Module No. 5 Internetworking Layer

4.1 Internet Protocol (IP) datagram, header fields & their function

- Introduction
  - → position of IP in TCP/IP protocol suite.
- Datagram
  - → IP datagram = Header + Data
  - → IP Header format
    - → Service Type
    - → Encapsulation of a small datagram in Ethernet frame.
    - → Multiplexing
    - → protocols
    - → Fragmentation
      - → MTU
      - → Fields Related to Fragmentation.
        - → Identification
        - → flags
        - → Fragmentation offset.
    - → Checksum.

Introduction:

- Internet protocol (IP) is the transmission mechanism used by TCP/IP protocols at the n/w layers.
- IP is an unreliable & connectionless datagram protocol — a best-effort delivery service.
- The term best-effort means that IP tries its best to deliver the packets but they can be corrupted, lost, arrive out of order, or delayed & may create congestion for the n/w.

- If reliability is important, IP must be paired with a reliable protocol such as TCP.
  - e.g of best-effort delivery service is the post office.

* IP relies on higher level protocol to take care of lost, corrupted & out of order datagrams.

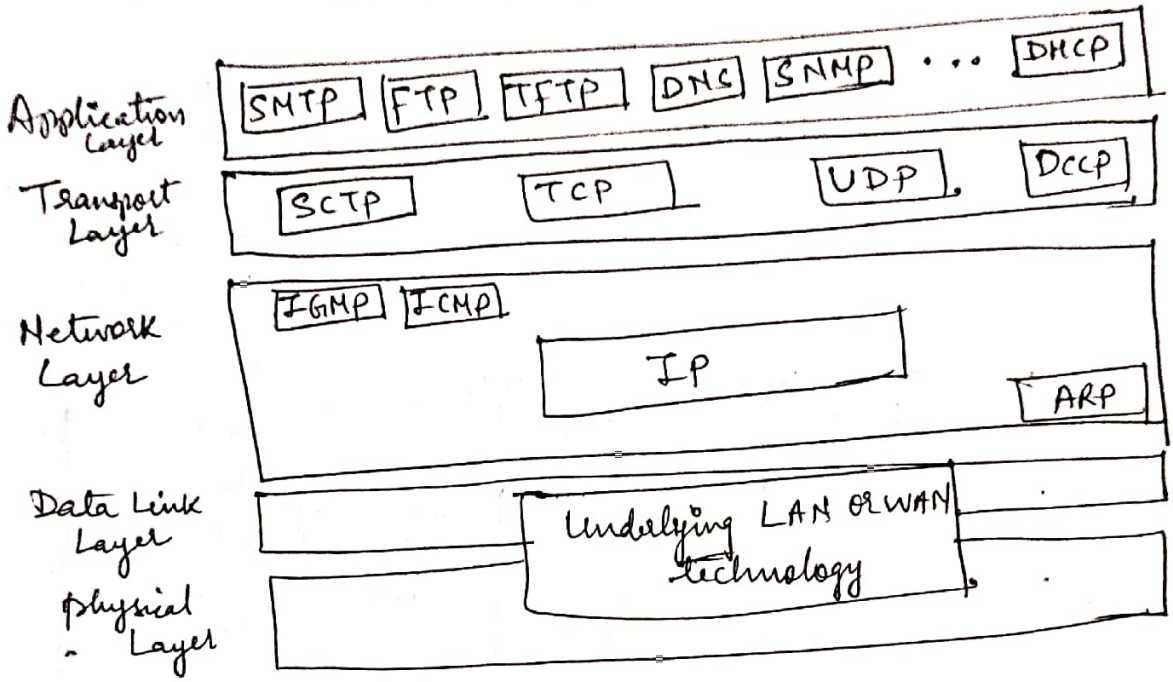


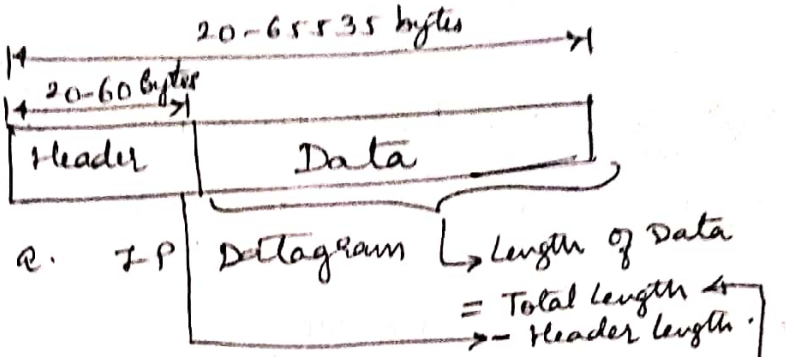
fig: Position of IP in TCP/IP protocol suite

DATAGRAMS

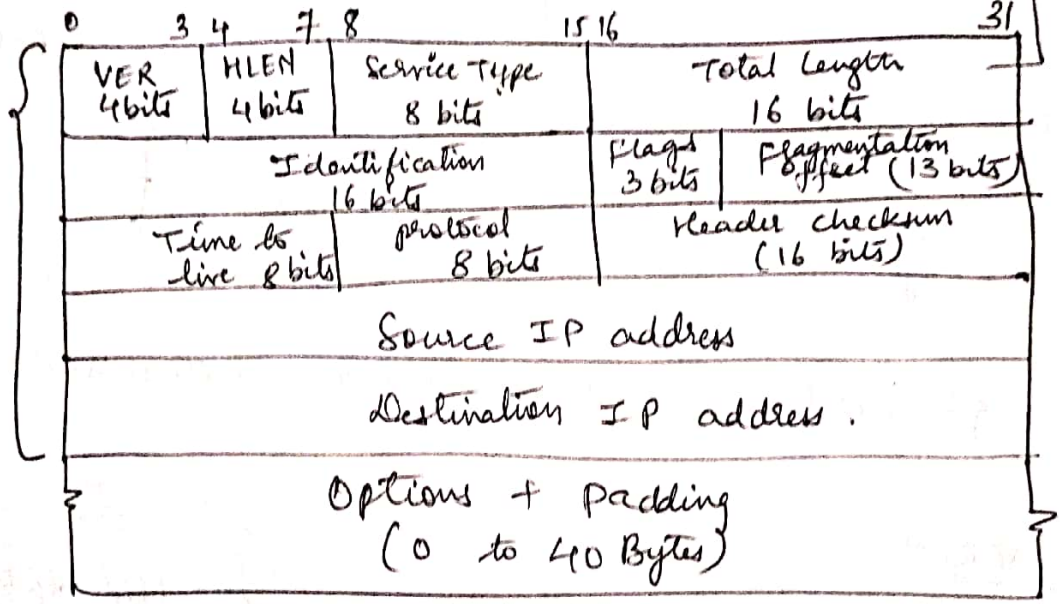
- Packets in the n/w (internet) layer are called datagrams.
- A datagram is a variable length packet consisting of two parts: Header & Data.
- The header is 20 to 60 bytes in length & contains information essential to routing & delivery.

UDP Header	TCP Header	IP Header
8 bytes	20 to 60 Bytes	20 to 60 Bytes.

IP Datagram:



Q. IP Datagram → Length of Data = Total Length − Header length.



b. Header format.

Q.1. An IP packet has arrived with the first 8 bits as shown 01000010 The receiver discards the packet. Why?

Q2. In an IP packet the value of HLEN is 1000 in binary. How many bytes of options are being carried by this packet? (Ans 12 bytes)

Q.3. In an IP packet, the value of HLEN is 5_{16} & the value of the total length field is 0028_{16}. How many bytes of data are being carried by this packet? (Ans 20 Bytes)

$2^4 - 1 = 40_D$

Q.4. An IP packet has arrived with the first few hex digits as shown below: 45000028000100000102. How many hops can this packet travel before being dropped? The data belong to which higher level protocol?

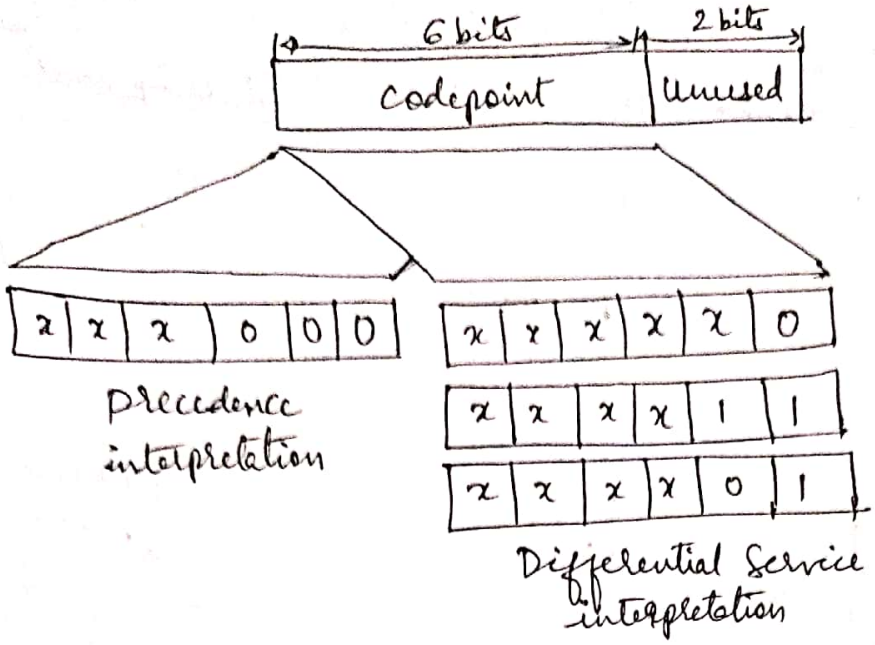


fig: Service Type ..

Values of codepoints :

Category	Codepoint	Assigning Authority
1	XXXXX0	Internet
2	XXXX11	Local
3	XXXX01	Temporary or Experimental

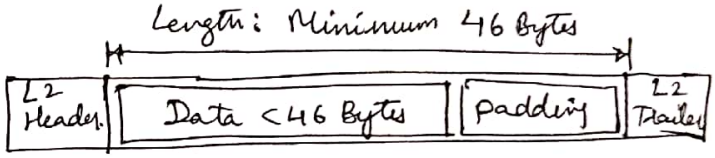


fig: Encapsulation of a small datagram in an Ethernet frame.

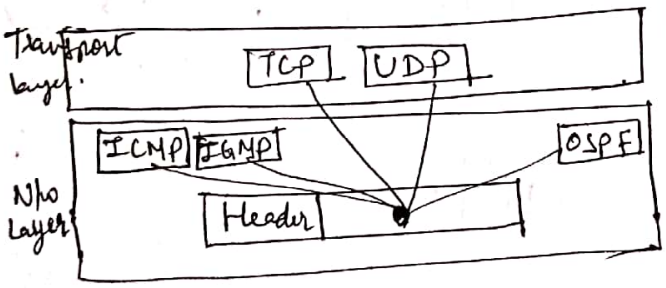


fig: Multiplexing

Value	protocol
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

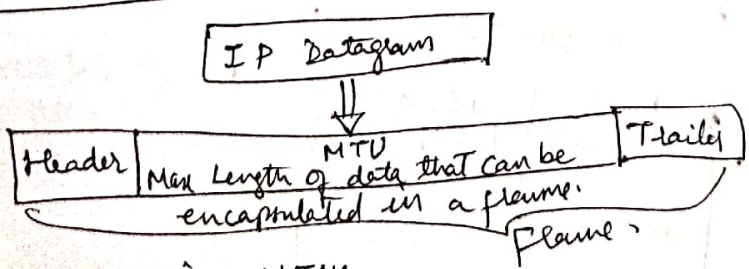


fig: MTU.

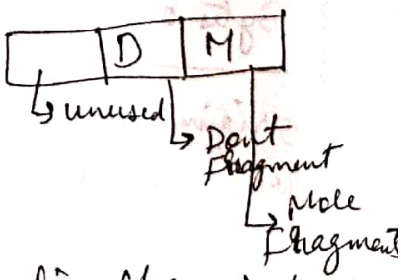


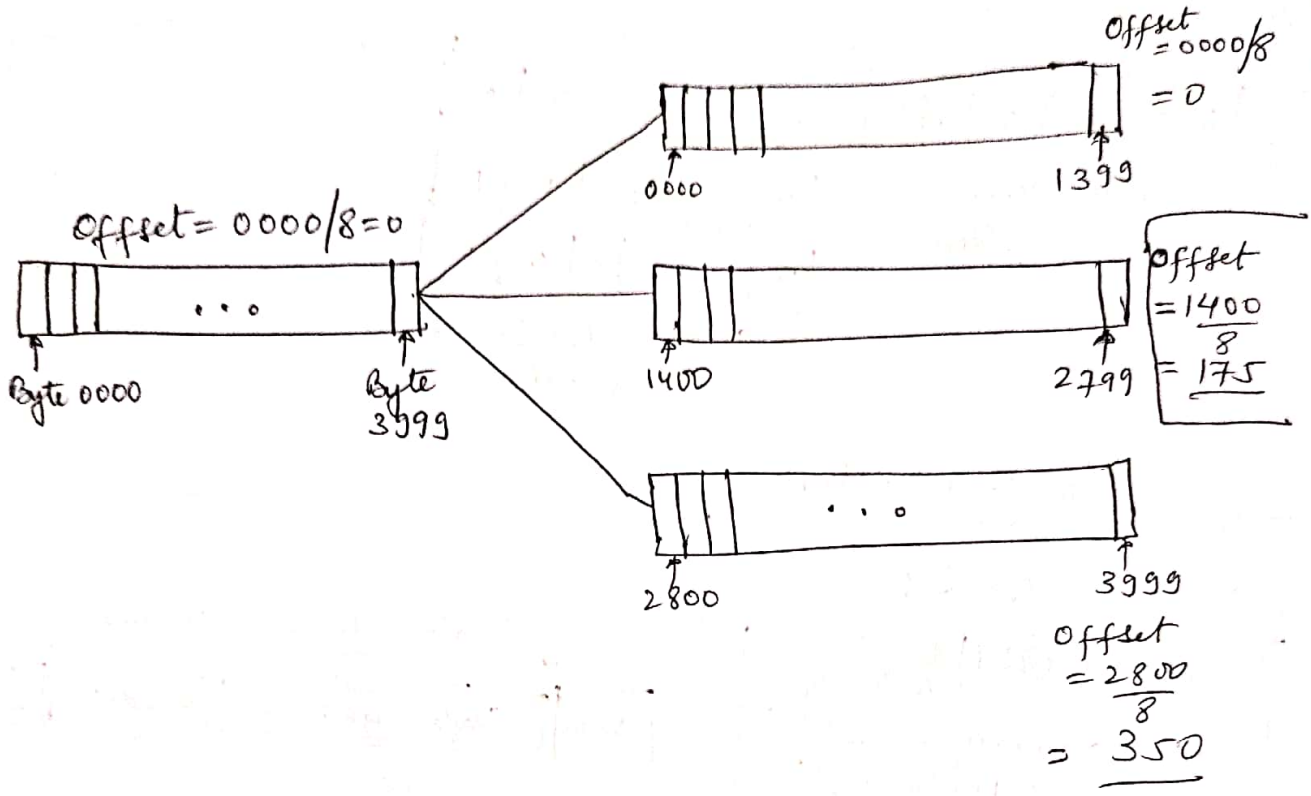
fig flags field.

000010 1000
40 Bytes
- 20
20 bits

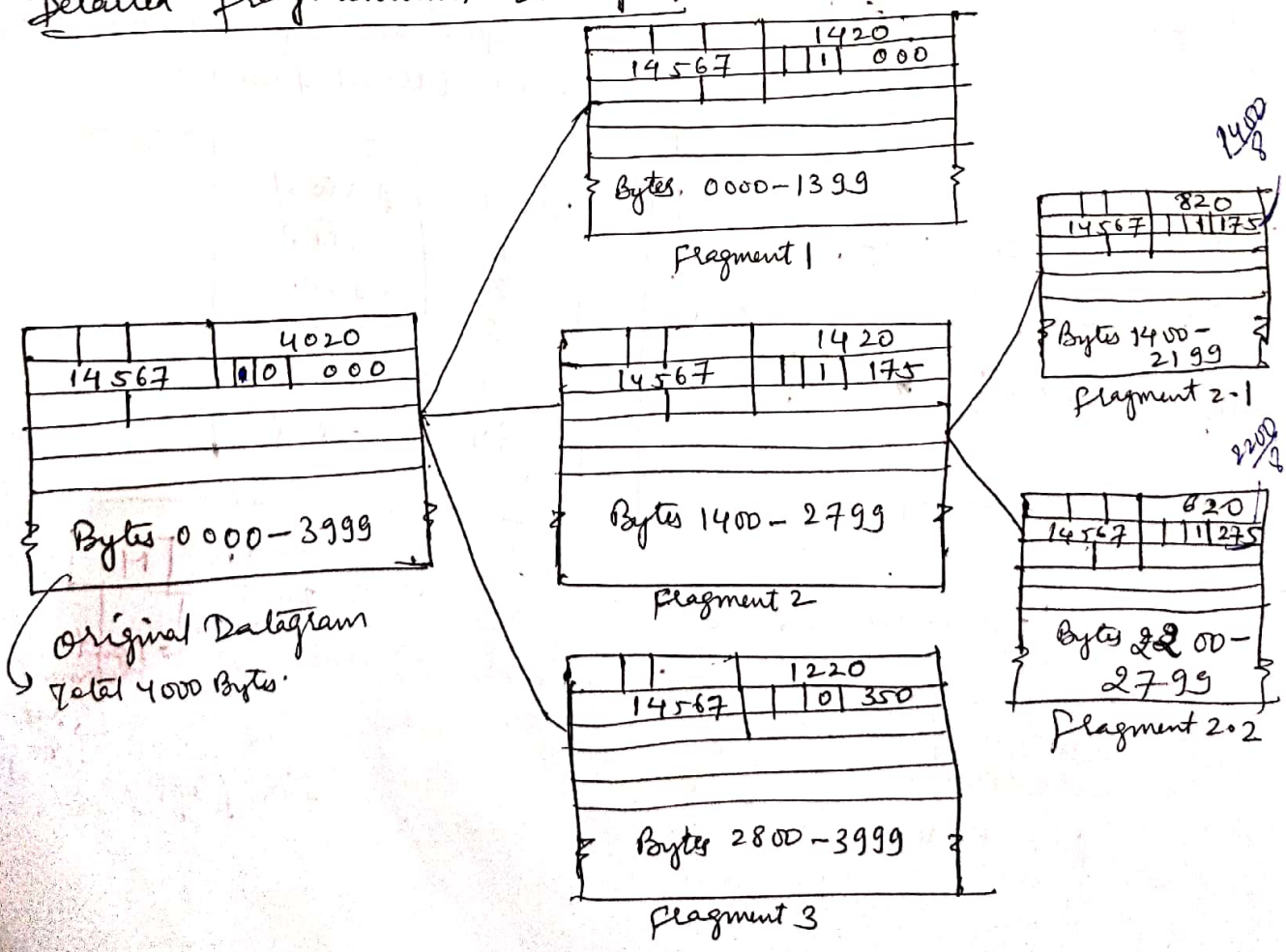
Shubhangi Khekale

Fragmentation Example.

Let 4000 Bytes packet is Fragmented into 3 Packets → 1400 Bytes, 1400 Bytes, 1200 Bytes.

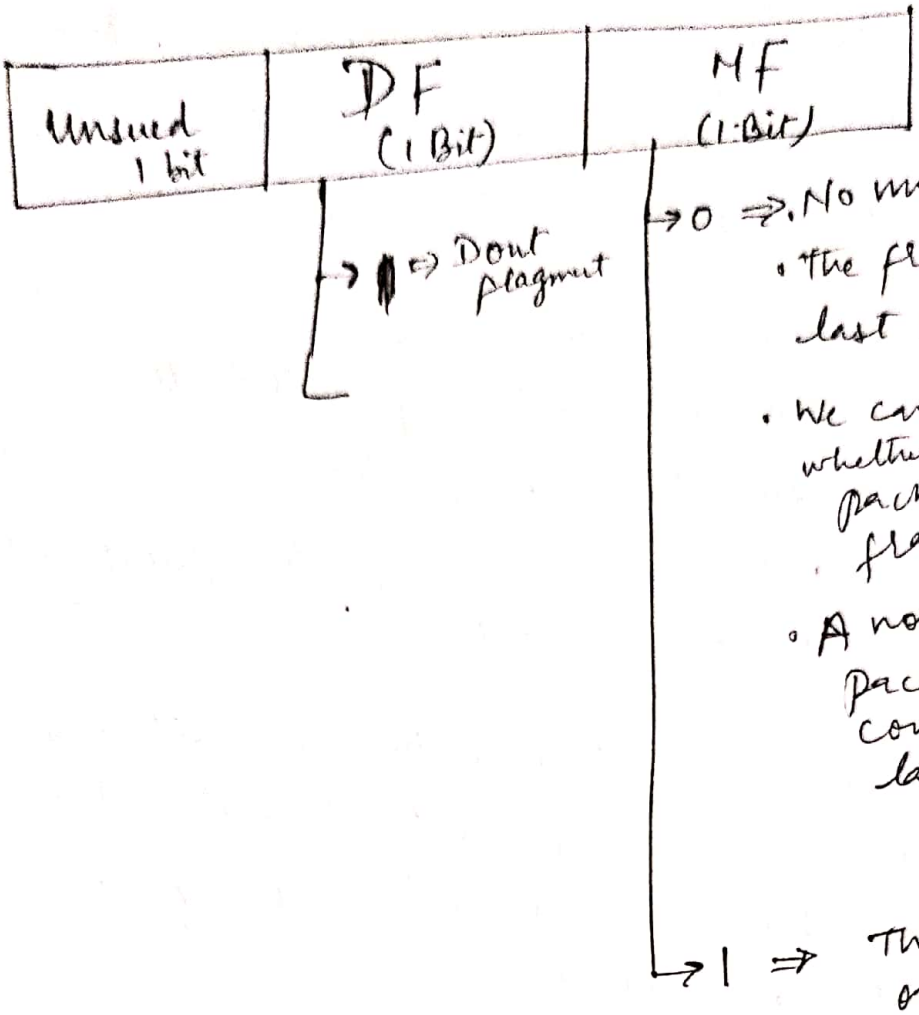


Detailed fragmentation Example:



DF ⇒ Do not fragment
MF ⇒ More fragments.

Flags field (3 bits)



- Offset value = 100 ⇒ No of 1st byte = 100 × 8 = 800
  Can't predict no of last byte w/o knowing Data length

& Offset value = 100 & HLEN = 5, Total length = 100
⇒ Length of Data = 100 − 5×4 = 80 Bytes
First byte no = 100 × 8 = 800
Last byte no = 879
} ⇒ Data length of 80 Bytes.

- The fragment can be first middle one, but not the last one.
- We cannot say whether it is first or middle one, need more information (value of fragmentation offset)

M=1 & offset value = 0
M=1 ⇒ 1st or middle fragment
But ∵ offset value = 0 ⇒ It is the first fragment.

Examples on flags field of IP Header.

Q.1. A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

→ M=0 ⇒ Last fragment

No we cannot say whether the packet was fragmented.

But the Non fragmented packet could be the last one.

Q.2. A packet has arrived with an M bit value of 1. Is this the first fragment, the last, or a middle fragment? Do we know if the packet was fragmented?

→ M=1 ⇒ fragment can be first or middle one.

But not the last one.

Yes obviously the packet is fragmented

But whether it is 1st or middle can only be known from the offset field value.

Q.3. A packet has arrived with an M bit value of 1 and a fragmentation offset value of zero. Is this the first fragment, the last fragment, or a middle fragment?

→ M=1 ⇒ fragment can be 1st or middle

But as offset value = 0 it has to be 1st fragment

Q.4. A packet has arrived in which the offset value is 100. what is the no of the first byte? Do we know the no of the last byte?

→ No of 1st Byte = 100 × 8 = 800

The no of last byte cannot be predicted w/o knowing data length.

Q.5. A packet has arrived in which the offset value is 100, the value of HLEN is 5 & the value of the total length field is 100. what is the no of the first byte & the last Byte?

