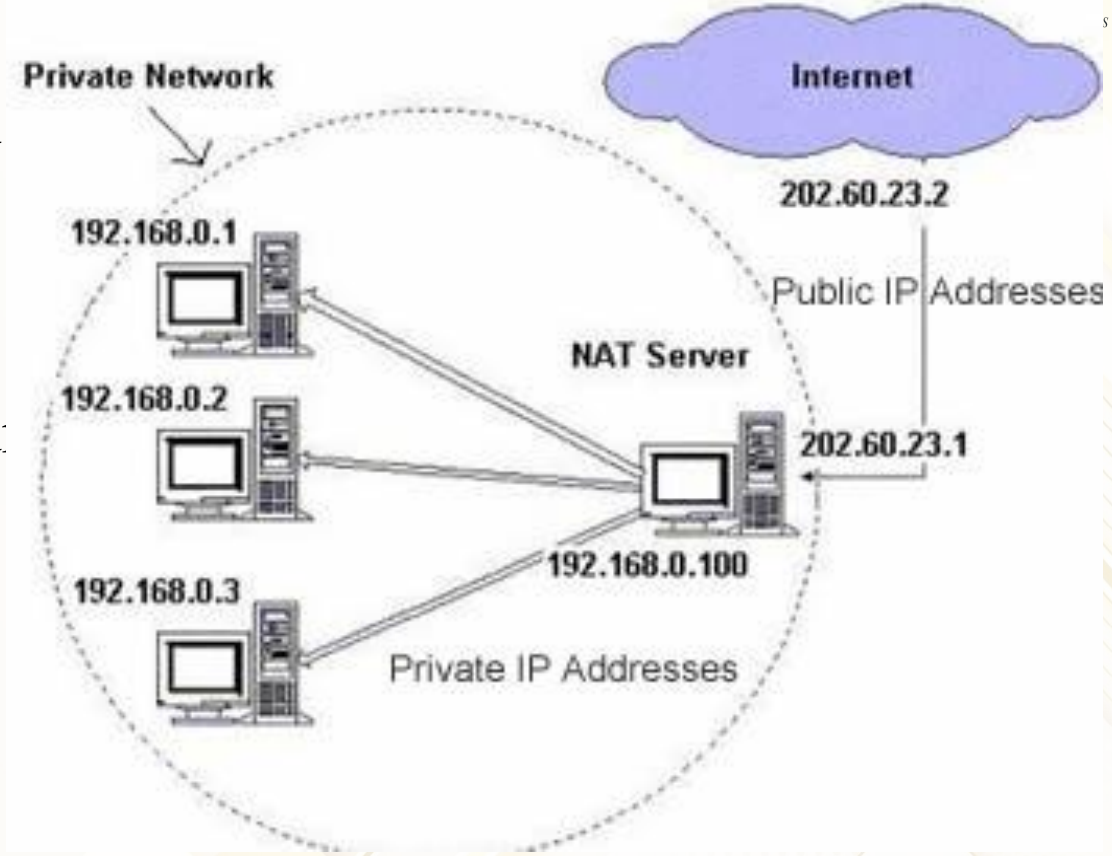
Intra-domain Routing	Inter-domain Routing
Routing within an AS	Routing between ASs
Ignores the Internet outside the Autonomous System	Assumes that the Internet consists of a collection of Interconnected AS's
Protocols for Intradomain routing are called **Interior Gateway Protocols** or **IGPs**	Protocols for Interdomain routing are also called **Exterior Gateway Protocols** or **EGP's**
Popular routing protocols are: - Routing Information Protocol (**RIP**) - Simpler - Open Shortest Path First (**OSPF**) - Better	**Routing Protocol:** - Border Gateway Protocol (**BGP**)

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

Private and Public IPs

Private and Public IPs

- Just as your network's public IP address is issued by your ISP, your router issues private (or internal) IP addresses to each network device inside your network. **- Through DHCP**
- This provides unique identification for devices that are within your network, such as your computer, your video conferencing systems, and so on



NAT: Network Address Translation

Reserved Private IP addresses

RV UNIVERSITY
Go, change the world
an initiative of RV EDUCATIONAL INSTITUTIONS

- The Internet Assigned Numbers Authority (**IANA**) and the Internet Corporation for Assigned Names and Numbers (ICANN) have excluded ranges withheld for private network use.
- **The private IP ranges are as follows:**
  - **10.0.0.0 … 10.255.255.255**
  - **172.16.0.0 … 172.31.255.255**
  - **192.168.0.0 … 192.168.255.255**
- These private IP addresses are used internally by many organizations without the need for them to be globally unique

What are the classes of these IP addresses?

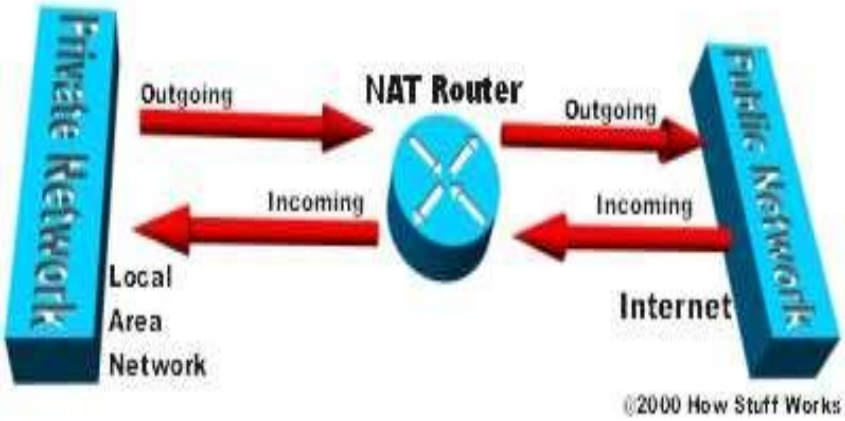
ANS: **Class A, B and C Respectively**

Motivation for Private IP Addresses

- Basically, without private IP addressing, we would have run out of IPv4 addresses many years ago.
- There are simply not enough IPv4 addresses for everyone to have a unique IPv4 address
- Many applications require connectivity only within one enterprise and do not need external (outside the enterprise) connectivity
- A large airport which has its arrival/departure displays individually addressable via TCP/IP.
- It is very unlikely that these displays need to be directly accessible from other networks outside of the airport
- For security reasons, many enterprises use application layer gateways to connect their internal network to the Internet.
- The internal network usually does not have direct access to the Internet, thus only one or more gateways are visible from the Internet.

Function of NAT

- NAT is required when the host that do not have globally unique IP addresses need to connect to the Internet
  - NAT maps (many-to-one) from private IP addresses to public IP addresses while sending out the IP packets over to the Internet
  - On receipt, they are converted back from Public IP to Private IP



Protocol	: TCP
Source Address	: 192.168.0.12
Source Port	: 1944
Destination Address	: 208.147.66.234
Destination Port	: 21

NAT

Protocol	: TCP
Source Address	: 157.54.35.39
Source Port	: 5001
Destination Address	: 208.147.66.234
Destination Port	: 21

NAT Mapping Table			
192.168.0.10: 3576	← TCP →	157.54.35.38: 5000	(Dynamic Address Translation)
192.168.0.11: 2258	← TCP →	157.54.35.39: 5000	(Dynamic Address Translation)
192.168.0.12: 1944	**← TCP →**	**157.54.35.39: 5001**	**(Dynamic Port & Address Translation)**