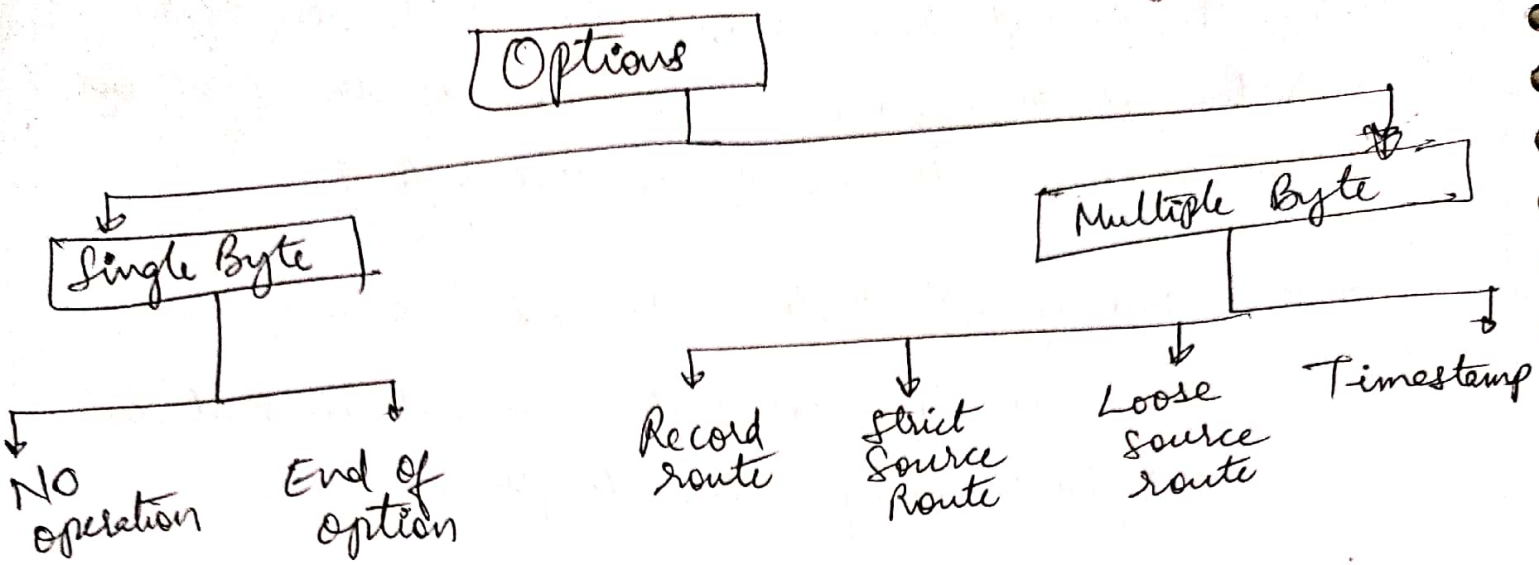
→ HLEN = 5 ⇒ Length of Header = 5 × 4 Bytes
= 20 Bytes

Total length = 100 Bytes

∴ Length of data = Total length − length of Header
= 100 − 20
= 80 Bytes

No of 1st Byte = 100 × 8 = 800

No of Last Byte = 800 + 79 = 879
(Total 80 Bytes)



Checksum calculation in the IP packet

Step 1: Value of the checksum field is set to 0.

Step 2: Entire Header is divided into 16-bit sections & added together.

Step 3: The sum is complemented & inserted into the checksum field.

Checksum in the IP packet covers only the header, not the data.

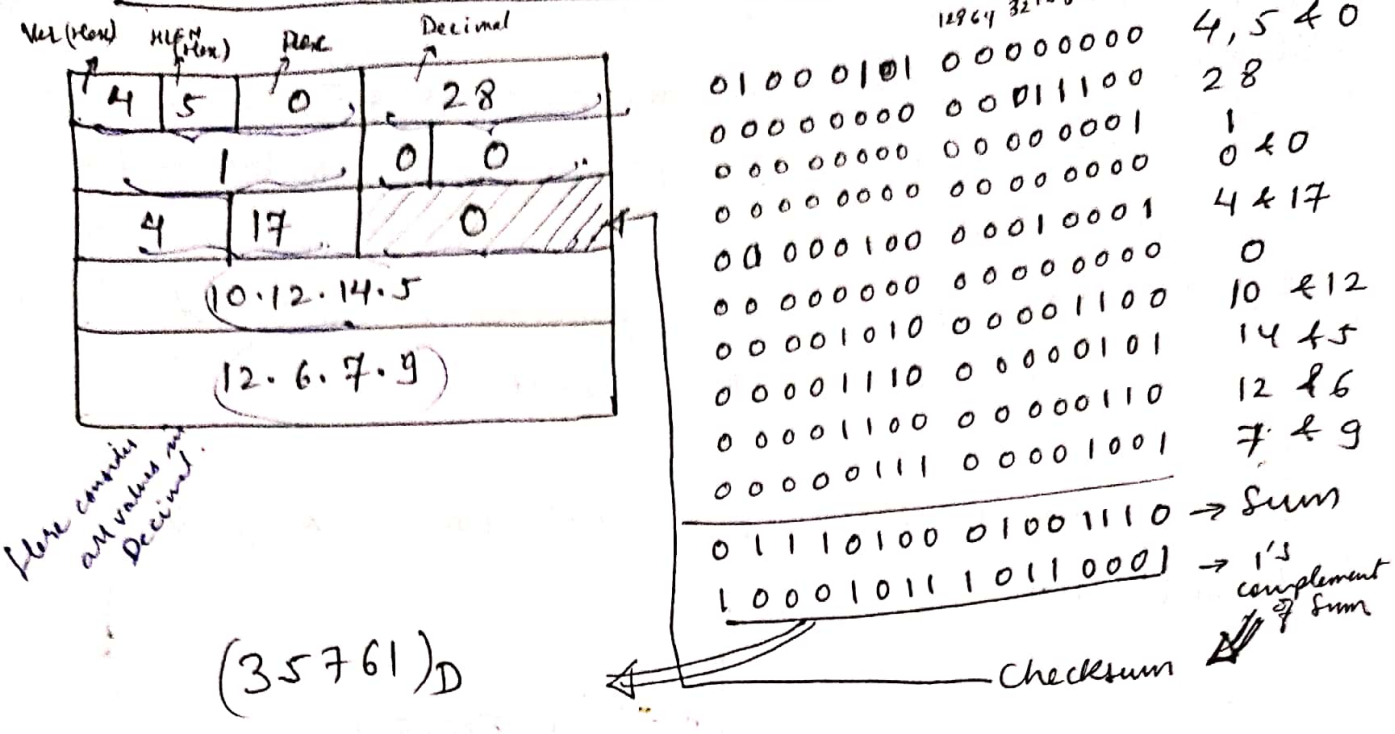
2 Good Reasons

(1) Appl^n data encapsulated in TCP & UDP is already verified using checksum. So IP need not repeat checksum calculation on encapsulated data

(2) IP Header changes with each visited router, but not the data. So checksum calculation for Header only is sufficient.

UDP	TCP	IP
Checksum Calculation is done on (Header + Data)	Checksum calculation is done on (Header + Data)	Checksum Calculation done on Header only

IP Header Checksum calculation at the Sender:



$(35761)_D$

(1) what is the Version of IP (Ans ~~version 4~~ Version → 4)

(2) what is the length of Header (Ans 5 × 4 Bytes = 20 Bytes)

(3) what is the length of data (Ans Total length − Header length
= 28 − 20
= 8 Bytes)

(4) what is the identification no of IP datagram (Ans → 1)

(5) what is the fragment offset? (Ans offset = 0)

(6) Is fragmentation done? (Ans NO as DF bit is not set to 1)

(7) what is the value of TTL field (Ans 4 secs)

(8) which protocol is following IP (Ans UDP ∵ protocol field = 17)

(9) what is source IP address (Ans 10.12.14.5)

(10) what is destination IP address (Ans 12.6.7.9).

Checking of checksum calculation at the receiver

4	5	0	28
1		0	0
4	17	35761	
10.12.14.5			
12.6.7.9			

01000101	00000000 4,5&0
00000000	00011100 28
00000000	00000001 1
00000000	00000000 0
00000100	00010001 4&17
10001011	10110001 Checksum
00001010	00001100 10&12
00001110	00000101 14&5
00001100	00000110 12&6
00000111	00001001 7&9
11111111	11111111 → Sum
00000000	00000000 → checksum (1's complement of sum)

∵ Checksum = 0
The packet is w/o any error.

$(35761)_D = (1\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1)_B$

32768 16384 8192 4096 2048 1024 512 256 128 64 32 16 8 4 2 1

2^{15} ... 2^0

```
  1 2 4
  32768
+  2048
    512
    256
    128
     32
     16
      1
-------
  35761 ✓
```

Examples

Q.1. Calculate the HLEN value if the total length is 1200 bytes, 1176 of which is data from upper layer.

→ HLEN = Total length - data length
= 1200 - 1176
= 24 bytes.

Q.2. Given a fragmented datagram with an offset of 120, how can you determine the first & last byte number?

→ 120 × 8 = 960 → 1st Byte no

960 + (Data length - 1)
= Last byte number.

Q.3. What is the max number of routers that can be recorded if the timestamp option has a flag value of 1? why?

→ 1 router at the max because the TTL value will become zero (1-1) at this router. So packet will not be forwarded further.

Q.4. The value of HLEN in an IP datagram is 7. How many options bytes are present?

→ HLEN = 7 ⇒ 7 × 4 = 28 Bytes

∴ 28 − 20 = 8 Bytes option is present.
(20 ← fixed HLEN)

Q.5. The size of the option field of an IP datagram is 20 bytes. What is the value of HLEN? What is the value in binary?

→ Value of HLEN = 10 [5 + 5]
(5 ↓ for fixed HLEN; 5 ↓ for options (5 × 4) = 20 Bytes.)

Value in Binary = 1010

Q.6. The value of the total length field in an IP datagram is 36 & the value of the header length field is 5. How many bytes of data is the packet carrying?

→ Header length = 5 × 4 bytes = 20 bytes

Data length = Total length − Header length
= 36 − 20
= 16 Bytes

∴ Packet is carrying 16 Bytes of data.

Q.7. A datagram is carrying 1024 bytes of data. If there is no option information, what is the value of the header length field? What is the value of the total length field?

→ Value of HLEN will be 5 (i.e 20 Bytes) (w/o Options)

Total length = HLEN + Data
= 20 Bytes + 1024 = 1044 Bytes

Q. 8. A host is sending 100 datagrams to another host. Pg-15
If the identification number of the first datagram is 1024, what is the identification number of last datagram?

→ first datagram Identification no = 1024

Identification no of last datagram
= 1024 + 100
= 1124

Q. 9. An IP datagram arrives with fragmentation offset of 0 & an M bit (more fragment bit) of 0. Is this a first fragment, middle fragment, or last fragment?

→ M = 0 ⇒ No fragmentation

∴ It is the last fragment.

Q. 10. An IP fragment has arrived with an offset value of 100. How many data bytes of data were originally sent by the source before the data in this fragment?

→ offset values will range from 000 to 100
total 101 ⇒ 101 data bytes were originally sent by the source

But 100 data bytes were sent before the data in this fragment.

Q.11 An IP datagram has arrived with the following information in the header (in hexadecimal)

45 00 00 54 00 03 00 09 20 06 00 00 7C 4E 03 02 B4 0E 0F 02

Ver | HLEN | TOS | Total length | Identification | Flags & Offset | TTL | Protocol | Checksum | SIP | DIP

a. Are there any options? [No options as HLEN = 5 = 5 × 4 = 20 Bytes]

b. Is the packet fragmented? [No ∵ M flag = 0]

c. What is the size of data? [54 H = 01010100 B = 84 Bytes Total ∴ Data size = 34 - 20 = 64 Bytes]

d. Is a checksum used? [No ∵ checksum field is zero]

e. How many more routers can the packet travel to?

[TTL = 20 ⇒ 20 routers]

f. What is the identification no? [0003]

g. What is the Type of Service? [TOS = 00 ↳ Internet]

Q.12. In a datagram, the M bit is zero, the value of HLEN is 5, the value of total length is 200, & the offset value is 200. What is the no of the first byte & number of the last byte in this datagram? Is this the last fragment, the first fragment, or a middle fragment?

→ M = 0, HLEN = 5 ⇒ header = 20 Bytes, Total length = 200 ⇒ Data Bytes = 200 − 20 = 180 Bytes

↳ last fragment

No of 1st Byte = 200 × 8 = 1600

+ 179

No of last Byte ← 1779 ← Total 180 Bytes

4.2. Internet Control Message Protocol,

Shubhangi Kherde

- Introduction
  - Position of ICMP in the n/w layer
  - ICMP encapsulation
- Messages
  - Message format
  - Error reporting messages
  - Query messages.

Introduction:

- The IP protocol has no error reporting or error-correcting mechanism
- The IP protocol also lacks a mechanism for host and management queries.
- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.
- It is the companion to IP protocol.
- ICMP itself is a n/w layer protocol.
- However, its messages are not passed directly to the data link layer. Rather they are encapsulated in IP datagrams & then forwarded to data Link layer.
- The value of the protocol field in the IP datagram is 1 to indicate that the IP data is an ICMP message.

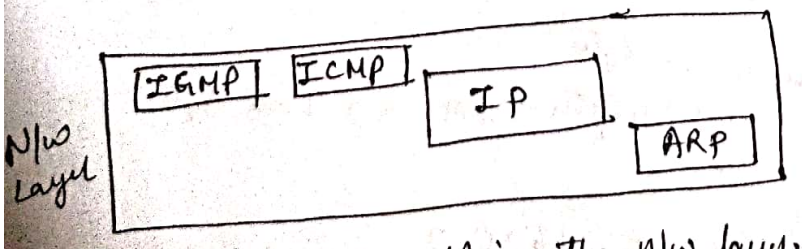


fig: Position of ICMP in the n/w layer.

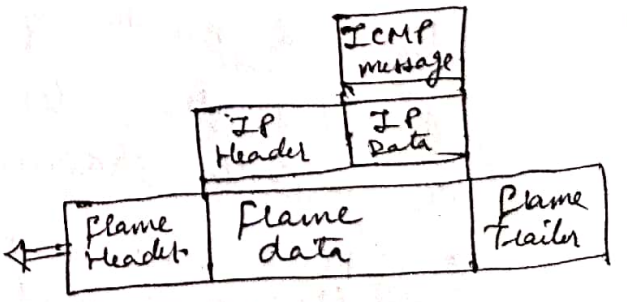


fig: ICMP Encapsulation.

Messages:

- ICMP messages are divided into two broad categories: Error-reporting messages and Query message.
- The Error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The Query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

for e.g. nodes can discover their neighbors.

Also, hosts can discover and learn about routers in their network and routers can help a node redirect its messages.

Table below lists the ICMP messages in each category.

ICMP messages

Category	Type	Message
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query Messages	8 or 0	Echo Request or reply
	13 or 14	Timestamp request or reply.

Message format

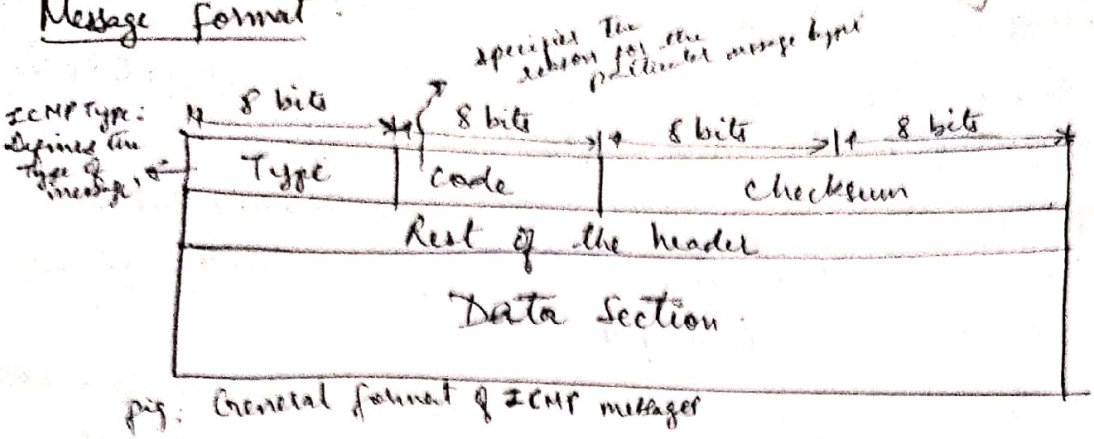
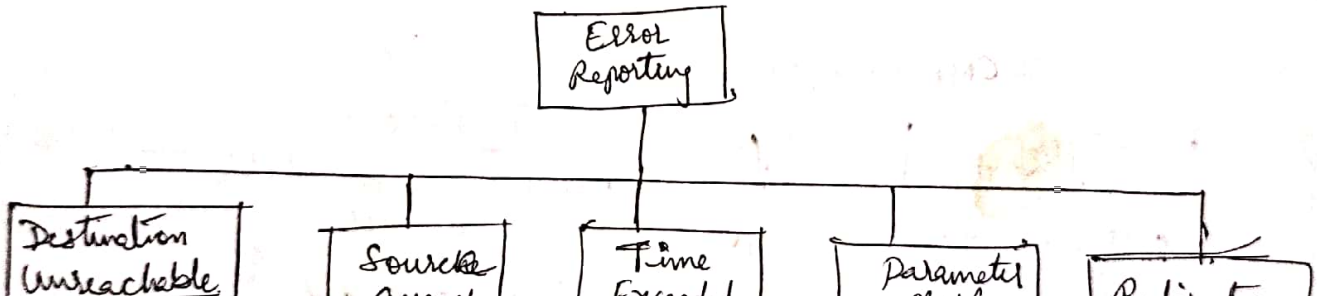
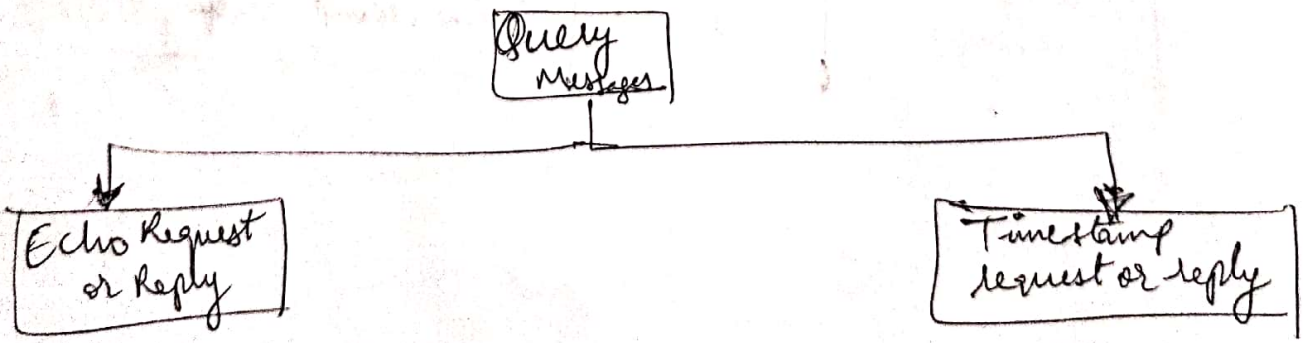


fig: General format of ICMP messages

ICMP always reports error messages to the original source

Error Reporting Messages



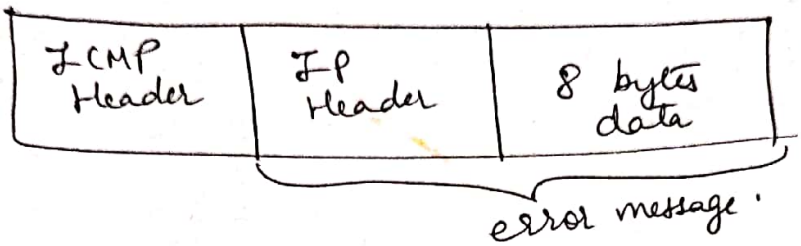


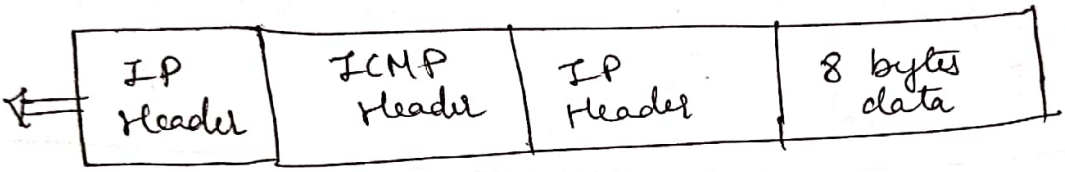
Error Reporting messages

Destination Unreachable	Source Quench	Time Exceeded	Parameter problems	Redirection
• Router or host sends the destination unreachable message to the originating source host.	• Router or host sends the source quench message to the originating source host.	• Router sends the time exceeded message to the original source.	• Router or host sends the parameter problem message to the original source.	• Router sends redirection messages to a host in order to update its routing table.
• Destination unreachable message is sent if the the router cannot route a datagram or a host cannot deliver a datagram. • Destination - unreachable messages with codes 2 & 3 can be created only by the destination host. Other destination - unreachable messages can be created only by routers. • A router cannot detect all problems that prevent the delivery of a packet.	• There is no flow - control or congestion control mechanism in the IP protocol. • Source - quench message in ICMP was designed to add a kind a flow control and congestion control to the IP. • A Source quench message informs the source that a datagram has been discarded due to congestion in a router or destination host. The source must slow down the sending of datagrams until the congestion is relieved. • one ICMP message per datagram	• Whenever a router decrements a datagram with a time - to - live value to zero, it discards the datagram & sends a time exceeded message to the original source. • When the final destination does not receive all of the fragments in a set of time, it discards the received fragments & sends a time - exceeded message to the original source. • In a time exceeded message, code 0 is used only by routers to show that the value of the time - to - live field is zero. code 1 is used only by the destination host to show that not all of the fragments are received within a set of time.	• A parameter - problem message can be created by a router or the destination host. • A host usually starts with a small routing table that is gradually augmented & updated. one of the tools to accomplish this is the redirection message. • A redirection message is sent from a router to a host on the same n/w.	• A host usually starts with a small routing table that is gradually augmented & updated. one of the tools to accomplish this is the redirection message. • A redirection message is sent from a router to a host on the same n/w.

No ICMP error Messages are generated for a datagram; (pg-21)

1) carrying an ICMP error message.
2) If it is not the first fragment.
3) having multicast address.
4) having special address such as 127.0.0.0 or 0.0.0.0





Error Reporting Messages in Details:

(1) Destination-Unreachable form Message:

When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded & the router or host sends a destination-unreachable message back to the source host that initiated the datagram.

Type: 3	code: 0 to 15	Checksum
unused (All 0s)		
part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

code 0 : The n/w is unreachable
code 1 : The host is unreachable.
Code 2 : The protocol is unreachable
code 3 : The port is unreachable
code 4 : Fragmentation is reqd but DF bit is set
code 5 : Source routing cannot be accomplished.
code 6 : The destination n/w is unknown.
Code 7 : The destination host is unknown.
code 8 : The source host is isolated.
code 9 : comm with the destination ~~host~~ network is administratively prohibited.
code 10 : comm with the destination host is administratively prohibited.
code 11 : The n/w is unreachable for specified type of service.
code 12 : The host is unreachable —11—
code 13 : The host is unreachable because the administrator has put a filter on it.
code 14 : The host is unreachable because the host precedance is violated.
code 15 : The host is unreachable because its precedance was cut off.

created only by host

code 0,1 & code 4,15 created by routers only.

* A router cannot detect all problems that prevent the delivery of a packet.

e.g. packet routed thro Ethernet is not acked & so router may give destination unreachable message though the datagram is delivered correctly.

(2) Source Quench :

- The IP protocol is a connectionless protocol.
- There is no communication bet" the source host, which produces the datagram, the routers, which forward it, and the destination host, which process it.
- One of the ramifications of this absence of communication is the lack of flow control & congestion control.

> There is no flow-control or congestion control mechanism in the IP protocol

The Source-Quench message in ICMP was designed to add a kind of flow control and congestion control to the IP. When a

- when the router or host discards a datagram due to congestion it sends a source quench message to the sender of the datagram.
- This message has 2 purposes :
  1) It informs the source that the datagram has been discarded.
  2) It warns the source that there is a congestion somewhere in the path that the source should slow down (quench) the sending process.

Fig: Source Quench format

Type: 4	code: 0	Checksum
Unused (All 0s)		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

Checksum:

- ICMP Checksum is calculated over the entire message (header & data)

Checksum Calculation

The sender follows these steps using one's complement arithmetic:

1) The checksum field is set to zero.
2) The sum of all the 16-bit words (header & data) is calculated.
3) The sum is complemented to get the checksum.
4) The checksum is stored in the checksum field.

Checksum testing

The Receiver follows these steps using one's Complement arithmetic:

1) The sum of all words (header & data) is calculated.
2) The sum is complemented.
3) If the result obtained in step 2 is 16 0's the message is accepted, otherwise, it is rejected.

Checksum calculation for a single Echo Request message. Here identifier = 1 & Seq no = 9. Pg25

8 (Type)	0 (Code)	0 (checksum)
1 (identifier)		9 (Seq no)
TEST (data)		

00001000 00000000 → 8 & 0
00000000 00000000 → 0
00000000 00000001 → 1
00000000 00001001 → 9
01010100 01000101 → T & E
01010011 01010100 → S & T

10101111 10100011 → sum
01010000 01011100 → checksum

T = 54 (Hex)
E = 45 H
S = 53 H
T = 54 H

---

(3) Time Exceeded : when → (i) TTL = 0
(ii) all fragments are not received in a set time at a destination

(1) TTL

- Routers use routing tables to find the next hop that must receive the packet.
- If there are errors in one or more routing tables, a packet can travel in a loop or a cycle; going from one router to the next or visiting a series of routers endlessly.
- We know that each datagram ~~visits the routers~~, contains a field called time to live that controls this situation.
- When a datagram visits a router, the value of this field is decremented by 1.
- When the time to live value reaches 0, after decrementing, the router discards the datagram.
- However, when the datagram is discarded, a Time Exceeded message must be sent by the router to the original source.

Whenever a router discards a datagram with a time to live value of zero, it discards the datagram & sends a time-exceeded message to the original source.

(ii) Fragments:

- A Time exceeded message is also generated when all fragments that make up a message do not arrive at the destination host within a certain time limit. When the first fragments arrives, the destination host starts a timer. If all the fragments have not arrived when the time expires, the destination discards all the fragments and sends a time exceeded message to the original sender.

When the final destination does not receive all of the fragments in a set time, it discards the received fragments & sends a time exceeded message to the original source.

Type: 11	Code: 0 or 1	Checksum
unused (All 0's)		
Part of received IP datagram including IP header plus the first 8 bytes of datagram data		

In a time-exceeded message, code 0 is used only by routers to show that the value of the time-to-live field is zero. Code 1 is used only by the destination host to show that not all of the fragments have arrived within a set of time.

(4) Parameter Problem

Any ambiguity in the header part of a datagram can create serious problems as the data travels through the Internet. If a router or the destination host discovers an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source.

> A parameter problem can be created by a router or a destination host

Type : 12	Code : 0 or 1	Checksum
Pointer	unused (All 0s)	
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

fig: parameter problem format

- **Code 0**: There is an error or ambiguity in one of the header fields.
  - In this case the value of the pointer field points to the byte with the problem. For example, if the value is zero, then the first byte is not a valid field.
- **Code 1**: The required part of an option is missing. In this case, the pointer is not used.

(5) Redirection

When a router needs to send a packet destined for another network, it must know the IP address of the next appropriate router. The same is true if the sender is a host. Both routers and hosts then must have a routing table to find the address of the router or the next router.

router	host
routing table is dynamic (keeps on updating), large size (more no of entries)	routing table is static (does not keep on updating), mostly single entry (small size) for next hop router addr.

Due to limited entry in the routing table of a host (that too for a default router), the host may deliver a packet to a wrong router in another n/w.

So correct such a host it is updated with the proper routing information in a n/w by the router by sending redirection message.

RM: Redirection message.

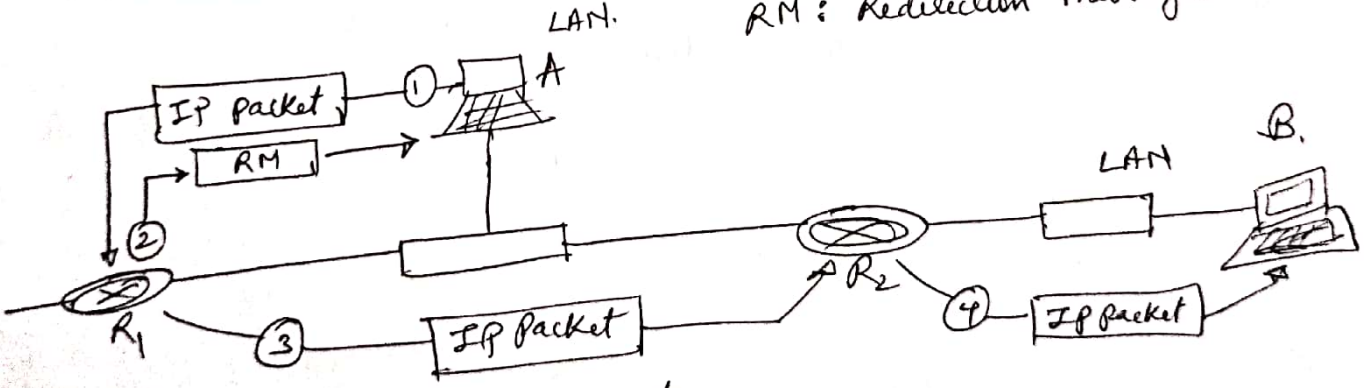


fig: Redirection concept.

A host usually starts with a small routing table that is gradually augmented and updated. One of the tools to accomplish this is the redirection message.

Type: 5	Code: 0 to 3	Checksum
IP address of the target router.		
Part of the received IP datagram including IP header plus the first 8 bytes of datagram data		

fig: Redirection message format.

Although the redirection message is considered an error reporting message, it is different from the other error messages. The router does not discard the datagram in this case; it is sent to the appropriate router. The code field for the redirection message narrows down the redirection:

- Code 0. Redirection for a network-specific route
- Code 1 Redirection for a host specific route
- Code 2 Redirection for a network-specific route based on a specified type of service.
- Code 3 Redirection for a host-specific route based on a specified type of service.

A redirection message is sent from the router to a host on the same Local network

Query Messages

In addition to error reporting, ICMP can also diagnose some network problems. This is accomplished through the query messages. These messages occur in pairs:

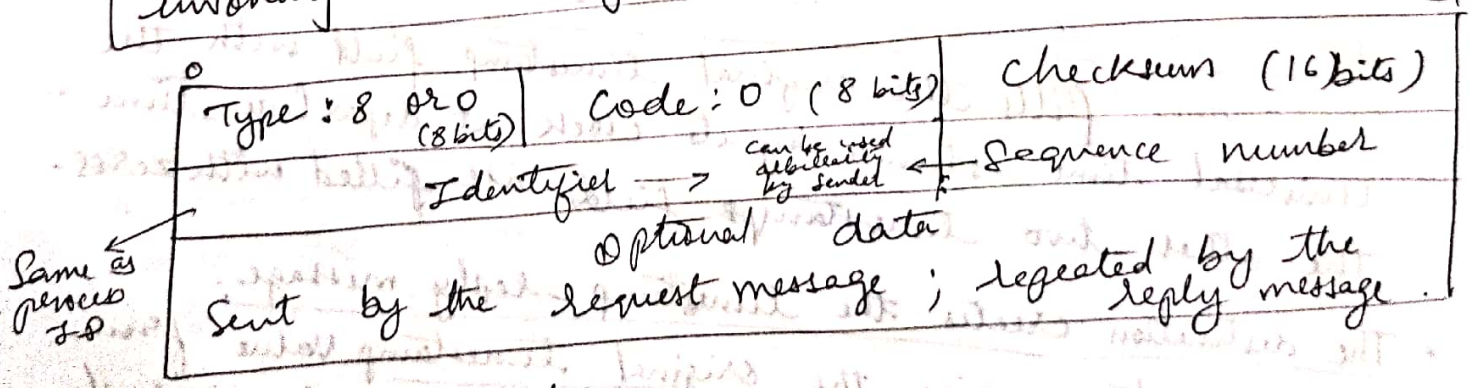
1) Echo request & reply
2) Timestamp request & reply.

1) Echo Request & Reply

- Designed for diagonistic purposes
- An echo-request message can be sent by a host or router. An echo reply message is sent by the host or router that receives an echo-request message.
- The receipt of echo reply for the sent echo request by a host gives a proof that IP protocols in sender & received are communicating with each other using IP datagram.
- Also it is the proof that the intermediate routers are receiving, processing & forwarding IP datagrams.

Thus, Echo-request and echo reply messages can be used by the network managers to check the operation of the IP protocol.

Echo-request & echo reply messages can test the reachability of a host. This is usually done by invoking the ping command.

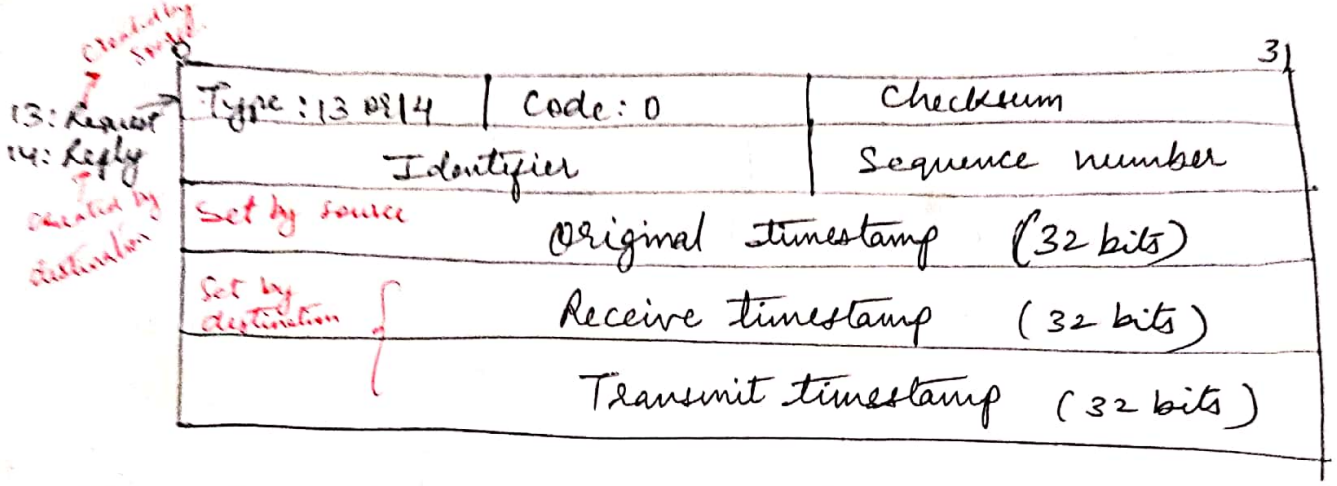


Type 8: Echo request
Type 0: Echo reply.

fig: Echo request & reply messages

2) Timestamp Request and Reply → RTT synchronization (Pg-31)

Two machines (hosts or routers) can use the timestamp-request & timestamp-reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.



Timestamp value = 24 hrs × 60 min × 60 sec × 1000 ms

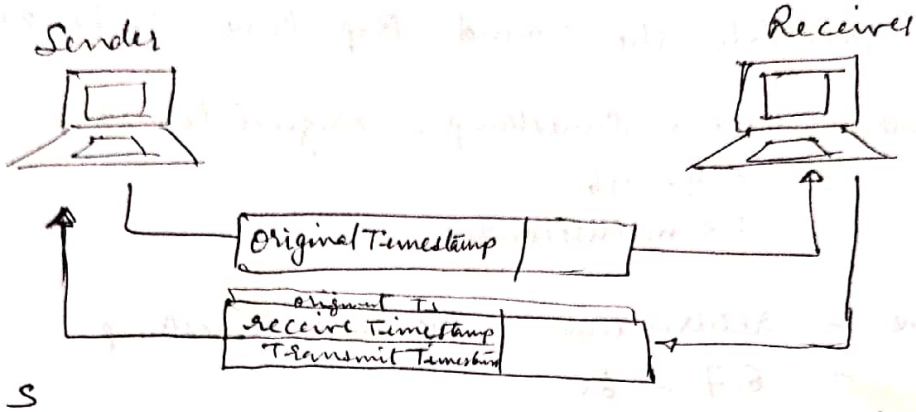
= 86,400,000 ms

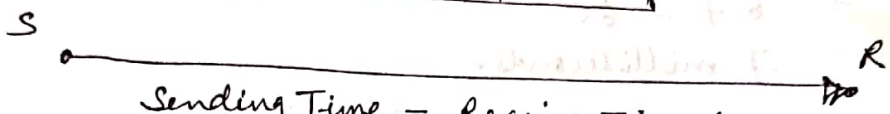
* Timestamp value cannot exceed 86400000 through $2^{32} = 4,294,967,295$

- **The source creates a timestamp-request message.**
  The source fills the original timestamp field with the Universal time shown by its clock at departure time. The other two timestamps fields are filled with zeros.

- **The destination creates the timestamp-reply message.**
  The destination copies the original timestamp value from the request message into the same field in its reply message. It then fills the receive timestamp field with the Universal time shown by its clock at the time the request was received. Finally, it fills the transmit timestamp field with the Universal Time shown by its clock at the time the reply message departs.

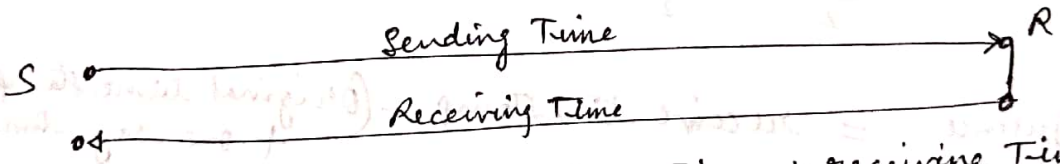
The timestamp-request and timestamp-reply messages can be used to compute the one-way or round trip time required for a datagram to go from a source to a destination & then back again.





Sending Time = Receive Timestamp − Original Timestamp

Receiving Time = returned time − Transmit Timestamp



round Trip Time = Sending Time + receiving Time.

Note that the sending & receiving time calculations are accurate only if the two clocks in the source & destination machines are synchronized. However, the round trip calculation is correct even if the two clocks are not synchronized because each clock contributes twice to the round trip calculation, thus canceling any difference in synchronization.

Timestamp-request and timestamp-reply messages can be used to calculate the round trip time between a source and a destination machine even if their clocks are not synchronized.

For example, given the following information: Pg-33

Original Timestamp : 46 — Receive Timestamp : 59

Transmit Timestamp: 60 — Return time : 67

We can calculate the round trip time to be 20ms:

Sending time = receive timestamp - original timestamp
= 59 - 46
= 13 milliseconds.

Receiving time = Return time - Transmit timestamp
= 67 - 60
= 7 milliseconds.

Round trip time (RTT) = Sending time + receiving time
= 13 + 7
= 20 milliseconds.

One way time = $\frac{RTT}{2} = \frac{20}{2} = 10$ ms

Time difference in Synchronization = receive timestamp - (original timestamp + one way time)

= 59 - (46 + 10)
= 59 - 56
= 3 milliseconds.

The Timestamp-request and timestamp-reply messages can be used to synchronize two clocks in two machines if the exact one-way time duration is known.

The following 3 pairs of ICMP query messages are declared obsolete by IETF

1) Information request & reply (as its job is done by ARP)
2) Address Mask request & reply (-u- by DHCP)
3) Router solicitation & advertisement (-u- by DHCP)

Q.1. What is the minimum size of an ICMP packet? What is the maximum size of an ICMP packet?

→

Q.2. What is the minimum size of an IP packet that carries an ICMP packet? What is the maximum size?

→

Q.3. What is the minimum size of an Ethernet frame that carries an IP packet which in turn carries an ICMP packet? What is the maximum size?

→.

Q.4. How can we determine if an IP packet is carrying an ICMP packet?

→ We can determine if an IP packet is carrying an ICMP packet from the protocol field of IP packet.

If protocol field = 1 => ICM packet.

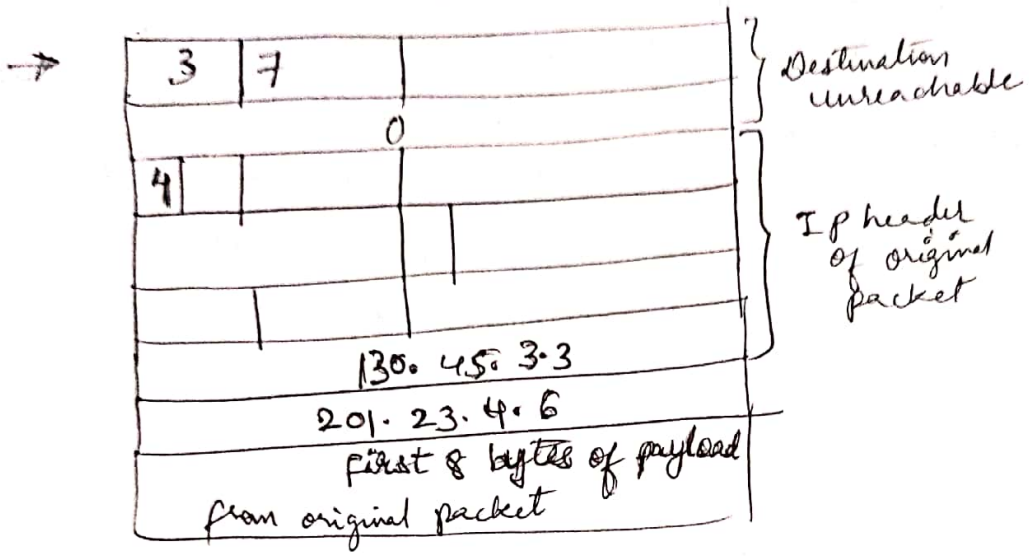
Q.5. Calculate the checksum for the following ICMP packet: Pg-35

Type: Echo Request Identifier: 123 Sequence Number: 25

Message HELLO.

→

Q-6. A router receives an IP packet with source IP address 130.45.3.3 & destination IP address 201.23.4.6. The router cannot find the destination IP address in its routing table. Fill in the fields (as much as you can) for the ICMP message sent.



Q-7. TCP receives a segment with destination port address 234. TCP checks and cannot find an open port for this destination. Fill in the fields for the ICMP message sent.

Q.8 An ICMP message has arrived with the header (in hexadecimal): (Pg-37)

03 0310 20 00 00 00 00

What is the type of the message? what is the code? What is the purpose of the message?

→ The Type in this message is 3, which means it is a destination unreachable message. The code in this message is 3, which means that the target port is unreachable. The purpose of this message is to inform the sender that the destination port is not available on the distination host at this time.

Q.9. An ICMP message has arrived with the header (in hexadecimal):

05 00 11 12 11 0B 03 02

what is the type of the message? what is the code? what is the purpose of the message? what is the value of the last 4 bytes? what do the last bytes signify?,

→ Type 05 → Redirection Message
code 00 → N/w specific route
checksum → 1112
IP address of target router → 11 0B 03 02 in Hex.

0001 0001, 0000 1011, 0000 0011, 0000 0010

IP adress → 17.11.3.2 in dotted decimal format.

Q.10. A computer sends a timestamp request. If its clock shows 5:20:30 A.M. (Universal Time), show the entries for the message.

Q.11. Repeat Q.10 for the time of 3:40:30 P.M. (Universal Time).

Q.12. A computer ser receives a timestamp request from another computer at 2:34:20 P.M. The value of the original timestamp is 52453000. If the sender clock is 5ms slow, what is the one-way time?

5.13. A computer sends a timestamp request to another computer. It receives the corresponding timestamp reply at 3:46:07 A.M. The values of the original timestamp, receive timestamp, and transmit timestamp are 13,560,000, 13,562,000 and 13,564,300 respectively. What is the sending trip time? What is the receiving trip time? What is the round-trip time? What is the difference between the sender clock & the receiver clock?

→

IPv4 Addresses

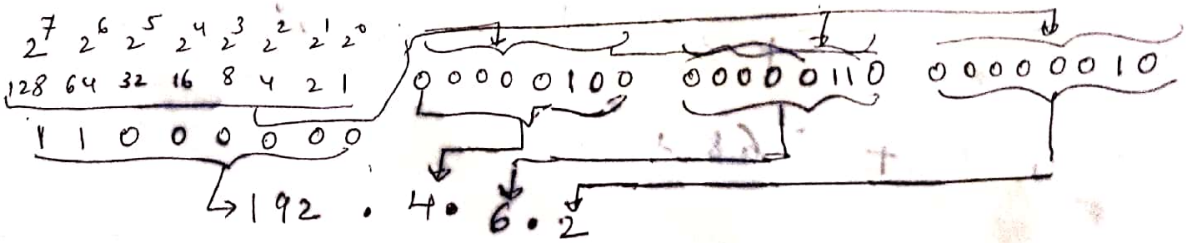
- An IP address identifies each host connected in Internet.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- The IPv4 addresses are unique and universal.
- The address space of IPv4 is 2^{32} or 4,294,967,296
- Representation of IPv4 addresses:

① Binary notation (Base 2)
↓
Base 2 since a binary no can take only 2 values

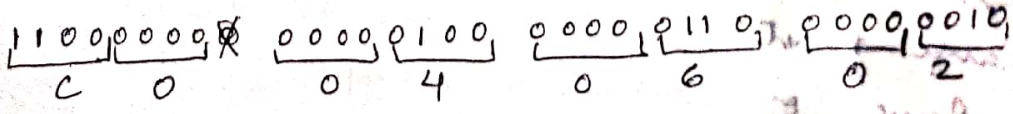
② Dotted-decimal notation (Base 256)
↓
Base 256 since an 8 bit decimal no can take maximum 256 values

③ Hexadecimal notation (Base 16)
↓
Base 16 since a hexadecimal no can take 16 values

e.g. 11000000 00000100 00000110 00000010
↳ Binary notation



∴ 192.4.6.2 ⇒ dotted decimal notation



∴ C0040602 ⇒ Hexadecimal notation

Range of Addresses

We often deal with a range of addresses instead of one single address.

We sometimes need to find the number of addresses in a range if the first & last address is given.

OR we need to find the last address if the first address & the number of addresses in the range are given.

Q.1 Find the number of addresses in a range if the first address is 146.102.29.0 & the last address is 146.102.32.255.

→

146.102.32.255 → Last Address

− 146.102.29.0 → First Address

0.0.3.255 ⇒ range of addresses in dotted decimal notation (i.e. base 256)

Let us now convert it in decimal range using base 256.

$$0 \times 256^3 + 0 \times 256^2 + 3 \times 256^1 + 255 \times 256^0$$

$$= 0 + 0 + 768 + 255$$

$$= 1023$$

But as the address starts from zero the above calculated range must be added with one.

∴ Range of addresses = 1023 + 1

= 1024 — Ans.

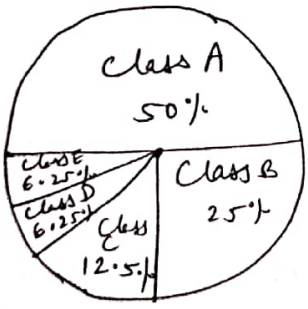
Q2. The first address in a range of addresses is 14.11.45.96. If the number of addresses in the range is 32, what is the last address?

→ To find last address add the first address with no of addres in range & then subtract one from it (as the 32 ⇒ 0.0.0.0 to 0.0.0.31)

14.11.45.96 ⇒ First address
\+ 32 ⇒ no of addresses in range.
14.11.45.128
\- 1
14.11.45.127 ⇒ Last address in range.

Classful Addressing :

. Here IP address space is divided into 5 Classes:
A, B, C, D & E



Class A : 2^{31} = 2147483643 addresses, 50%.
Class B : 2^{30} = 1073741824 addresses, 25%.
Class C : 2^{29} = 536870912 addresses, 12.25%
Class D : 2^{28} = 268435456 addresses, 6.25%
Class E : 2^{28} = 268435456 addresses 6.25%

Total 100%.

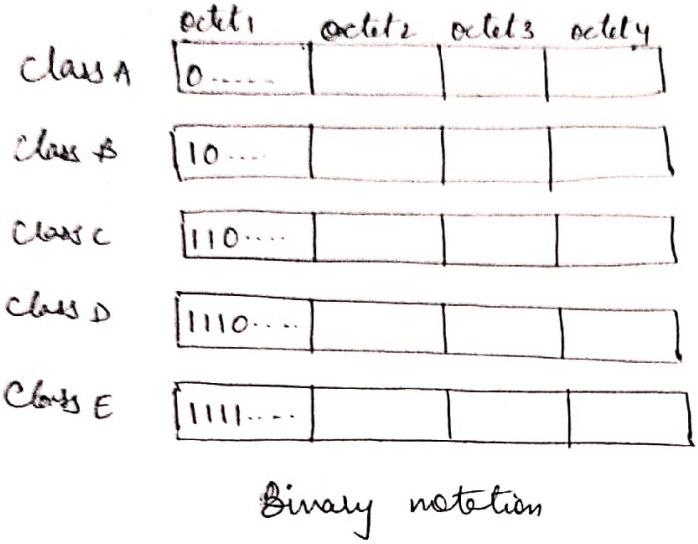
2^{31} in class A as 1 bit is required to identify class A n/w's
2^{30} in class B as 2 bits are —11— class B —11—
2^{29} in class C as 3 bits are —11— class C —11—
2^{28} in class D as 4 bits —11— class D —11—
2^{28} in class E as 4 bits —11— class E —11—

32 bits Total in IPV4 addr

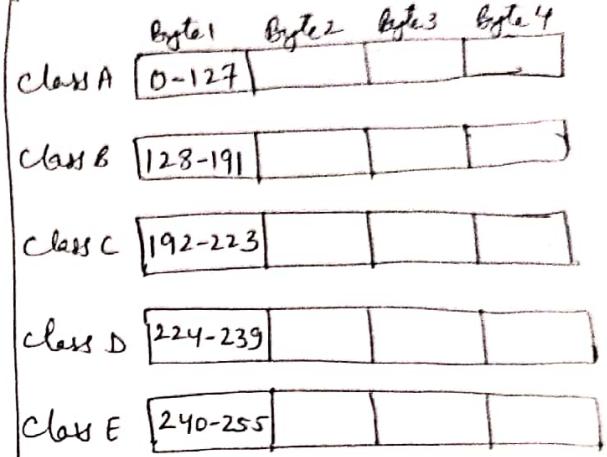
Recognizing Classes

Class of an IP address is recognized based on

- First few bits in binary notation
- First octet value in dotted decimal notation.



Binary notation



Dotted - decimal notation.

Q-3 Find the class of each address :

a. 00000001 00001001 00001011 11101111

→ It is a class A address as first bit is 0

b. 11000001 10000011 00011011 11111111

↳ Class C address

→ As first 3 bits are 110, it is class C address.

c. 10100111 11011011 10001011 01101111

→ As first 2 bits are 10, it is class B address.

d. 11110011 10011011 11111011 00001111

↳ Class E

→ As first 4 bits are 1111, it is class E address.

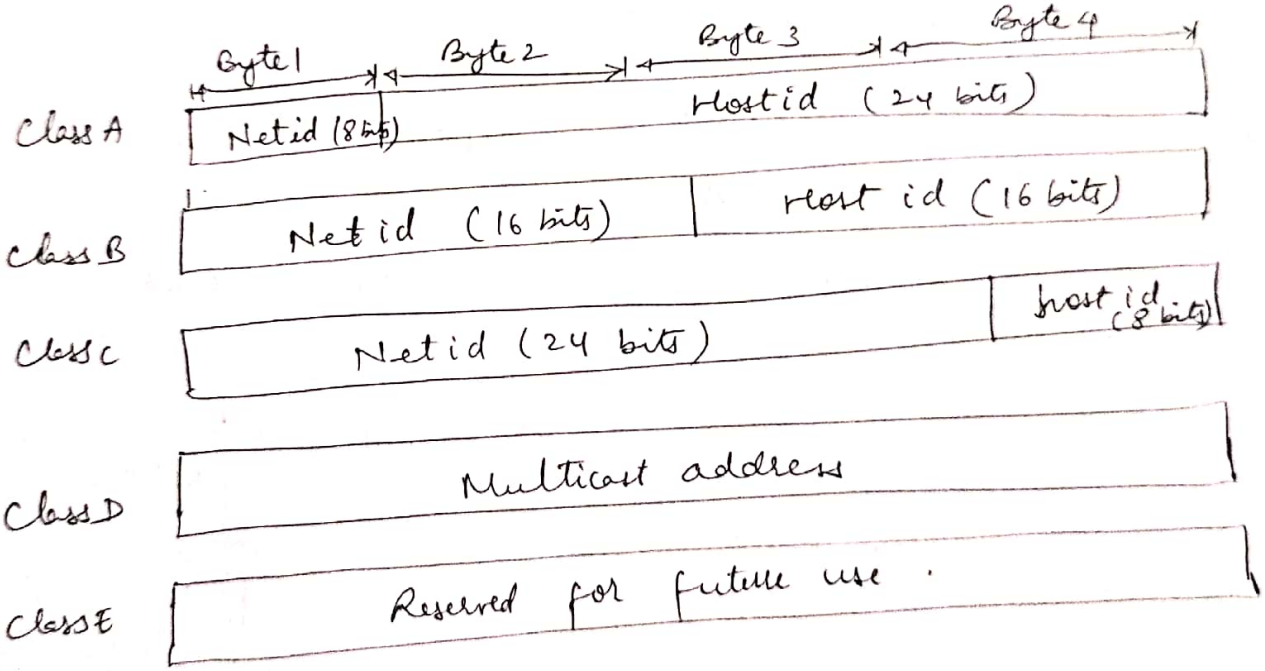
Q.4. Find the class of each Address

a. 227.12.14.87
b. 193.14.56.22
c. 14.23.120.8
d. 252.5.15.111

→ a. 227 lies bet" 224 & 239, so it is class D Address.
b. 193 lies bet" 192 & 223, so it is class C Address
c. 14 lies bet" 0 & 127, so it is class A Address
d. 252 lies bet" 240 & 255, so it is class E Address.

Netid and Hostid

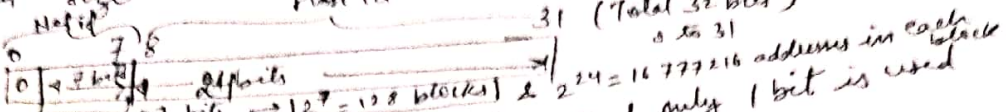
In classful addressing, an IP address in classes A, B & C is divided into netid & hostid.



Classes & Blocks

One problem with classful addressing is that each class is divided into a fixed number of blocks with each block having a fixed size.

① Class A



We know that Class A range is 0 to 127 & only 1 bit is used to identify class. Remaining 7 bits in Netid define no of blocks can be

∴ There are 128 blocks in class A which are assigned to 128 organizations.

- Each block with 2^{24} addresses = 16,777,216 address.

∴ Class A represent large size n/w's.

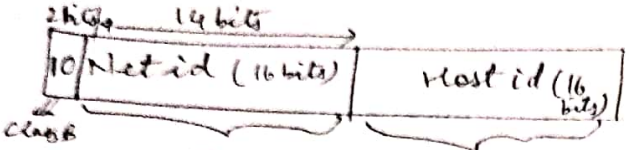
- Millions of addresses in class A are wasted as organizations may not need so many addresses.

Blocks in class A →

0.0.0.0 ⋮ 0.255.255.255	Netid 0	Block 1
1.0.0.0 ⋮ 1.255.255.255	Netid 1	Block 2
2.0.0.0 ⋮ 2.255.255.255	Netid 2	Block 3
⋮	⋮	⋮
127.0.0.0 ⋮ 127.255.255.255	Netid 127	Block 128

Class B (Range 128-191)

- We know that there are 16 bits in Netid & remaining 16 in Hostid of Class B IP address
- First 2 bits in Netid identify the class.
  So remaining 14 bits give the no of blocks in class B.
- ∴ No of Blocks in Class B = 2^{14} = 16384 blocks.



2^{14} = 16384 Blocks. 2^{16} addresses in each block = 65336 addresses in each block

Blocks in Class B →

128.0.0.0 ⋮ 128.0.255.255	Netid 128.0 } Block 1
128.1.0.0 ⋮ 128.1.255.255	Netid 128.1 } Block 2
128.2.0.0 ⋮ 128.2.255.255	} Block 3
⋮	⋮
128.255.0.0 ⋮ 128.255.255.255	Netid 128.255 } Block 256
⋮	⋮
191.255.0.0 ⋮ 191.255.255.255	Netid 191.255 } Block 16384

Again in class B addresses are more which cannot be used by many organizations.
So many class B addresses are wasted.

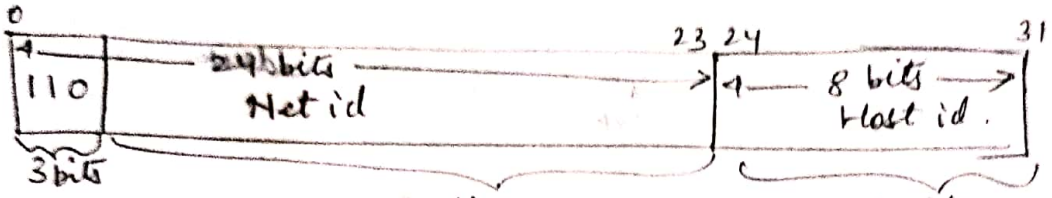
~~(2) Class B~~

(3) Class C.

We know that there are 24 bits in netid part & remaining 8 bits in hostid part of class C addresses.

We also know that the first 3 bits in netid part identify class C address.

∴ 24 − 3 = 21 bits can be used to calculate no of blocks in class C.



21 bits ⇓ 2^{21} = 2097152 blocks

8 bits ⇓ 2^8 = 256 addresses in each Block.

Class C range: 192–223

Blocks in class C →

192.0.0.0 ⋮ 192.0.0.255 } Net id 192.0.0] Block 1

192.0.1.0 ⋮ 192.0.1.255 } Net id 192.0.1] Block 2

192.0.2.0 ⋮ 192.0.2.255

192.0.3.0 ⋮ 192.0.3.255

⋮

192.0.255.0 ⋮ 192.0.255.255

192.1.0.0 ⋮ 192.1.0.255

⋮

192.255.255.0 ⋮ 192.255.255.255 } Net id 192.255.255

⋮

223.255.255.0 ⋮ 223.255.255.255 } Net id 223.255.255] Block 2097152

In Class C there are $2^8 = 256$ addresses in each block & not so many addresses organizations were satisfied with so small no of addresses.

④ Class D :

- There is only one block in Class D
- We know that first 4 bits (out of 32) identify the Class D address.
- ∴ Remaining 28 bits are used to determine no of addresses in class D block.
- ∴ There are $2^{28} = 268,435,456$ addresses in class D block.

We also know that Class D range is 224 to 239.

Class D

224.0.0.0 ----- 239.255.255.255
One block : 268,435,456 addresses

Class D addresses are made of one block, used for multicasting.

⑤ Class E

- There is just one block of Class E addresses.
- It was designed for use as reserved addresses.

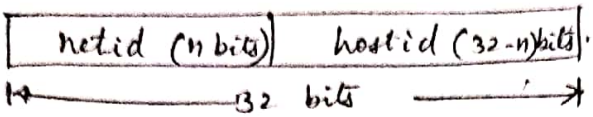
Single Block in Class E

240.0.0.0
⋮
255.255.255.255

One block = 268,435,456 addresses

Two-Level Addressing:

Each Address Block in classful addressing contains two parts: netid & hostid



e.g. of two-level addressing used in other comm systems like telephone system.

(022) 2772 6969

area code — Subscriber number.

Extracting Information in a Block

① No of addresses in a block, N, can be found using

$$N = 2^{32-n}$$

② 1st Address in a block:

Keep n leftmost bits

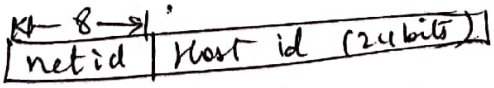
& set the (32-n) rightmost bits to all zeros

③ Last Address in a block:

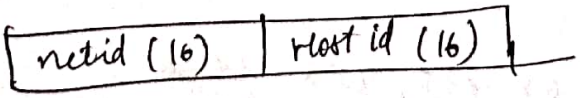
Keep n leftmost bits

& set the (32-n) rightmost bits to all ones

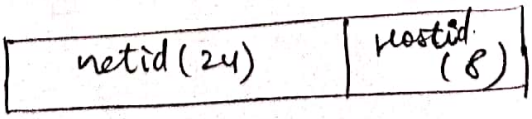
Class A



class B



class C



✓ Q.5 An address in a block is given as 73.22.17.25. Find the number of addresses in the block, the first address & the last address.

→ 73.22.17.25
→ first octet value is 73 → lies bet^n 0 & 127
→ ∴ The given addr is class A
→ class A has 8 bits in net id & 24 bits in Host id
→ ∴ $2^8 = 256$ blocks are there & $2^{24} =$ ( ) addresses in each block.
→ first addr is 73.0.0.0] ⇒ 2^{24} addresses.
→ Last addr is 73.255.255.255]

73.0.0.0 ⇒ n/w address
73.255.255.255 ⇒ Direct Broadcast address.

✓ Q.6. An address in a block is given as 180.8.17.9. Find the number of addresses in the block, the first address & the last address.

→ . Given IP 180.8.17.9 belongs to class B as first octet value is lying bet^n 128 & 191
. Class B has 16 bits each in net id & host id
∴ $2^{16} = 65536$ blocks are there & $2^{16} = 65536$ addresses in each block.
→ first addr is 180.8.0.0 → n/w addr] 2^{16} addresses.
→ Last addr is 180.8.255.255 → Direct BC address.

✓ Q.7. An address in a block is given as 200.11.8.45. Find the no of addresses in the block, the first address & the last address.

→ . Given IP 200.11.8.45 belongs to class C as first octet value (200) lies bet^n 192 & 223.
. class C has 24 bits in net id & remaining 8 in host id.
∴ $2^{24} =$ ( ) blocks in class C & $2^8 = 256$ addresses in each block.
→ first addr is 200.11.8.0 → n/w addr] 2^8 addrs.
→ Last addr is 200.11.8.255 → Direct BC address.

Network Mask:

Network mask or default mask is determined by setting all netid bits to 1 and all hostid bits to 0.

∴ for class A → default mask → 11111111 00000000 00000000 00000000
(netid (8 bits)) (Hostid = 24 bits)

= 255.0.0.0

for class B → default mask → 11111111 11111111 00000000 00000000
(net ID 16 bits) (Host ID 16 bits)

= 255.255.0.0

for class C → default mask → 11111111 11111111 11111111 00000000
(netid) (Host id)

= 255.255.255.0

Now Let us consider an IP addr 201.24.67.2 for which we need to determine the n/w addr.
Now here the n/w addr can be determined by bit wise ANDing the default subnet mask with the given IP addr.

→ 201.24.67.2 ⇒ Class C IP addr → 24 bits in netid & 8 bits Host id.
for class c default subnet mask is 255.255.255.0

```
11001001 00011000 01000011 00000010
11111111 11111111 11111111 00000000
AND
-----------------------------------
11001001 00011000 01000011 00000000
```

↳ 201.24.67.0 is the n/w addr.

Unsolved Examples Fourozan (Pg-52) page 154 4th edition.

Q.1. What is the address space in each of the following systems?

a. a system with 8-bit addresses

b. a system with 16-bit addresses

c. a system with 64-bit addresses.

Solution:

a. 2^8 = 256 addresses

b. 2^{16} = 65536 addresses

c 2^{64} = ( ) addresses

Q.2. An address space has a total of 1024 addresses. How many bits are needed to represent an address?

Solution:

$$2^x = 1024$$

$$\therefore \boxed{x = 10} \text{ bits}$$

Q.3 An address space uses three symbols: 0, 1, and 2 to represent addresses. If each address is made of 10 symbols, how many addresses are available in this system?

Solution:

$$3^{10} =$$

Q.4. Change the following IP addresses from dotted-decimal notation to binary notation:

(Pg-53)

a. 114.34.2.8
b. 129.14.6.8
c. 208.34.54.12
d. 238.34.2.1

Solution:

a. 114:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1
a. 0	1	1	1	0	0	1	0

114 = 64 + 32 + 16 + 2

a. 01110010 00100010 00000010 00001000
b. 10000001 00001110 00000110 00001000
c. 11010000 00100010 00110110 00001100
d. 11101110 00100010 00000010 00000001

Q.5. Change the following IP addresses from dotted-decimal notation to hexadecimal notation:

a. 114.34.2.8
b. 129.14.6.8
c. 208.34.54.12
d. 238.34.2.1

Solution:

a. 114.34.2.8 = 01110010 00100010 00000010 00001000
= 72220208 H

b. 129.14.6.8 = 10000001 00001110 00000110 00001000
= 810E0608 H

Q.6 Change the following IP addresses from hexadecimal notation to binary notation :

→ a. 0X13477FFAB = 00010011 01000111 11111110 10101011

b. 0XAB234102 = 10101011 00100011 01000001 00000010

c. 0X0123A2BF =

d. 0X00001111 =

Q.7. How many hexadecimal digits are needed to define the netid in each of the following classes ?

a. Class A

b. class B

c. class C

Solution:

a. In class A there are 8 bits in netid.

∴ 2 Hex digits are needed to define netid.

b In class B there are 16 bits in netid.

∴ 4 Hex digits are needed to define netid.

c. In class C there are 24 bits in netid.

∴ 6 Hex digits are needed to define netid.

Q.8 Change the following IP addresses from binary notation to dotted decimal notation :

a. 01111111 11110000 01100111 01111101 (128 64 32 16 8 4 2 1 / 128 64 32 16 8 4 2 1)

192 + 48 = 240 ; 96 + 7 = 103 ; 96 + 29 + 1 = 125

b. 1010 1111 11000000 11111000 00011101

c. 11011111 10110000 00011111 01011101

d. 11101111 11110111 11000111 00011101

Solution: a. 128.240.103.125

Q.9. Find the class of the following IP addresses: (Pg-55)

a. 208.34.54.12

b. 238.34.2.1

c. 242.34.2.8

d. 129.14.6.8

Solution:

a. First octet value is 208 which lies between 192 & 223 which is class C range.
∴ The IP belongs to class C

b. 238.34.2.1 ⇒ class D | ∵ Class D range is 224 to 239

c. 242.34.2.8 ⇒ class E | ∵ class E range is 240 to 255

d. 129.14.6.8 ⇒ Class B | ∵ Class B range is 128 to 191

Q.10 Find the class of the following IP addresses:

a. 1111 0111 1111 0011 1000 0111 1101 1101

b. 1010 1111 1100 0000 1111 0000 0001 1101

c. 1101 1111 1011 0000 0001 1111 0101 1101

d. 1110 1111 1111 0111 1100 0111 0001 1101

Solution:

a. 1111 0111 ⇒ 248 ⇒ Class E address.

256 − 8 = 248

b. 1010 1111 ⇒ 176 ⇒ Class B address

256 − 64 = 192; 192 − 16 = 176

c.

d.

Q.11 Find the netid and the hostid of the following IP addresses:

a. 114.34.2.8

b. 132.56.8.6

c. 208.34.54.12

d. 251.34.98.5

Solution:

a. 114.34.2.8

octet 1 value 114 lies in the range 0 to 127

∴ The address belongs to class A

In class A netid = 8 bits host id = 24 bits.

∴ netid = 114.0.0.0

hostid = 34.2.8

b. 132.56.8.6 ⇒ Class B

netid → 132.56

hostid → 8.6

c. 208.34.54.12 ⇒ Class C

netid 208.34.54

Hostid 12

d. 251.34.98.5 ⇒ Class E

pg-57

Q.12 Find the number of addresses in the range if the first address is 14.7.24.0 & the last address is 14.14.34.255

Solution:

Last address → 14.14.34.255

Subtract → − First address → 14.7.24.0

Ragage → 0.7.10.255

∴ Entire range is 0.0.0.0 to 0.7.10.255

$0 \times 256^3 + 7 \times 256^2 + 10 \times 256^1 + 255 \times 256^0$ | ∵ dotted decimal format has Base 256.

= ( )

∴ Number of addresses = ( ) + 1

= ____

∵ first address begins from 0.0.0.0

Q.13. If the first address in a range is 122.12.7.0 & there are 2048 addresses in the range, what is the last address?

Solution:

$\frac{2048}{256} = 8 \Rightarrow$ 8 Subnetworks each of 256 addresses are needed.

∴ 122.12.7.0 : .255 → ①

122.12.8.0 : 255 → ②

⋮

122.12.14.0 → ⑧

14.255

∴ Last address is 7+8=15

122.12.14.255

Verification → 122.12.14.255 − 122.12.7.0 = 7.255

range is 0.0.0.0 to 0.0.7.255

No of addresses $(0 \times 256^3 + 0 \times 256^2 + 7 \times 256^1 + 255) + 1$

= 2048

Q.14 Find the result of each operation:

a. NOT (22.14.70.34)
b. NOT (145.36.12.20)
c. NOT (200.7.2.0)
d. NOT (11.20.255.255)

Solution:

a. NOT (22.14.70.34)

= NOT (00010110 00001110 01000110 00100010)

= 11101001 11110001 10111001 11011101

Q.15. Find the result of each operation:

a. (22.14.70.34) AND (255.255.0.0)
b. (12.11.60.12) AND (255.0.0.0)
c. (14.110.160.12) AND (255.200.140.0)
d. (28.14.40.100) AND (255.128.100.0)

Solution:

a.
```
  00010110 00001110 01000110 00100010
AND 11111111 11111111 00000000 00000000
-----------------------------------------
  00010110 00001110 00000000 00000000
```

= 22.14.0.0

b. 12.11.60.12 AND 255.0.0.0 = 12.0.0.0

c. 14.110.160.12 AND 255.200.140.0 14.64.128.0

```
  01100100 . 10100000
AND 11001000 . 10001100
-----------------------
  01000000 . 10000000
```

⇒ 64 . 128

Q.16. Find the result of each operation:

(a) (22.14.70.34) OR (255.255.0.0)

(b) (12.11.60.12) OR (255.0.0.0)

(c) (14.110.160.12) OR (255.200.140.0)

(d) (28.14.40.100) OR (255.128.100.0)

Solution:

(a) 255.255.70.34 → Ans

(b) 255.11.60.12 → Ans.

(c)

```
  00001110 01101110 10100000 00001100
OR 11111111 11001000 00001100 00000000
-----------------------------------------
  11111111 11101110 10101100 00001100
```

⇒ 255.239.172.12

Q.17 In a class A subnet, we know the IP address of one of the hosts and the subnet Mask as given below:

IP address 25.34.12.56

Subnet Mask 255.255.0.0

What is the first address (subnet address)?

What is the last address?

Solution:

25.34.12.56 → Class A

255.255.0.0 → Subnet Mask

To get subnet address AND given IP with Mask.

```
  25.34.12.56
AND 255.255.0.0
-----------------
  25.34.0.0
```

⇒ subnet address

The given mask has 16 bits high &
∴ Remaining 16 bits provide the no of addresses in a subnet.
i.e. $2^{16} = 65536$ addresses in a subnet.
∴ If 25.34.0.0 is subnet address Then
last address is 25.34.255.255 → special address (Direct Broadcast address)

Q.18 In a Class B subnet, we know the IP Address of one of the hosts and the subnet Mask as given below:

IP address : 131.134.112.66
Subnet Mask : 255.255.224.0

what is the first address (subnet address) ?
what is the last address ?

Solution :
Subnet Mask is 255.255.224.0
⇒ 11111111 11111111 111,00000 00000000
⇒ 19 bits are high
⇒ /19 notation
⇒ 19 bits in netid & subnetid part & remaining (32-19) = 13 bits in hostid part

But 16 bits in netid in class B
So remaining 3 bits in subnetid.
↳ $2^3 = 8$ subnetworks

∴ 2^{13} addresses in each subnetwork.
& $2^{13} = 2^{10} \times 2^3 = 1024 \times 8 = 8192$ addresses.

Now $\frac{8192}{256} = 32 \Rightarrow$ 32 subnetworks. → range 0.0.0.0 to 0.0.31.255

Now 10000011 10000110 01110000 01000010 → IP addr. 112 +31 143
AND 11111111 11111111 11100000 00000000

10000011 10000110 01100000 00000000
⇒ 131.134.112.0 → subnet address.
131.134.143.255 → Last address.

Q.19. In a class C subnet, we know the IP address of one of the hosts and the subnet mask as given below:

IP address: 202.44.82.16

Subnet Mask: 255.255.255.192

What is the first address (subnet address)? What is the last address?

Solution:

IP address 202.44.82.16 .16 ⇒ 00010000

Subnet Mask 255.255.255.192 AND .192 ⇒ 11000000 AND

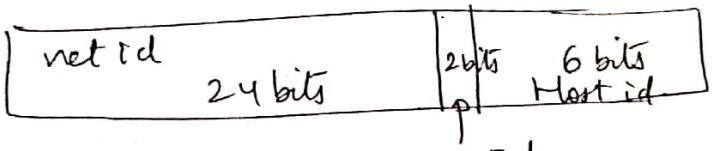
00000000

202.44.82.0 ⇒ Subnet address.

26 bits are high in mask.

for class C → 24 bits in net id

with subnetting (26-24) = 2 bits in subnet id.



Subnet id

$2^2 = 4$ subnets

$\therefore 2^6 = 64$ Hosts per subnetwork.

202.44.82.0/26 → Subnetwork addr.

Subnet 1

202.44.82.63/26 → Last addr. of 1st subnet.

64 ⇒ 0 to 63

202.44.82.64/26

Subnet #2 .127/26

.128/26

Subnet #3 .191/26

Subnet #4 202.44.82.192

202.44.82.255 — Last addr.

Q.20. Find the Subnet Mask in each case :

(a) 1024 Subnets in class A

(b) 256 Subnets in class B

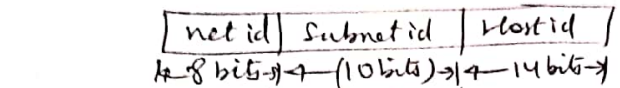
(c) 32 Subnets in class C

(d) 4 Subnets in class C

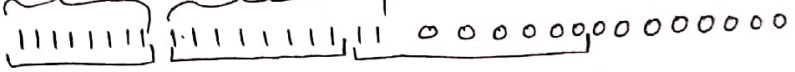
Solution :

(a) 1024 Subnets in class A means 10 bits in subnet id part.

[∵ $2^x = 1024$
∴ $x = 10$



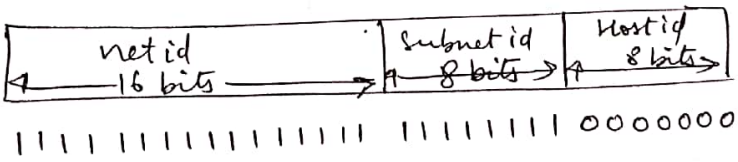
∴ Subnet mask is



255. 255. 192. 0 /18

(b) 256 Subnets in class B

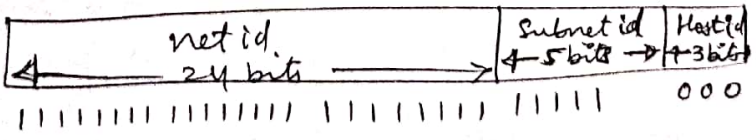
i.e. 8 bits in subnet id



∴ Subnet Mask is 255. 255. 255. 0 /24

(c) 32 Subnets in class C

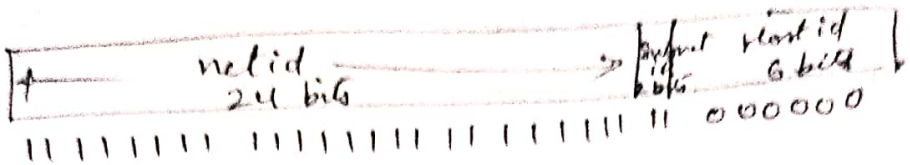
means 5 bits in subnet id



∴ Subnet Mask is 255. 255. 255. 248 /29

d. 4 Subnets in class C

means 2 bits in Subnet id part



∴ Subnet Mask is 255.255.255.192 /26

Q. 21 In a block of addresses, we know the IP address of one host is 25.34.12.56/16. What is the first address (network address) & the last address (limited broadcast address) in this block?

Solution:

25.34.12.56/16

Prefix is 16 (& Suffix is 16 ⇒ 2^{16} hosts)

∴ Subnet mask is 255.255.0.0

∴ n/w add is (25.34.12.56) AND (255.255.0.0)

i.e. = 25.34.0.0 /16

& limited Broadcast address is

25.34.255.255/16

↳ All bits high in Suffix part.

Q. 22. In a block of addresses, we know the IP address of one host is 182.44.82.16/26. What is the first address (network address) & the last address (limited broadcast address) in this block?

Solution:

IP address of host is 182.44.82.16/26

/26 means 26 bits are high in Subnet mask

∴ the mask becomes

255.255.255.192/26

Network addr = (IP Addr) AND (Subnet Mask).

∴ network addr = (182.44.82.16) AND (255.255.255.192)

= 182.44.82.0

.16 00010000
AND 192 11000000
00000000

/26 ⇒ 6 bits in host id.

∴ 2^6 hosts = 64

∴ range 0 to 63

& limited Broadcast addr is 182.44.82.63 (last address)

∴ 182.44.82.0/26 → first addr (N/W addr).

⋮

182.44.82.63/26 → last addr. (limited BC addr)

Q. 23 In fixed length Subnetting, find the number of 1s that must be added to the mask if the number of desired Subnets is

(a) 2
(b) 62
(c) 122
(d) 250

Solution:

(a) for 2 subnets only one 1 must be added to the mask ($\because 2^1 = 2$)

(b) for 62 subnets; Six 1s must be added to the mask ($\because$ 62 is not power of 2 & $2^6 = 64$ nearest value).

(c) for 122 subnets; Seven 1s

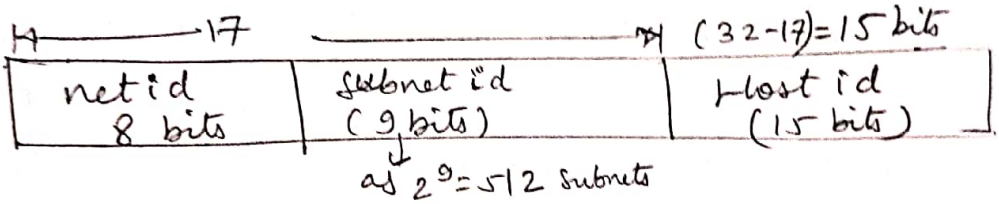
(d) for 250 subnets; eight 1s

Q.24 An organization is granted the block 16.0.0.0/8. The administrator wants to create 500 fixed-length subnets.

a. Find the subnet Mask
b. Find the number of addresses in each subnet
c. Find the first & the last address in the first (lowest numbered) subnet.
d. Find the first & the last address in the last subnet (subnet 500)

Solution:

16.0.0.0/8 is class A address



as $2^9 = 512$ subnets (requirement is of 500 subnets) so 512 is only nearest number.

$2^9 = 512$ subnetworks

$2^{15} = 2^5 \times 2^{10} = 32 \times 1024$

$= 32768$ addresses per subnetwork.

1024
32
2048
30720 x
32768

$\frac{32768}{256} = 128 \Rightarrow$ 128 Blocks of 256 addresses.

(0 to 127)

or 0.0.0.0 to 0.0.127.255 in Base 256

with 9 bits in subnet id, the prefix becomes /8+9 = /17

(a) Subnet mask can be calculated by making all left most bits (17 in this case) high

i.e. 11111111 11111111 10000000 00000000

∴ Subnet mask is 255.255.128.0

(b) Number of addresses in each Subnet are 32768

(c) First address in the first Subnet :

Subnet#1 — 16.0.0.0/17 → Subnet addrs.
16.0.0.1/17 → first addr.
⋮
16.0.127.255/17

Subnet#2 — 16.0.128.0/17
128.1
⋮
16.0.255.255/17

500 Subnets each with 32768 (ie 2^{15}) addresses
But $32768 = 128 \times 256$
∴ 500 Subnets will occupy
$= 500 \times 128 \times 256$ addresses
Block starts from 0.0.0
∴ ends at 249.255.255

(d) Subnet#500 — 16.249.128.0/17 → first address in Subnet #500
⋮
16.249.255.255/17 → last address in Subnet #500

249.255.255
− 128.255 → largest subnet
249.128.0

Subnet 500
⇒ 499 × 32678
= 16351232
⇒ 0.249.128.0 in Base 256

Now add this to first subnet addr 16.0.0.0

∴ Subnet #500 address will be 16.0.0.0
+ 0.249.128.0
16.249.128.0

#511 — 16.255.0.0/17
16.255.127.255/17
Subnet#512 — 16.255.128.0/17
⋮
16.255.255.255/17

Q.25 An organization is granted the block 130.56.0.0/16. The administrator wants to create 1024 Subnets.

(a) Find the Subnet mask

(b) Find the number of addresses in each subnet.

(c) Find the first and the last address in the first Subnet.

(d) Find the first and the last address in the last subnet (Subnet 1024)

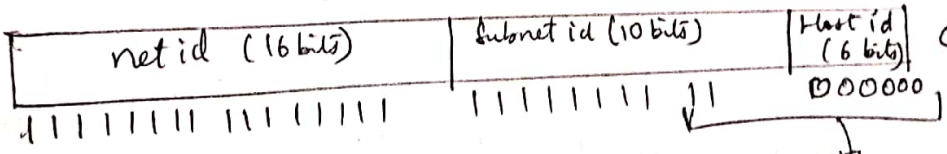
Solution:

Given IP is 130.56.0.0/16 ⇒ Class B as 16 bits in net id

1024 Subnets are required.

$2^{10} = 1024$ ∴ 10 Bits in Subnet id

(a)



∴ Subnet mask becomes 255.255.255.192 /(16+10)

i.e. /26

(b) No of addresses in each subnet $= 2^6 = 64$

(c) Subnet #1 130.56.0.0 → Subnetwork addr (First addr)

130.56.0.1 } Valid IP addresses assigned to hosts

130.56.0.62 }

130.56.0.63 → Limited Broadcast addr. (Last addr)

(d) $\frac{1024 \times 64}{256} = 256 \Rightarrow$ 256 Blocks of 256 ⇒ 0.0 to 255.255

0.0.3.255 in Between 256. 255 − 64 = 191

~~(b) total range is 0.0.0.0 to 0.0.3.255~~ (1024 Addition

~~(4×256=~~

Subnet # 1024 130.56.255.192 → First addr (Subnet addr)

130.56.255.255 → Last addr (Directed broadcast addr)

192
+63
255

OR

Subnet #1 130.56.0.0/26

0.63

130.56.0.64

#2 0.127

0.128

#3 0.191

0.192

#4 0.255

130.56.255.192 /26

Subnet # 1024 130.56.255.255

Q.26 An organization is granted the block 211.17.180.0/24. The organization wants to create 32 subnets.

a. Find the subnet mask
b. Find the number of addresses in each subnet
c. Find the first and the last address in the first subnet.
d. Find the first & the last address in the last subnet (subnet 32).

Solution:

32 subnets ⇒ 2^5 ⇒ 5 bits in SubnetID part.

(a)

Net id (24 bits)	Subnet ID (5 bits)	Host ID (3 bits)
11111111 11111111 11111111	11111	000

class C. (24+5)

∴ Subnet Mask is 255.255.255.248/29

b. Number of addresses in each subnet will be $2^3 = 8$

c.

Subnet # 1 — 211.17.180.0/29 → first addr (Subnet addr.)
⋮ (6 valid hosts)
211.17.180.7/29 → last addr (Broadcast addr.)

Subnet # 2 — 211.17.180.8/29
⋮
211.17.180.15/29

⋮

Subnet # 32 — 211.17.180.248/29 → first addr
⋮
180.255/29 → last addr.

32
8 | 256
256

5^2+3
$=256$

Q.29 In classless addressing, we know the first & the last address in the block. Can we find the prefix length? If the answer is yes, show the process & give an example.

Q. 28. Find the range of addresses in the following blocks:

(a) 123.56.77.32/29

(b) 200.17.21.128/27

(c) 17.34.16.0/23

(d) 180.34.64.64/30

Solution :

(a) 32 − 29 = 3 bit

$2^3 = 8$ Hosts / subnet.

∴ The range is

123.56.77.32/29

To 123.56.77.39/29

(b)

32 − 27 = 5 bits

$2^5 = 32$ Hosts

∴ The range is 200.17.21.128/27

To 200.17.21.159/27

(c) range is 17.34.16.0/23 to 17.34.~~17~~.255/23

∵ 9 bits in Host id ⇒ $2^9 = 512$ ~~Address~~.

512 in Base 256 = 0.0.~~256~~.255

(d) 180.34.64.64/30 to 180.34.64.67/30 | ∵ only 4 addresses (2^2) in Host]

Q.27. Write the following mask in slash notation (/n):

Ans

(a) 255.255.255.0	(a) 255.255.255.0/24
(b) 255.0.0.0	(b) 255.0.0.0/8
(c) 255.255.224.0	(c) 255.255.224.0/19
(d) 255.255.240.0	(d) 255.255.240.0/20

Q.33 An ISP is granted a block of addresses starting with 150.80.0.0/16. The ISP wants to distribute these blocks to 2600 customers as follows:

(a) The first group has 200 medium-size businesses, each needs approximately 128 addresses.

(b) The second group has 400 small businesses; each needs approximately 16 addresses.

(c) The Third group has 2000 households; each needs 4 addresses.

Design the subblocks & give the slash notation for each subblock. Find out how many addresses are still available after these allocations.

Solution:

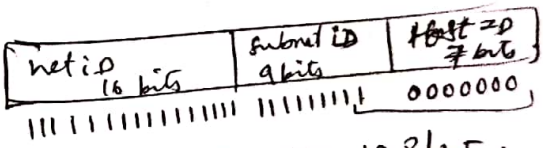
(a) 200 customers with 128 addresses each.

Group 1

$2^7 = 128 \Rightarrow 7$ bits in Host ID $\rightarrow$ 150.80.0.0/25

(32 − 7) = 25

1st customer : 150.80.0.0/25 to 150.80.0.127/25



2nd customer : 150.80.0.128/25 to 150.80.0.255/25 255.255.255.128/25. Subnet Mask.

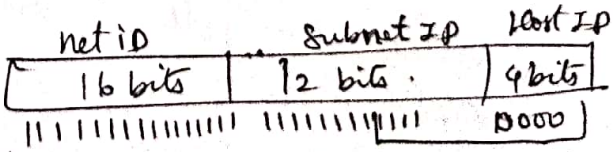
200th customer : 150.80.99.128/25 to 150.80.99.255/25

25600 / 256 = 100 Blocks @ 256

Total address for group 1 = 200 × 128 = 25600 addresses.

(b) Group 2 400 customers each needing 16 addresses.

$2^4 = 16$



1st customer : 150.80.100.0/28 to 150.80.100.15/28 255.255.255.240/28 Subnet mask.

2nd customer : 150.80.100.16/28 to 150.80.100.31/28

400th customer : 150.80.124.240/28 to 150.80.124.255/28

400 × 16 = 6400

6400 / 256 = 25 blocks

Pg-72

Total address for group 2

= 400 × 16 = 6400 addresses.

150.80.0.0 will have 16 address blocks
150.80.101 will have 16 blocks
∴ 125 × 16 = 2000

Range for group 2 (0.0.0.0 - 255.255) + 1
= (0 × 256³ + 0 × 256² + 255 × 256¹ + 255 × 256⁰) + 1
= (255 × 256 + 255) + 1
= 6400

(c) Group 3

2000 customers each with 4 addresses. $2^2 = 4$

1st customer : 150.80.125.0/30 to 150.80.125.3/30

2nd customer : 150.80.125.4/30 to 150.80.125.7/30

⋮

2000th customer : 150.80.157.60/30 to 150.80.157.63/30

32 ← 25
25 Blocks
256 | 8000
This helps to determine last addr
150.80.100.0
+ 150.80.124.255

means 0.0 to 24.255
i.e. 100.0 + 124.255
124.255

Total addresses for group 3

= 2000 × 4

= 8000 addresses.

2000 × 4
= 8000
256 | 8000 (31)
7936
64
⇒ 31 Blocks of 256 + 64 addresses

125.0
+ 30.255
155.255
1
155.0
+ 63
155.63

No of addresses granted = 2^{16} = 65536

No of addresses allocated = 25600 + 6400 + 8000 = 40000

No of addresses still available
= 65536 − 40000
= 25536

157.63
157.0

Q.34. An ISP is granted a block of addresses starting with 120.60.4.0/20. The ISP wants to distribute these blocks to 100 organizations with each organization receiving 8 addresses only. Design the subblocks & give the slash notation for each subblock. Find out how many addresses are still available after these allocations.

→ 120.60.4.0/20 ⇒ class A address.

$2^7 = 128 \Rightarrow$ near to 100.

∴ No of bits in subnet ID = 7

∴ 120.60.4.0/27

Subnet mask 255.255.255.224 /27

100 organizations × 8 address = 800 address.

$256 \overline{)800}\ 3$, 768, 32 ⇒ 3 complete blocks of 256 + 32 address.

∴ 120.60.4.0 + 0.255 = 120.60.4.255

+ 32 address.

120.60.7.31 ↳ last address.

0.0		
⋮		
0.255		
1.0		
⋮		
1.255		
2.0		
⋮		
2.255		
3.31		

32 − 20 = 12

Organization 1	120.60.4.0/27	120.60.4.7/27
2	120.60.4.8/27	120.60.4.15/27
3	120.60.4.16/27	120.60.4.23/27
4.	120.60.4.24/27	120.60.4.31/27
⋮	⋮	
!	120.60.4.248/27	120.60.4.255/27
⋮		
100	120.60.7.24/27	120.60.7.31/27.

No of granted addresses

$2^{12} = 2^{10} \times 2^2$

$= 1024 \times 4$

$= 4096$

No of allocated addresses = 800

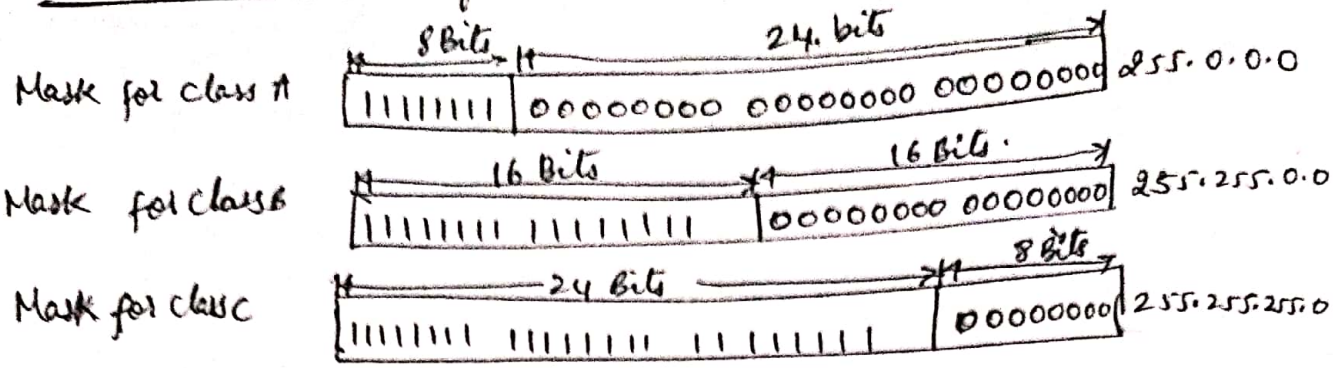
∴ No of available addresses

$= 4096 - 800$

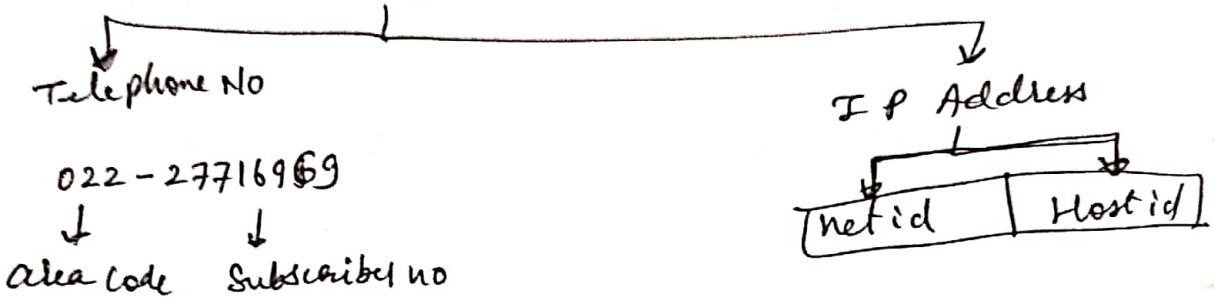
$= 3296$

Q.35. An ISP has a block of 1024 addresses. It needs to divide the addresses to 1024 customers. Does it need Subnetting? Explain your Answer.

Network Mask (Default Mask)

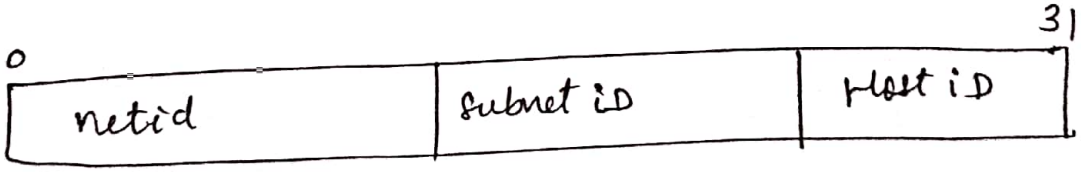


Two Level Addressing



In Two Level IP addressing most of the addresses go waste. So to avoid this westage 3-level IP addressing (called Subnetting is done.

Subnetting (Creating Small Networks)



Subnetting can be done based on the requirement of n/w's or based on requirement of hosts in a n/w.

Q.1. An ISP assigns a block of 196.0.0.0/24 IP addresses. It is required to form equal size subnets each with 62 addresses.

Solution:

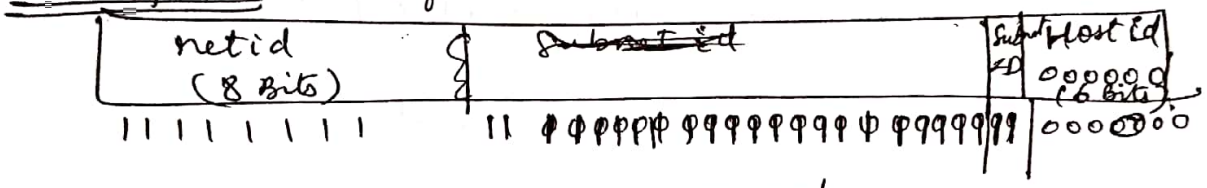
Here 62 addresses are required in each subnet.

62 is near to 64.

∴ Let us borrow 6 bits in Host id part to get $2^6 = 64$ addresses.

Given IP 196.0.0.0/24 Belongs to class C.

Calculating mask: Default mask is 255.255.255.0 But with subnetting mask becomes:



32
−14
18

∴ Subnet Mask : 255.255.255.192/26

With 2 bits in subnet id ; $2^2 = 4$ subnetworks are possible.

Subnet #1 196.0.0.0/26 Subnet addr.

196.0.0.1
:
0.0.62 } can be assigned to Hosts.

196.0.0.63/26 → Special address (BC addr)

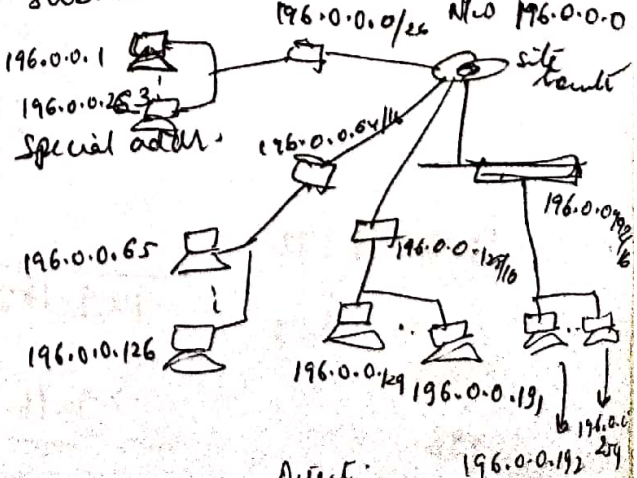
Subnet #2 196.0.0.64/26 → Subnet addr.

.65
.126
.127/26 — Special addr.

Subnet #3 196.0.0.128/26

.129
.190
.191/26

Subnet #4 196.0.0.192/26
.193/26
.254
.255/26 → Special addr (BC addr)

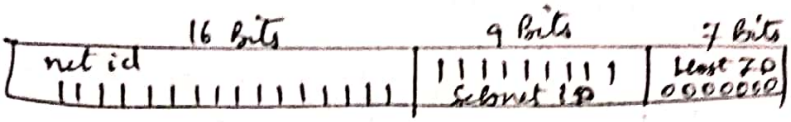


Q.2. An ISP grants a block of IP addrs 129.16.0.0/16. It is required to have 512 equal sized subnets. Find the first & last address in Subnet# 217

→ Given IP is class B

129.16.0.0/16

To Have 512 subnets ; 9 bits must be made high in Subnet id



Subnet Mask 255.255.255.128 /(16+9) 25

$2^7 = 128$ hosts

Subnet # 1 129.16.0.0/25 — Subnet addrs

:

:126

:127/25 — BC addrs.

129.16.0.128/25

:129/25

:

:254/25

:255/25

Subnet # 2

:

Subnet # 217

129.16.108.0

:1

:

:108-126

129.16.108.127 | 25

:

Subnet # 512

129.16.255.128/25

:129/25

:254/25

129.16.255.255/25

512 + 128

217 × 128

= 27776

256 | 27776 (108)

27648

128

108 blocks of 256 + 128 addrs

0.0

+ 107.255

107.255

108:0

:1

108.127

129.16.255.255

- 129.16.0.0

0.0.255.255

Pg - 78

Q.3 Find the no of addresses in a range if the first address is 160.112.19.0 & the last addr is 160.112.26.255 (Ans 2048)

Q.4. The first addr in a range of addresses is 18.12.44.64. If the number of address in the range is 64, what is the last address?
(Ans 18.12.44.127)

Q.5. An address in a block is given as 72.56.12.28. Find the no of addresses in the block, the first addr & the last addr. (Ans 72.0.0.0 to 72.255.255.255)

Q.6. Repeat Q.5 for 168.64.3.5 (Ans 168.64.0.0 to 168.64.255.255)

Q.7. Repeat Q.5 for 221.8.6.10 (Ans (221.8.6.0 to 221.8.6.255)

Q.8. A router receives a packet with destination address 172.155.38.96. If the subnet mask is 120 find the subnet address.

(172.155.38.96
AND 255.255.240.0

10101010.172.155.00100110.01100000
AND 255.255.11110000.00000000
172.155.00100000.00000000

∴ subnetwork addr is 172.155.32.0)

Special addresses

- All-zeros address → 0.0.0.0/32 → used by DHCP client (who is not knowing its IP address)
- All ones address → 255.255.255.255/32 → used by DHCP client to Broadcast to DHCP servers.
  - ↳ Limited Broadcast address.
- Loopback address → 127.0.0.0/8 → Loopback testing.
- Special addresses in Each Block
  - → n/w address → suffix = 0's e.g. 223.1.2.0/24
  - → Direct Broadcast addr. → suffix = 1's. 223.1.2.255/24

Private addresses:

Class A → Block 10.0.0.0/8 ⇒ 10.0.0.0/8 to 10.255.255.255/8 (16777216 addresses)

Class B → Block 172.16.0.0/16 ⇒ 172.16.0.0/16 to 172.31.255.255/16 (1047584 addresses)

Class C → Block 192.168.0.0/16 ⇒ 192.168.0.0/16 to 192.168.255.255/16 (65536 addresses)

Class ~~D~~ → Block 169.254.0.0/16 ⇒ 169.254.0.0/16 to 169.254.255.255/16 (Total 65536 addresses.)

Multicast Addresses:

The Block 224.0.0.0/4 is reserved for multicast communication.

Subnetting (3-Level Addressing)

- Subnetting divides the larger size Blocks (like in class A & B) into smaller size blocks, so that the sub blocks could be shared with other organizations.
- In Subnetting, a network is divided into several smaller subnetworks (subnets) with each subnetwork having its own subnetwork address.

Supernetting

Subnetting drawback:

- did not solve the address depletion problem
- Many organization did not like to share the subblocks from class A & class B addresses.

Supernetting:

- Class C Blocks did not satisfy the need of IP addresses in several organizations.
- So organizations combined several class C Blocks to create a larger range of addresses.
- Supernetting thus forms large size networks.
- e.g. If an organization needs 2048 addresses then it could combine 8 class C Blocks.

Subnetting	Supernetting
• Divides larger n/w's into smaller ones	• Combines smaller n/w's into larger ones.
• Increases the no of bits in n/w id part	• Decreases the no of bits in n/w id part
• No of bits in Host id are reduced	• No of bits in Host part are increased.

What is Subnetting?

Subnetting is a method for maximizing the limited 32-bit IPv4 addressing space and reducing the size of routing tables in a large internetwork. With any address class, subnetting provides a means of allocating a part of the host address space to network addresses, which lets you have more networks. The part of the host address space that is allocated to new network addresses is known as the subnet number.

In addition to making more efficient use of the IPv4 address space, subnetting has several administrative benefits. Routing can become complicated as the number of networks grows. A small organization, for example, might give each local network a class C number. As the organization grows, the administration of a number of different network numbers could become complicated. A better idea is to allocate a few class B network numbers to each major division in an organization. For example, you could allocate one class B network to Engineering, one class B to Operations, & so on. Then you could divide each class B network into additional networks, using the additional network numbers gained by subnetting. This division can also reduce the amount of routing information that must be communicated among routers.

Why Subnetting is done ?

Subnetting an IP network can be done for a variety of reasons, including organization, use of different physical media (such as Ethernet, FDDI, WAN etc.) preservation of address space, & security. The most common reason is to control network traffic. In an Ethernet network, all nodes on a segment see all the packets transmitted by all the other nodes on that segment. Performance can be adversely affected under heavy traffic loads, due to collisions and the resulting retransmissions. A router is used to connect IP networks to minimize the amount of traffic each segment must receive.

Reasons for Subnetting

- Most IP address assignments were not used very efficiently.
- Broadcast problem.
- Many sites were requesting multiple network numbers due to variable amounts of networks at their sites.
- Imagine a Network class A with over 16 millions of hosts or a class B network with 65 thousand hosts, it is impractical...

Benefits of Subnetting:

- Reduced network traffic
- Simplified management.
- Smaller broadcast domains

Supernetting

People realized that addresses could be conserved if the class system was eliminated. By accurately allocating only the amount of address space that was actually needed, the address space crisis could be avoided for many years. This was first proposed in 1992 as a scheme called Supernetting. Under Supernetting, the classful subnet masks are extended so that a n/w address & subnet mask could, for example specify multiple class C subnets with one address.

For example, if I needed about 1000 addresses, I could supernet 4 class C networks together.

192.60.128.0 (class C subnet address)
192.60.129.0 (class C subnet address)
192.60.130.0 (—11—)
192.60.131.0 (—11—)

192.60.128.0 (Supernetted subnet address).

Subnet mask calculation:

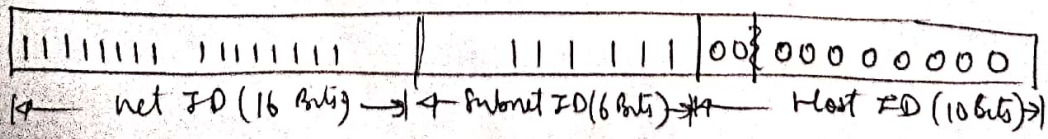
1000 addresses ⇒ 1000 Hosts

1000 is not perfect power of 2

∴ consider 1024

$2^x = 1024 \quad x = 10$

∴ 10 Bits in Host ID



Subnet mask 255.255.252.0/22
⇒ 22 Bits in n/w part & 10 Bits in Host part.

For class C /24 ⇒ 24 Bits in net ID But with Supernetting no of prefix Bits are reduced.

Broadcast address → 192.60.131.255

In this example, the subnet 192.60.128.0 includes all the addresses from 192.60.128.0 to 192.60.131.255.

Classless Interdomain Routing (CIDR pronounced cider)

In CIDR, the subnet mask notation is reduced to a simplified shorthand. Instead of spelling out the bits of the subnet mask, it is simply listed as the number of ones (1's) that start the mask. In the above example, instead of writing the address & subnet mask as 192.60.128.0, subnet mask 255.255.252.0, the network address would be written simply as: 192.60.128.0/22.

which indicates starting address of the network, and number of 1s bits (22) in the network portion of the address.

In short

The four entries 192.60.128.0
192.60.129.0
192.60.130.0
192.60.131.0

will be aggregated to a single entry
192.60.128.0/22 in the router

So routing table size will reduce.

Advantages of Supernetting

- Routing table size is minimized (minimum memory storage at routers)
- Stable n/w's since the topology updates are advertised to required subnets only.
- minimised processing overhead.
- Efficient use of BW → energy not wasted when n/w goes down.

Why Supernetting is done?

→ Due to exhaustion of class B addresses
→ To group different class C n/w's (so that n/w's appear single large n/w's)

→ To reduce size of n/w routing tables.

Advantages of minimised routing table size

- Increase in routing table lookup speed.
- Decrease in overhead for routing protocols since fewer routing entries are being advertised.

Routing protocols which do not support CIDR or VLSM (supernetting)	Routing protocols which support CIDR or VLSM (supnetting)
RIPv1, EGP, IGRP	RIPv2, EIGRP, BGP, OSPF

Example of Supernetting

- Consider that there are 50 districts with 150 accounting services; requiring 7500 routers altogether without supernetting.
- With supernetting, every district routers are summarized in a centralized site (router) as an interconnection point (similar to distribution points in case of telephone n/w's; recognising area codes).
- Thus, each router knows its summary route & other 49 routers summary routes.

e.g. A router has following entries in its routing table.

192.168.98.0
192.168.99.0
192.168.100.0
192.168.101.0
192.168.102.0
192.168.105.0

Now convert each octet in binary

← 20 bits →

11000000 10101000 01100010 00000000
11000000 10101000 01100011 00000000
11000000 10101000 01101001 00000000
11000000 10101000 01101010 00000000
11000000 10101000 01101100 00000000
11000000 10101000 01101101 00000000.

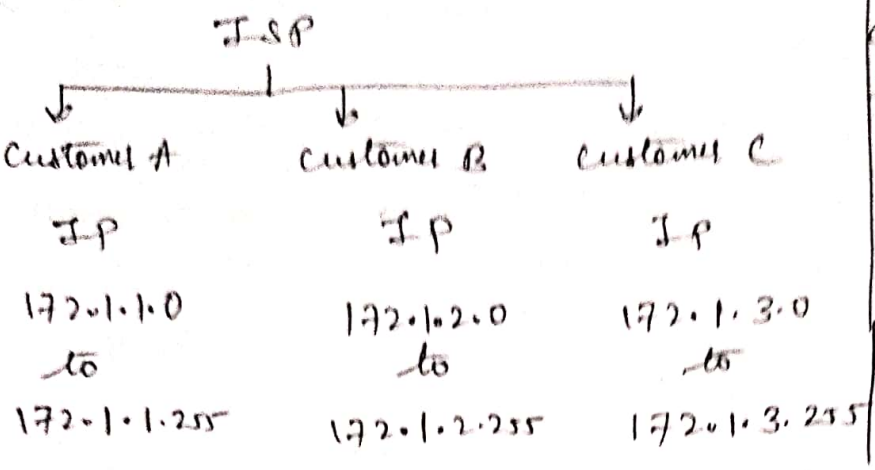
← common bits →

192.168.96.0/20 ⇒ CIDR notation.

& Subnet mask 255.255.240.0/20.

But with this the missing n/w's 192.168.96.0, 192.168.97.0 192.168.103.0 & 192.168.104.0 are taken into account. These can be excluded by summarizing the entries to 192.168.98.0/20

Another example on CIDR



In 1996, the Internet authorities announced a new architecture called classless addressing or CIDR that allows an organization to have a block of addresses of any size as long as the size of the block is a power of two

Instead of providing these IP's the ISP can advertise single IP on the Internet with CIDR notation 172.1.0.0/16

which could reduce the number of entries in the global routing table.

Examples on CIDR

Q.1 If an address in a block is given in CIDR classless notation as 60.33.18.4/27 then find the following:

(1) Number of addresses in the block (N)
(2) The first address
(3) The last address.

Solution:

Slash 27 → /27 means 27 bits in n/w ID & (32-27)=5 Bits in host ID.

(1) ∴ $2^5 = 32$ addresses in the Block.

(2) First addr 60.33.18. can be calculated by ANDING Subnet mask with given address.

Subnet mask will be 255.255.255.224/27

(27 Bits High)

∴ 60.33.18.4/27

AND 255.255.255.224/27

60.33.18.0/27.

4 ⇒ 00000100

224 ⇒ 11100000

00000000

∴ First addr is 60.33.18.0/27

(3) Last addr can be obtained by keeping leftmost 27 bits as it is & making Host ID bits all 1's.

∴ 60.33.18.

∴ Last octet will be 00011111 = 31

∴ Last addr will be 60.33.18.31/27

Q2. For the classless address 131.66.23.1/24 find the following;

(1) Number of addresses in the block
(2) The first address
(3) The last address

Solution:

(1) No of addresses in the block = $2^8 = 256$ (∵ 32 − 8 = 24 bits in Host ID)

(2) the first address → 131.66.23.0/24

(3) The Last address → 131.66.23.255/24.

Q.3. A router has following CIDR entries in its routing table: (Pg -89)

Address/Mask	Next Hop
136.64.32.0/22	Interface 0
136.64.40.0/22	Interface 1
196.55.40.0/23	Router 1
Default	Router 2

For each of the following IP addresses, what does the router do if a packet with that address arrives?

① 136.64.47.20 ② 196.55.46.9

Solution:

① Given IP 136.64.47.20 → This IP addr is closer to Interface 1 with /22

AND 255.255.252.0/22

So determine Subnet mask for /22

00101111
11111100
00101100

136.64.44.0/22 ⇒ ~~IP addr of Interface 1~~

∴ The packet with IP addr 136.64.47.20 will be forwarded to ~~Interface~~ default Router

② 196.55.46.9 is closer to router 1 addr with /23

So determine Subnet mask for /23

255.255.254.0/23

Now 196.55.46.9 — 00101110

AND 255.255.254.0 — 11111110

196.55.46.0 — 00101110 ⇒ 46

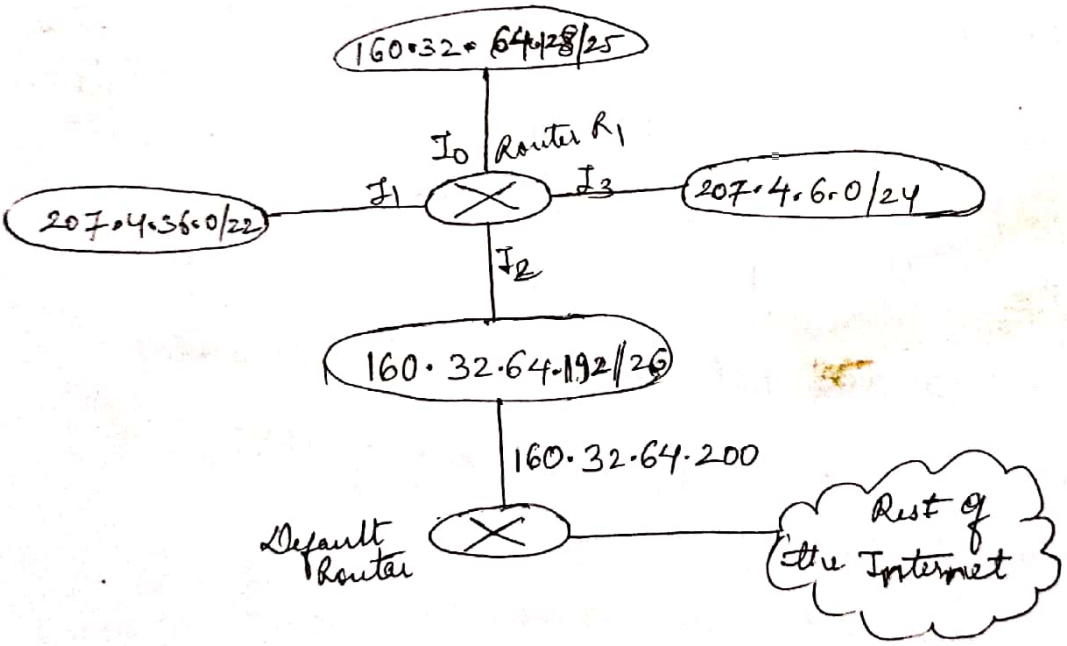
↳ This IP address does not belong to Interface 0, 1 & first even to Router 1

∴ Packet with IP addr 196.55.46.9 will be forwarded to Default Router 2.

Q4. A router is networking four different networks with network addresses 160.32.64.192/26, 160.32.64.128/25, 207.4.6.0/24, 207.4.36.0/22 and default router on 160.32.64.200 make a routing table for this router and explain the forwarding process for packet with destination IP 16.24.42.60

Solution:

Let us show the networks connected to the router.



Routing Table:

Mask	Network address	Next Hop	Interface
/26	160.32.64.192	—	I_2
/25	160.32.64.128	—	I_0
/24	207.4.6.0/24	—	I_3
/22	207.4.36.0/22	—	I_1
Any	Any	160.32.64.200	I_2

Forwarding process for the packet with destination address (Pg-91)

16.24.42.60

- First of all the router will apply the mask of /26 to 16.24.42.60

Mask of /26 ⇒ 255.255.255.192

16.24.42.60
AND 255.255.255.192
16.24.42.0 → does not match with any n/w addr.

60 = 00111100
192 = 11000000 AND
00000000

- The router will now apply the mask of /25 to 16.24.42.60

Mask of /25 ⇒ 255.255.255.128

16.24.42.60
AND 255.255.255.128
16.24.42.0 → does not match with any n/w addr.

60 = 00111100
128 = 10000000
00000000

- The router will now apply the mask of /24 to 16.24.42.60

Mask of /24 ⇒ 255.255.255.0

16.24.42.60
AND 255.255.255.0
16.24.42.0 → does not match with any n/w addr.

- The router will finally apply the mask of /22 to 16.24.42.60

Mask of /22 ⇒ 255.255.252.0

16.24.42.60
AND 255.255.252.0
16.24.40.0 ⇒ does not match with any n/w addr.

00101010
11111100
00101000

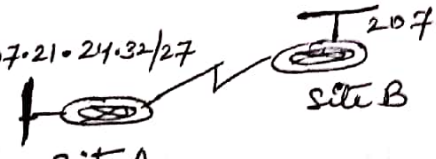
Since IP 16.24.192.60 does not match with any of the n/w addr, the packet will be forwarded to the default router.

Formulae

- First address = (Any address) AND (Network mask)
- Last address = first address + Number of addresses in the block
- Last address = (Any address) OR [NOT (Network Mask)]

Variable Length Subnet Masking (VLSM)

VLSM allows to use more than one subnet mask within the same n/w address space - Subnetting a subnet.



3 Bits in Subnet ID
$2^3 = 8$ Subnetworks

Subnet	Subnet Address
0	207.21.24.0/27
1	207.21.24.32/27
2	207.21.24.64/27
3	207.21.24.96/27
4	207.21.24.128/27
5	207.21.24.160/27
6	207.21.24.192/27
7	207.21.24.224/27

3 more bits in Subnet ID
$2^3 = 8$ Sub-Subnetworks

Subnet of Subnet	Sub-Subnet Address
Sub 0	207.21.24.192/30
Sub 1	207.21.24.196/30
Sub 2	.200/30
Sub 3	.204/30
Sub 4	.208/30
Sub 5	.212/30
Sub 6	.216/30
Sub 7	.220/30

Network Address Translation (NAT)

This Technology allows a site to use a set of private addresses for internal communication and a set of global Internet addresses (at least one) for communication with the rest of the world. The site must have only one single connection to the global Internet through a NAT-capable router that runs NAT software.

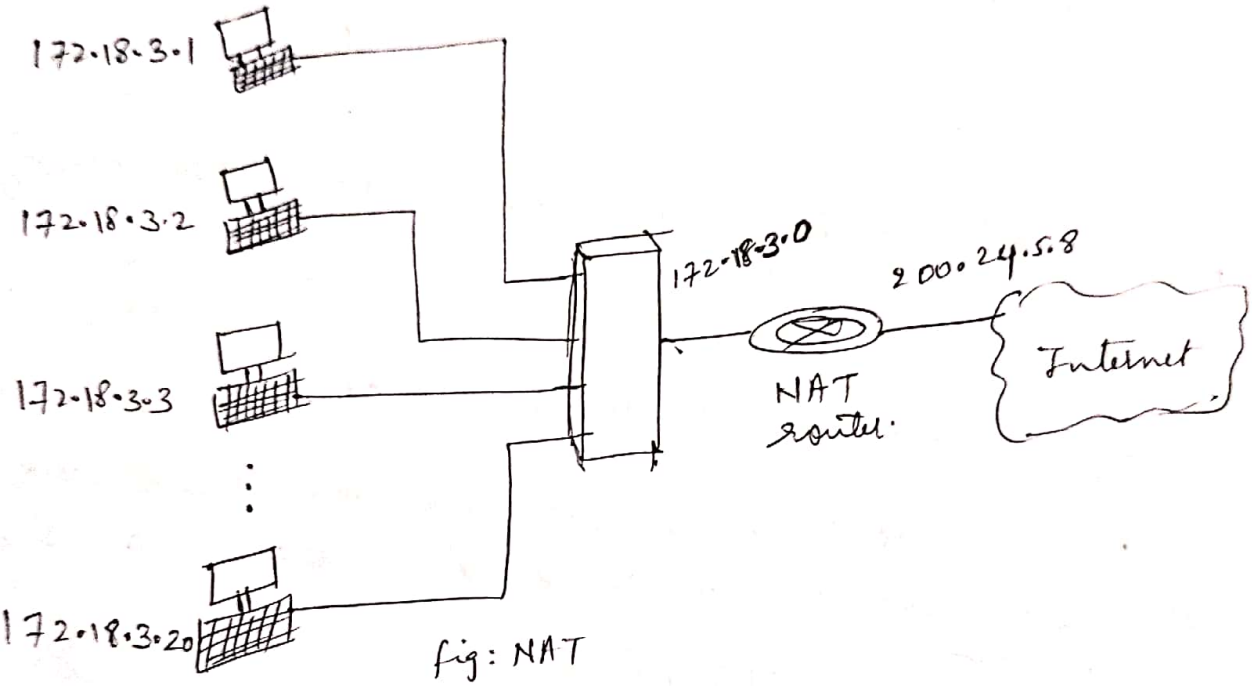


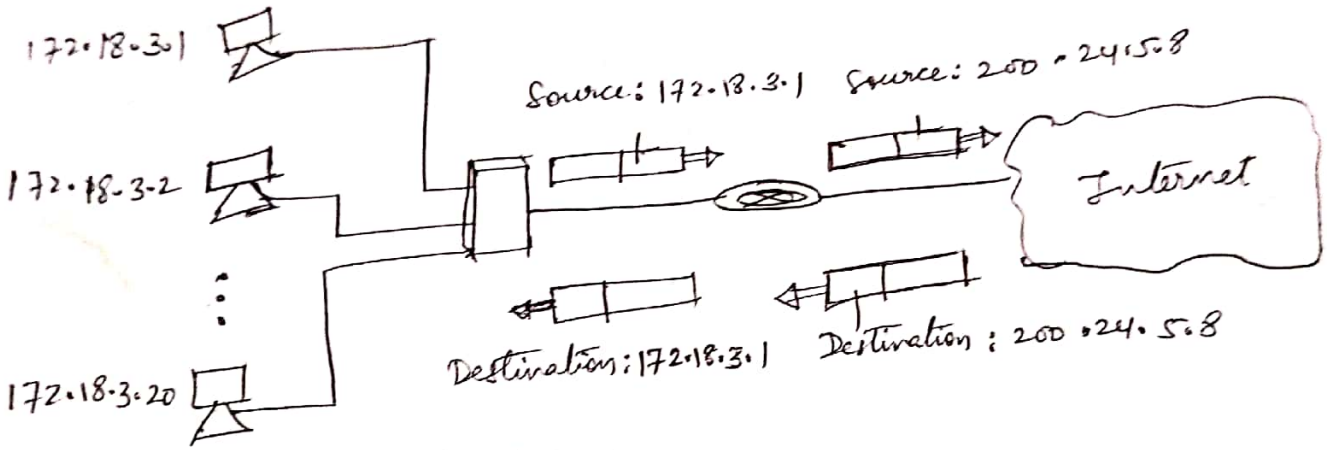
fig: NAT

As the figure shows, the private network uses private addresses. The router that connects the network to the global address (public IP address) uses one private address and one global address. The private network is transparent to the rest of the Internet; the rest of the Internet sees only the NAT router with the address 200.24.5.8.

NAT maps multiple private IP addresses to one or more global public IP addresses

Address Translation

- All of the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the destination address in the packet (the NAT global address) with the appropriate private address.



Site using private addresses

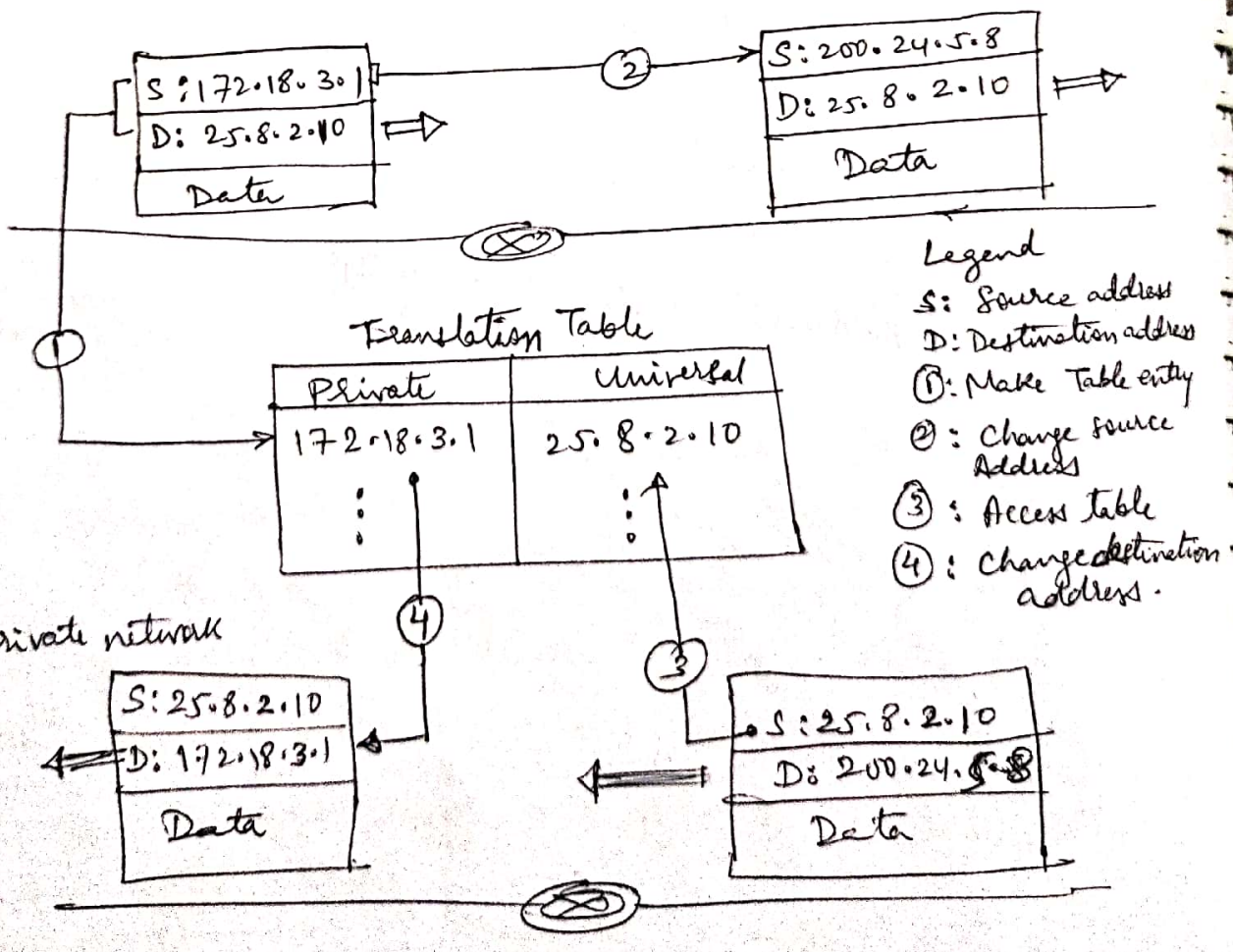
Translation Table

- Using one IP Address
- Using a Pool of IP Addresses
- Using Both IP addresses & Port Addresses.

- The translation of source addresses for an outgoing packet is straightforward.
- But how does the NAT router know the destination address for a packet coming from the Internet?
- There may be tens or hundreds of private IP addresses, each belonging to one specific host
- The problem is solved if the NAT router has a translation table.

Using One IP Address:

- A Translation table in its simplest form has only two columns: the private address and the external (global) address.



- NAT is used mostly by ISPs that assign one single address to a customer.
- The customer, however, may be a member of a private network that has many private addresses.
- In this case, communication with the Internet is always initiated from the customer site, using a client program such as HTTP, TELNET or FTP to access the corresponding server program.

For example, when e-mail that originates from a non customer site is received by the ISP email server, it is stored in the mailbox of the customer until retrieved with a protocol such as POP.

- A private network cannot run a server program for clients outside of its n/w if it is using NAT technology.

Using a Pool of IP Addresses:

- Using only one global address by the NAT router allows only one private-network host to access the same external host.
- To remove this restriction, the NAT router can use a pool of global addresses.
- For example, instead of using only one global address (200.24.5.8), the NAT router can use four addresses (200.24.5.8, 200.24.5.9, 200.24.5.10 and 200.24.5.11).
- In this case, four private-network hosts can communicate with the same external host at the same time because each pair of addresses defines a connection.

However, there are still some drawbacks.

No more than four connections can be made to the same destination.

- No private-network host can access two external server programs (e.g., HTTP and TELNET) at the same time.
- And, likewise, two private-network hosts cannot access the same external server program (e.g., HTTP or TELNET) at the same time.

Using Both IP Addresses and port Addresses

- To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the translation table.
- For example, suppose two hosts inside a private network with addresses 172.18.3.1 and 172.18.3.2 need to access the HTTP server on external host 25.8.3.2.
- If the translation table has five columns, instead of two, that include the source & destination port addresses & the transport layer protocol, the ambiguity is eliminated.

Private Address	Private Port	External Address	External port	Transport protocol
172.18.3.1	1400	25.8.3.2	80	TCP
172.18.3.2	1401	25.8.3.2	80	TCP
...	...	...	...	...

Table: Five Column Translation table.

Pg-98

Note that when the response from HTTP comes back, the combination of source address (25.8.3.2) & destination port address (1400) defines the private network host to which the response should be directed.

Note also that for this translation to work, the emphemeral port addresses (1400 & 1401) must be unique.

- Supernet
- Supernetting, route aggregation, route summarization
- CIDR
- Advantages of Supernetting
  - → Min storage req at routers (routing table size is minimised)
  - → Stable n/w's since the topology updates are advertised to required subnets only (routers).
  - → Minimised processing overhead.
  - → Efficient use of BW → Energy not wasted when n/w goes down.
- Why Supernetting is done?
  - → Due to Exhaustion of Class B addresses
  - → To group different class C n/w's (so that n/w's appear single large n/w's)
  - → To reduce size of n/w routing tables.
- Advantages of minimised routing table size
  - → Increase in routing table lookup speed.
  - → Decrease in overhead for routing protocols since fewer routing entries are being advertised.

Protocols

Protocols which do not support CIDR or VLSM i.e. Supernetting	protocols which support CIDR or VLSM i.e Supernetting
RIP V1, EGP IGRP	RIPV2, ~~EIGRP~~, EIGRP, BGP, OSPF.

Example of Supernetting

- Consider that there are 50 districts with 150 accounting services requiring 7500 routers altogether without Supernetting
- With Supernetting, every district's routers are summarised in a centralized site (router) as an interconnection point (similar to Distribution points in case of Telephone n/w's & Recognising area codes).
- Thus, each router knows its summary route & other 49 routers summary routes.

e.g. A router has following entries in its routing table.

192.168.98.0
192.168.99.0
192.168.100.0
192.168.101.0
192.168.102.0
192.168.105.0

Now, convert each octet in binary

20 →

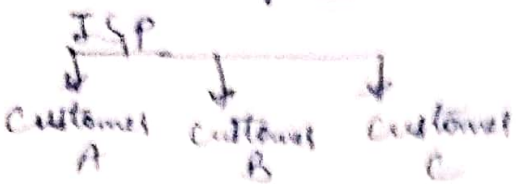
11000000.10101000.01100010.00000000
11000000.10101000.01100011.00000000
11000000.10101000.01100100.00000000
11000000.10101000.01100101.00000000
11000000.10101000.01100110.00000000
11000000.10101000.01101001.00000000

192.168.96.0/20 ⇒ CIDR notation.

& SubnetMask 255.255.240.0.

But with this the missing n/w's 192.168.96.0, 192.168.97.0 192.168.103.0 & 192.168.104.0 are taken into accer these can be excluded by summarizing the entries to 192.168.98.0/20.

Another example



IP	IP	IP
172.1.1.0	172.1.2.0	172.1.3.0
to	to	to
172.1.1.255	172.1.2.255	172.1.3.255

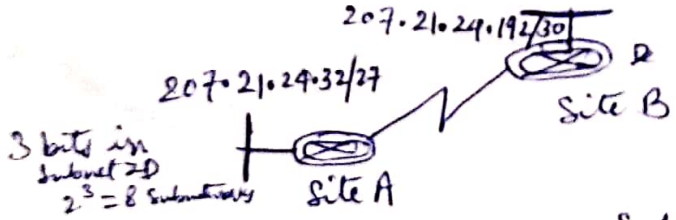
Instead of providing these IP's the ISP can advertise a single IP on the Internet with CIDR notation like

172.1.0.0/16.

which would reduce the number of entries in the global routing table.

VLSM allows you to use more than one subnet mask within the same NW address space – Subnetting a Subnetted

Example

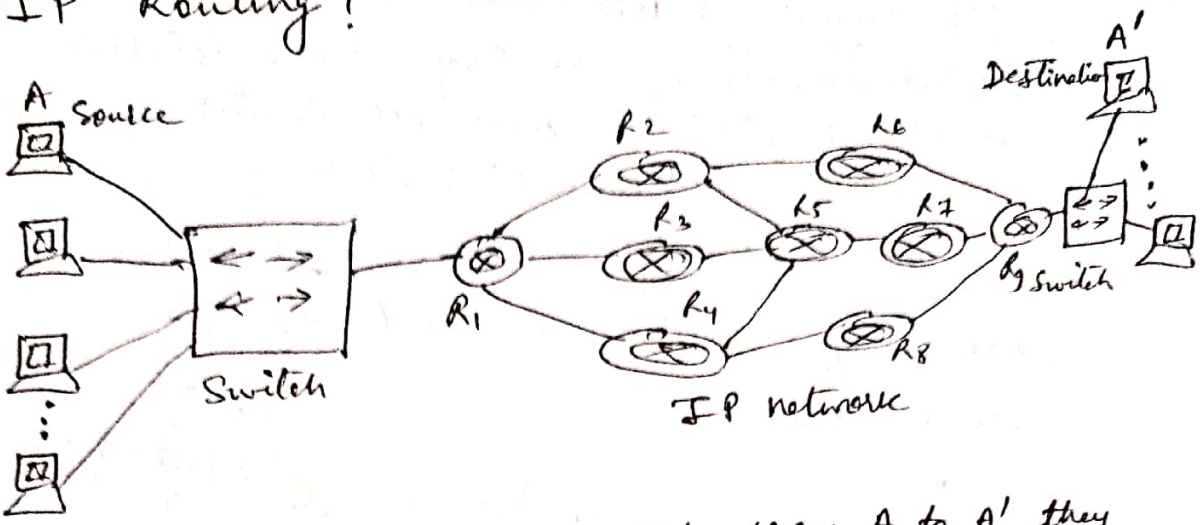


Subnet	Subnet Address
0	207.21.24.0/27
1	207.21.24.32/27
2	207.21.24.64/27
3	207.21.24.96/27
4	207.21.24.128/27
5	207.21.24.160/27
6	207.21.24.192/27
7	207.21.24.224/27
~~8~~	~~207.21.24.2~~

3 more bits in subnet ID /30 $2^3 = 8$ sub-subnetworks

Subnet of Subnet	Sub-Subnet Address
Sub 0	207.21.24.192/30
Sub 1	207.21.24.196/30
	.200/30
	.204/30
	.208/30
	.212/30
	.216/30
Sub 7	207.21.24.220/30

What are the drawbacks of Traditional IP Routing?

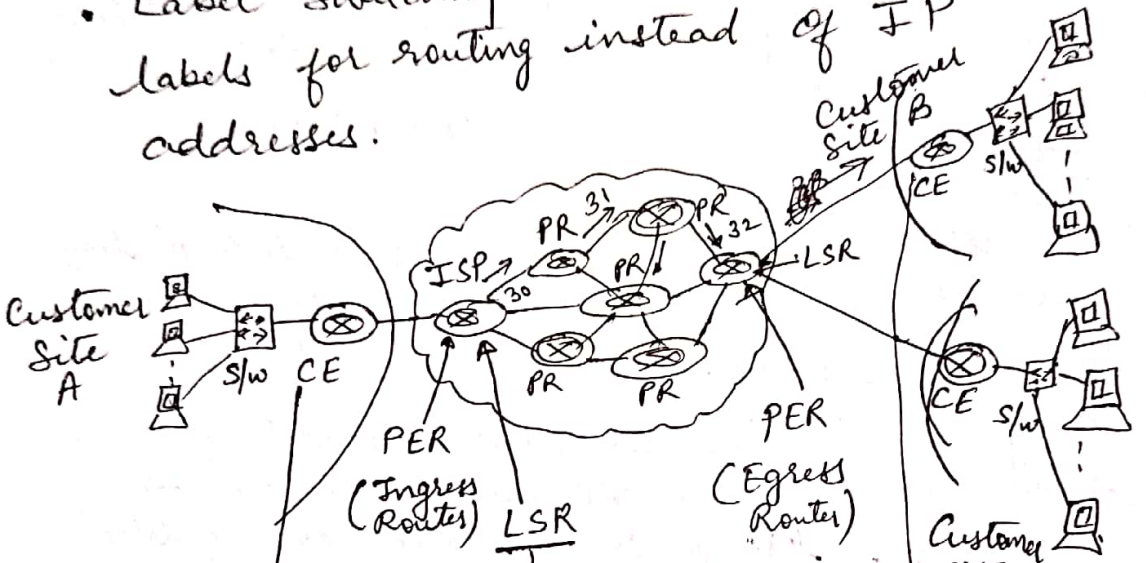


- When the packets are routed from A to A', they have to travel through a number of routers in the IP network.
- Every router receives the packets, Inspects for source & destination IP address available in the packet, lookups for IP table (Routing table) to find the next hop IP address, forwards the packet to next router in the path towards the destination.
- If the network is very large then it takes lot of time to lookup large size routing tables.
- This causes large transmission delays in the network (Drawback of traditional IP routing)
- Another issue with traditional IP routing is; the routing commands vary with Various kinds of routing protocols (e.g. multicast routing, Ethernet frame mode routing, ATM cell mode routing etc).
- To overcome these drawbacks MPLS is used.

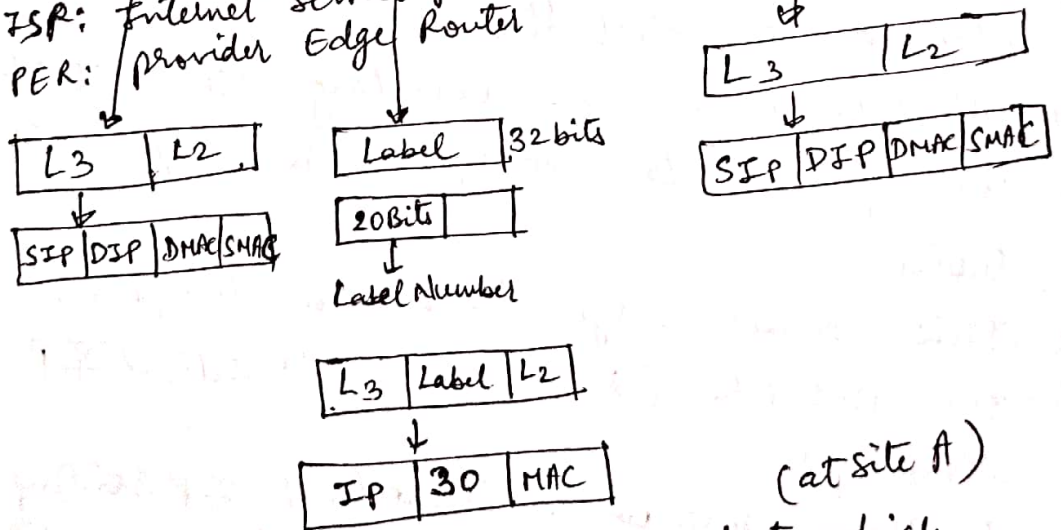
Shubhangi Kheche

Multiprotocol Label Switching (MPLS)

- Multiprotocol because this switching (forwarding) can work with various kinds of routing protocols (like multicast protocols, ATM cell switching, Frame mode (Ethernet) switching etc)
- Label Switching because it uses labels for routing instead of IP addresses.



CE : Customer Edge Router
PR : Provider Router
ISP : Internet Service provider
PER : Provider Edge Router



(at site A)

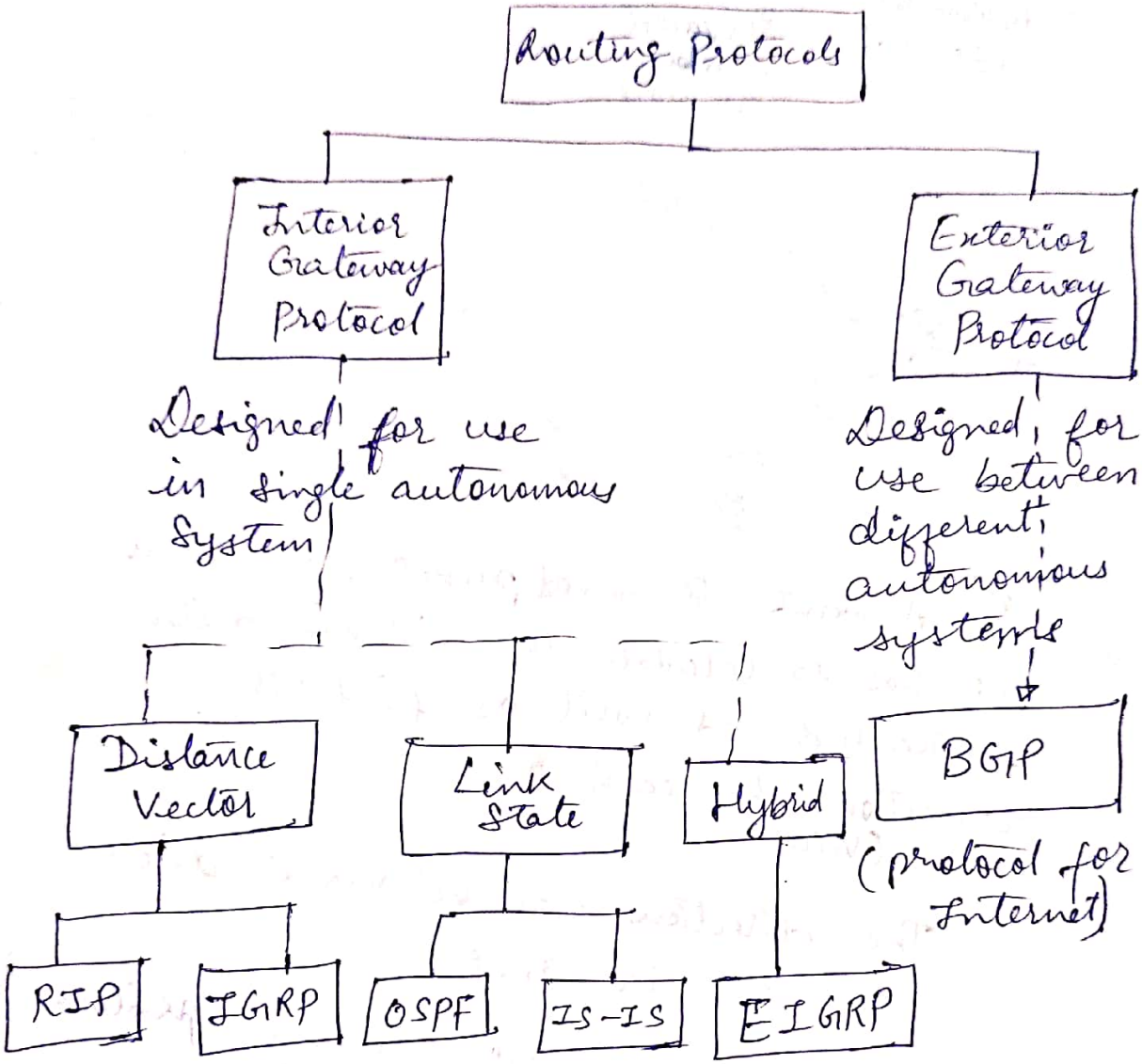
- The CE router generates a packet, which has source IP addr, destination IP address, destination MAC addr, source MAC addr followed by data.

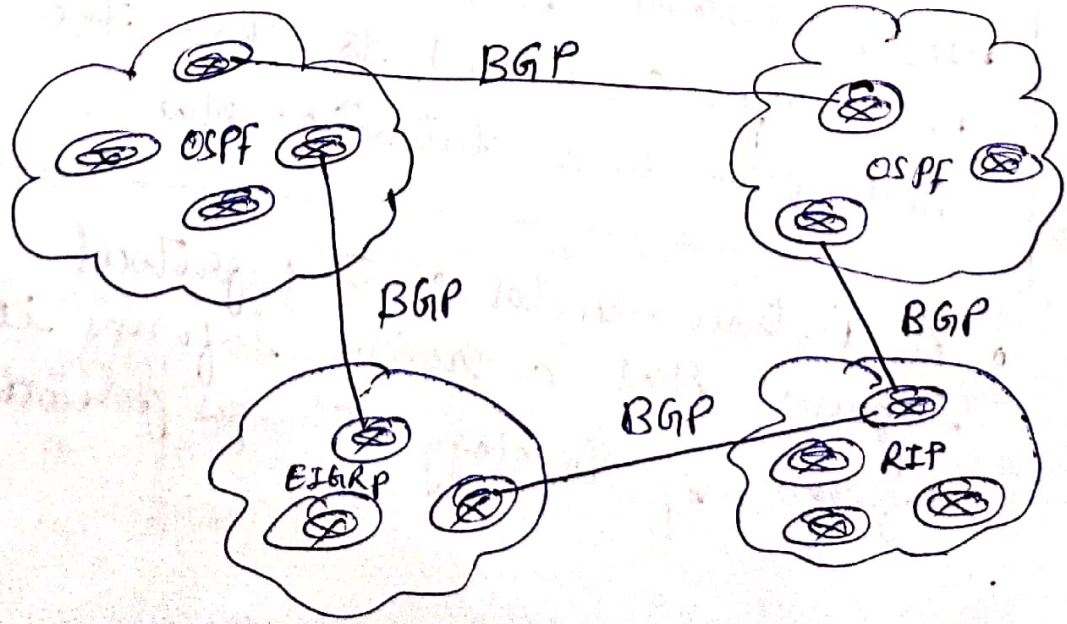
- The Label Switch Router (LSR) (ingress router) receives the packet, adds a label in between the IP address & the MAC address (let say label 30 is added) & forwards it to the next router (PR) in the path.
- This PR swaps the label present in the received packet with its own (say 31) & forwards it to next PR in the path.
- This happens swapping of labels takes place at every PR.
- Finally the PER (egress LSR) receives the packet; removes the label from it & forwards the packet to CE (at site B).
- The CE at site B then forwards the packet to the computer whose IP & MAC address matches with those present in the packet.

Advantages of MPLS

- Saves IP lookup time, so Switching (forwarding) is faster, no delay in communication.
- Works with various kinds of routing protocols.

Routing Protocols



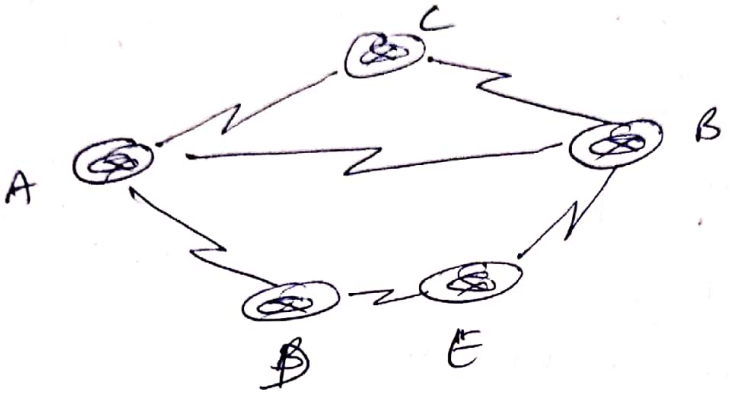


searching Best Path → Set of Rules

Distance Vector Routing Protocol

How much is the distance bet'n two n/w's

In which direction the packet can be forwarded



If A wants to send packet to B, then it has to calculate the minimum distance to reach B as well as find the direction to reach B.
(Vector)

The directions can be via C, direct path or via D & E.

Thus, a distance vector routing protocol uses a distance calculation plus an outgoing n/w interface (a vector) to choose the best path to a destination n/w

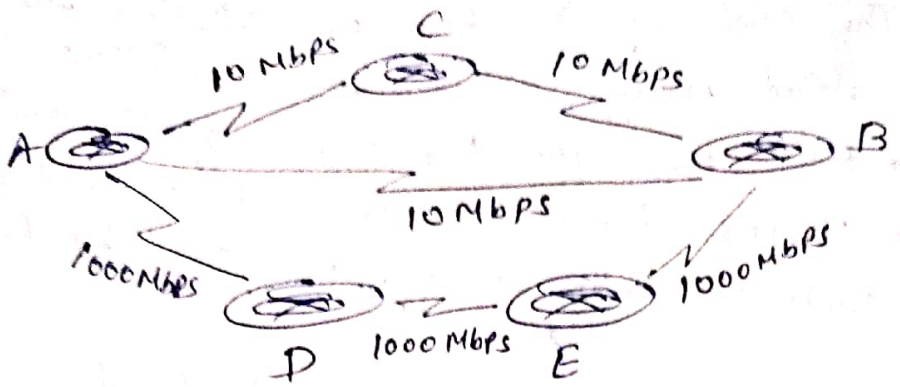
- A distance-vector routing protocol requires that a router informs its neighbors of topology changes periodically.

The cost of reaching a destination is calculated using various route metrics

- RIP uses the hop count of the destination
- I-GRP takes into account other information such as node delay and available Bandwidth

Link State Routing Protocol

- Link State
  - ↳ Track the states (up or down) and connection type of each link (Ethernet, FastEthernet, Gigabit Ethernet or Serial connection) (what is the BW of Serial connection).
  - → Produces a calculated metric based on these factors.
  - Some factors can be set by the network administrators.
- Link state protocols know whether a link is up or down
- Link state protocols know how fast the link is and calculates a cost to 'get there'.
- Link state protocols will take a path which has more hops, but that uses a faster medium over a path using a slower medium with fewer hops.



Paths available:

1. A to B
2. A to B via C
3. A to B via D & E

- RIP will select direct path (1) from A to B (only one hop)
- Link state routing will select path (3) i.e. from A to B via D & E as the BW for this path is 100 times better than the other two paths.
- Link state routing protocol uses a shortest path first (SPF) algorithm to choose the best path to a destination network.

Distance Vector Vs Link State Routing protocols

Distance Vector Routing Protocol	Link State Routing Protocol
• Entire routing table is sent as an update	• Updates are incremental and entire routing table is not sent as update.
• Send periodic update (Every fixed interval of time) at every 30 or 90 second.	• Updates are triggered not periodic.
• Updates are broadcasted (not in RIPV2) Due to this large BW is used	• Updates are Multicasted . No unnecessary BW consumption.
• Updates are sent to directly connected neighbor only.	• Update are sent to entire network
• Routers don't have end to end visibility of entire network	• Routers have visibility of entire network of that area only
• Prone to routing loops	• No routing loops

Routing Information Protocol (RIP)

- It is the most popular routing protocol.
- It is the Interior Gateway protocol (IGP)
- RIP is Dynamic routing protocol
- It is a Distance Vector protocol.
- It was developed for smaller networks
- RIP uses UDP port 520 for route updates
- RIP calculates the best route based on hop count.
- It is an open standard.
- RIP is sometimes referred to as IP RIP
- The Maximum number of hops allowed for RIP is 15
- A hop count of 16 is considered an infinite distance and used to deprecate inaccessible, inoperable, or undesirable routes.
- Periodic updates: RIP sends periodic updates at an interval. On Cisco routes RIP uses a 30-second update interval by default.
- Full updates: The routers send full updates every time instead of just sending new or changed routing information.

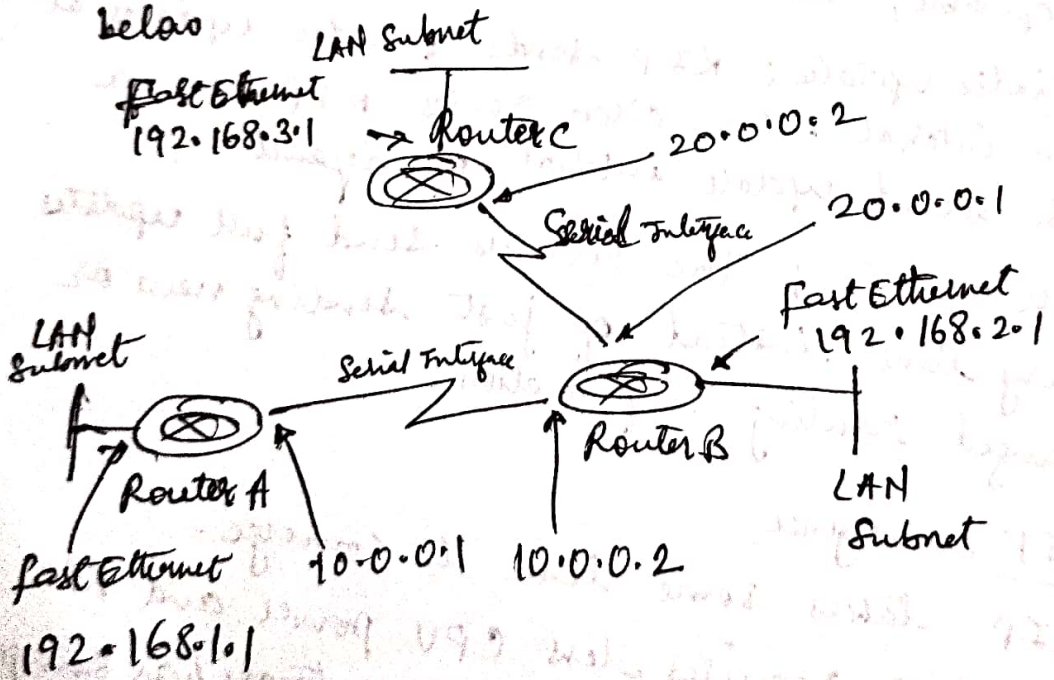
RIP Convergence

- RIP takes some time to converge.
- But RIP requires less CPU power and RAM than some other routing protocols (as compared to OSPF or EIGRP)

RIP Working

- Routers using RIP advertise information about each subnet to their neighbors.
- Their neighbors in turn advertise the information to their neighbors, and so on, until all routers have learned the information.
- This continues till every router in the n/w gathers information about every other router in the n/w.
- Such type of routing is called as routing by route rumors (Information remains same, doesn't change).

To understand the operation of RIP, Let us consider a n/w with 3 routers as shown below



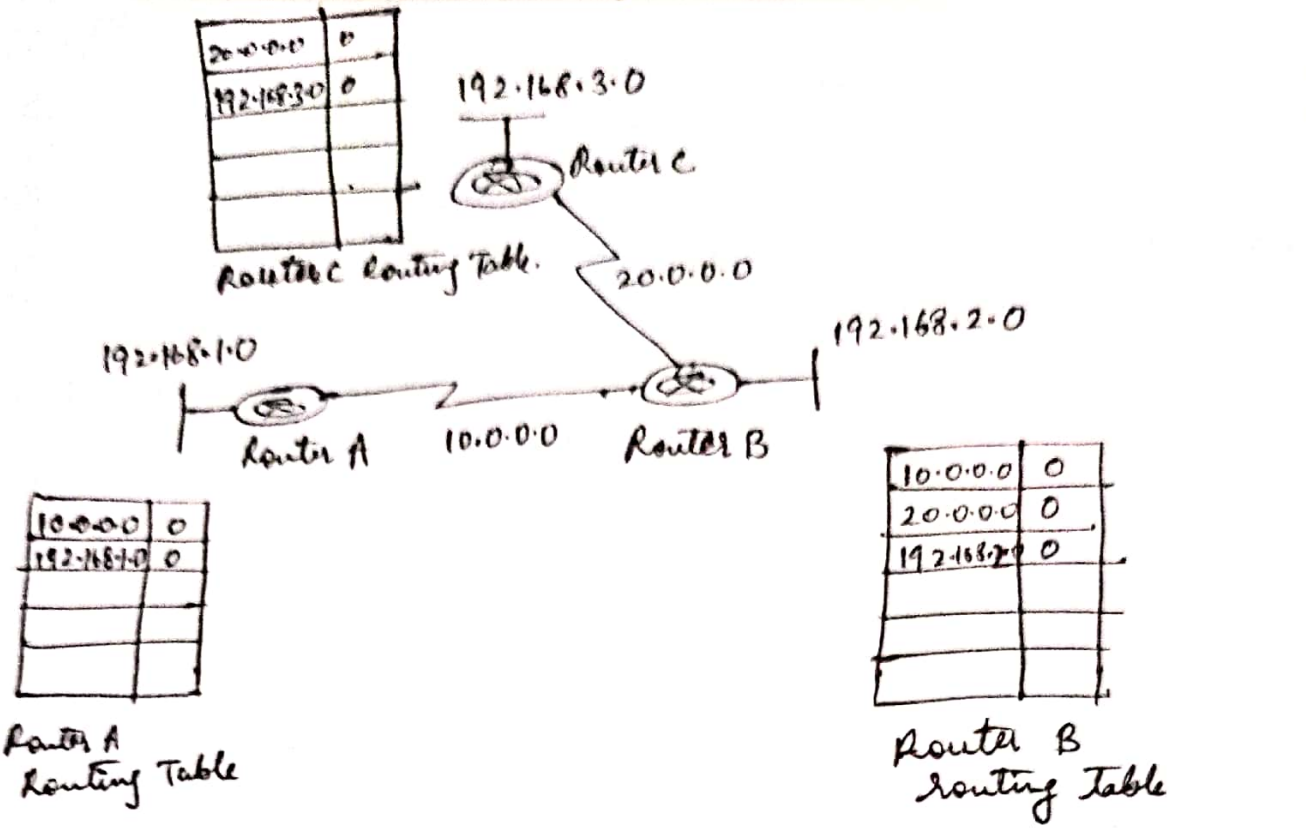
Subnet used bet^n Router A & B is 10.0.0.0

—"— Router B & C is 20.0.0.0

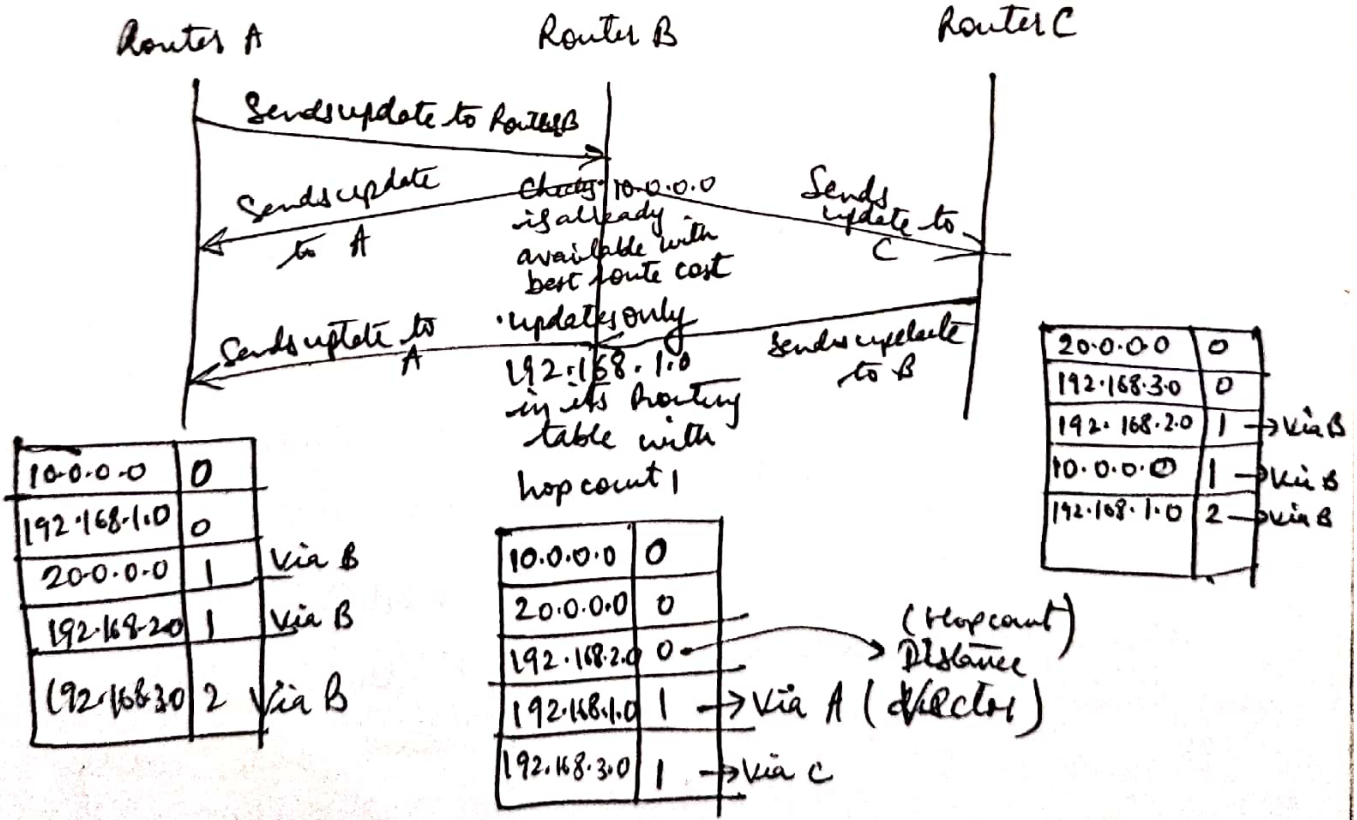
Illy Subnet used for Router A LAN is 192.168.1.0

—"— B —"— 192.168.2.0

—"— C —"— 192.168.3.0



Now Lets say RIP is configured on the routers.

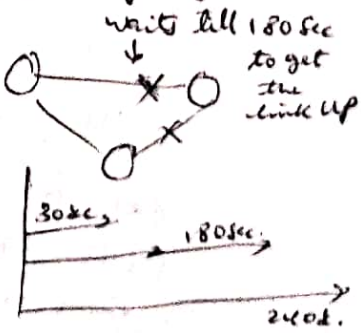


Routing Information Protocol

- **Routing Information Protocol V1**
  - Open standard Protocol (e.g. routers on all cisco, Juniper etc routing
  - Classful routing protocol (does not accept VLSM ; fixed /8 /16 or /24)
  - updates are broadcasted via 255.255.255.255
  - Administrative distance is 120
  - Metric : Hop count
    Max hop counts : 15
    Max routers : 16
  - Load Balancing of 4 equal paths
  - used for small organizations
  - Exchange entire routing table for every 30 seconds
  - uses Bellmanford routing protocol.

RIP Times

- Update timer : 30 sec
  - Time between consecutive updates.
- Invalid timer : 180 sec
  - Time a router waits to hear updates
  - The route is marked unreachable if there is no update during this interval.
- flush timer : 240 sec
  - Time before the invalid route is purged from the routing table.



Advantages of RIP

- Easy to configure
- No design constraints
- No complexity
- Less overhead.

Disadvantages of RIP :

- Bandwidth utilization is very high as broadcast for every 30 second.
- Works only on hop count
- Not scalable as hop count is only 15
- Slow Convergence.

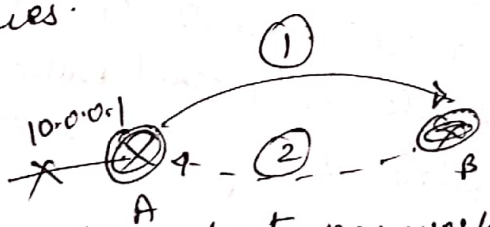
RIP Version 2

- Classless routing protocol
- Supports VLSM
- Auto Summary can be done on every router.
- Supports authentication
- Trigger updates
- Uses multicast address 224.0.0.9

Split Horizon

- A router never sends information about a route back in the same direction in which original information comes.

e.g.



Router A sends information about non working condition of 10.0.0.1 n/w to B via path (1) then B will not send any info about that same n/w on the via the same path rather it will use another path (say (2)) to send some other information.

Route Poisoning

- In this a router advertises infinite metric (metric 16) i.e. n/w unreachable) whenever a particular n/w is down.

Poison Reverse

- It breaks Split horizon rule.
- If Router A (metric 16) then Router B receives route poisoning from Route poisoning (metric 16) to A. Router B sends back the route
- In this way all routers in the n/w learn about the n/w condition (down condition) (Split horizon overruled).

Hold Down Timers

- After hearing a route poisoning, router starts a hold-down timer for that route.
- If it gets an update with a better metric than the originally recorded metric within the hold-down timer period then it uses that metric.

BGP

- Border Gateway Protocol
- Exterior Routing Protocol
- Routing between AS (Autonomous Systems)
- Routing Protocol for Internet.
- ISPs (like Bharti Airtel, BSNL, MTNL, Tikona Broadband) use BGP for comm bet^n them.
- Very Big organizations can also use BGP
- History of BGP
  - EGP
  - BGP v4
  - CIDR
- BGP is neigh neither Link State nor Distance Vector.
- BGP is called as path vector Routing protocol
- In BGP, Routing decisions are made based on
  - Path
  - Network Policies
  - Rules
- Metric of BGP is
  - Very complex and Big
  - Composite metric
  - Tunable with attributes

- If attributes are not tuned in BGP then it behaves similar to distance vector routing protocol (but instead of number of hops, it uses number of autonomous systems for routing decisions)
- For communication BGP uses;
  - → TCP port number 179
  - → TCP is used for reliability
  - → Slowest Routing protocol.

Q. BGP is ?

a) Path Vector routing protocol
b) Distance Vector routing protocol
c) Link state routing protocol.

BGP Terminology

- BGP Peers
- Autonomous Systems (AS)
- IANA & RIRs
- NLRI
- BGP Types
- BGP Attributes

BGP Peers and Peering

- BGP neighbors
- When BGP Routers exchange routes with another BGP Speaking device (the process is called BGP Peering)
- Established by manual configuration

BGP AS (Autonomous System)

- Group of routers
- Share similar routing policies
- Operate within a single administrative domain
- Typically belongs to one organization
- AS numbers can be between 1 to 65535

IANA and RIRs

- Internet Assigned Numbers Authority
  - Assigns IP addresses & AS numbers via RIRs
  - Manages
- Regional Internet Registries
  - RIPE for Central Asia
  - AfriNIC Africa Network Information Centre
  - APNIC Asia Pacific Network Information Centre
  - ARIN North America
  - LAC Latin America

BGP NLRI

- Network Layer Reachability Information (Tells how the information can reach the destination)
- Advertises Prefix/Length.

BGP Types

- Internal BGP (iBGP) [• Neighbors that belong to the same AS; • Neighbors need not be directly connected]
- External BGP (eBGP) [• Neighbors that belong to different AS; • Neighbors need to be connected directly]

BGP Attributes

- The metrics used by BGP are called Path attributes
- ★ AS Path
  ★ Next Hop
  ★ Local Preference etc

BGP Message Types

- Four Types
  - Open
  - update
  - Keepalive
  - Notification

Open Message

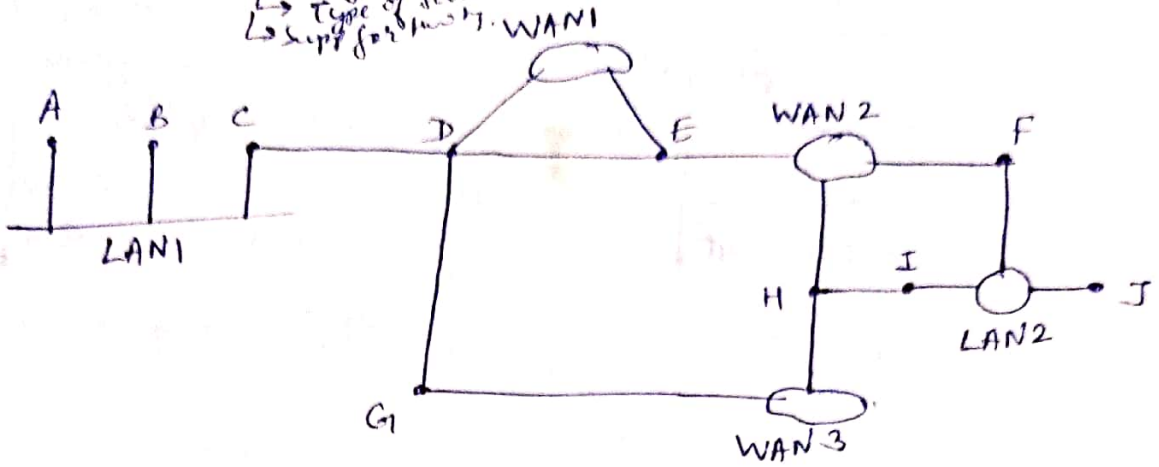
- ~~Used~~ After TCP connection has been established
- Open message is sent
- Includes set of parameters
- Have to be agreed upon by BGP neighbors

- Before establishing full BGP adjacency.

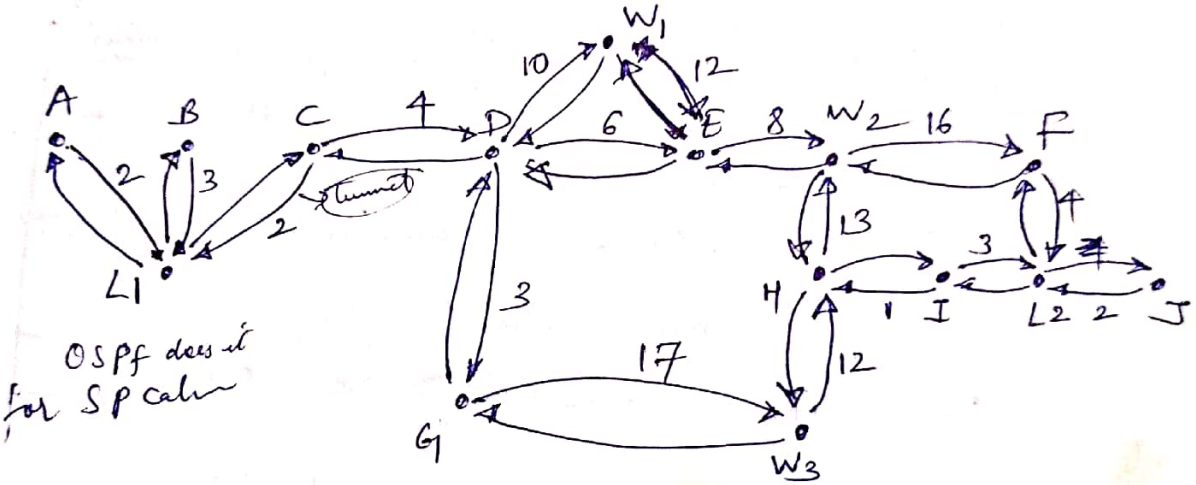
OSPF

- Multica
- O'
- Load Balan
- Dynamic pro
- Type of service
- Supp for host

3 Kinds of connection
1. Pt to Pt
2. Multiaccess n/w's with BC (eg LAN)
3. n/w w/o BC (WANs).



(a) An Autonomous System.



OSPF does it for SP calculation

(b) A Graph representation of (a).

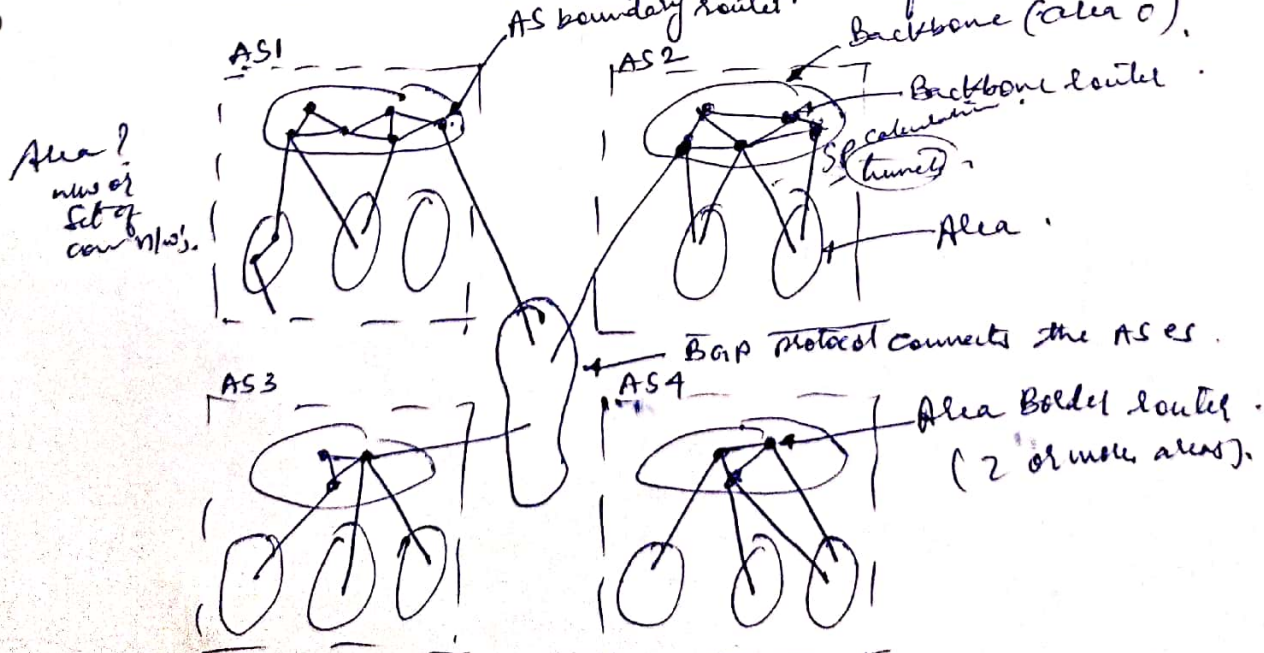


fig The relation between ASes, backbones, & areas in OSPF

Adjacent routers Designated routers (adj to all other routers & router flood)

Message Type	Description
Hello	used to discover who the neighbours are.
Link State Update	Provides the sender's costs to its neighbours
Link State ack	Acknowledges link state Update
Database description	Announces which updates the sender has
Link State request	Requests information from the partner

fig: The five types of OSPF messages (packets).

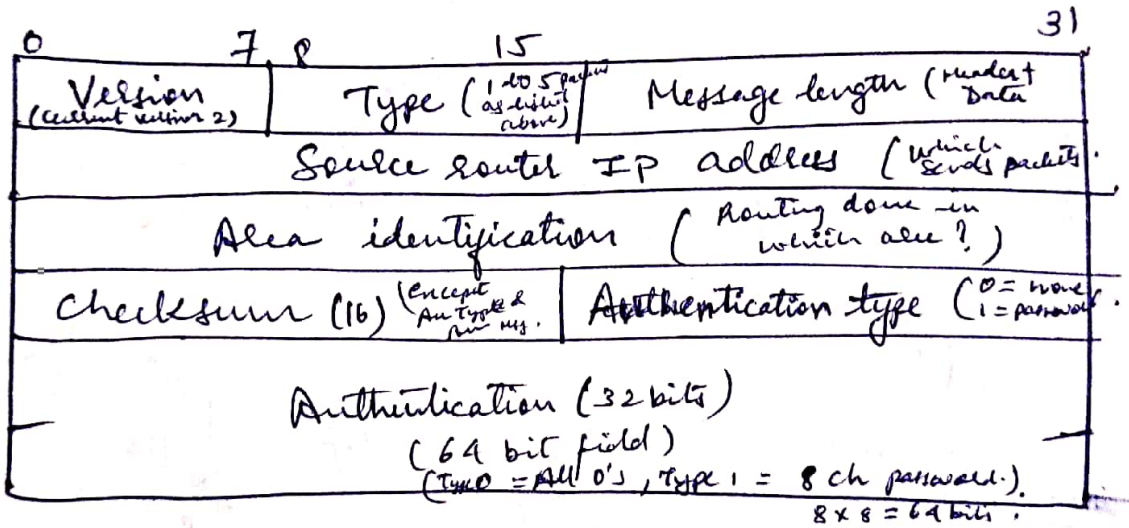


fig: OSPf common Header.

RIP (Interior Gateway protocol)

Count to infinity problem.

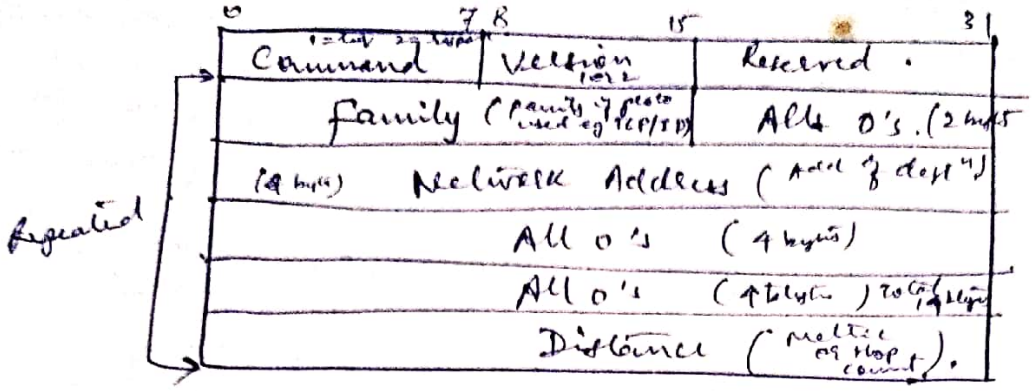
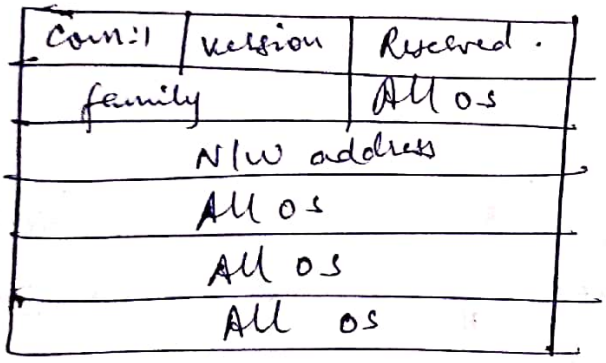
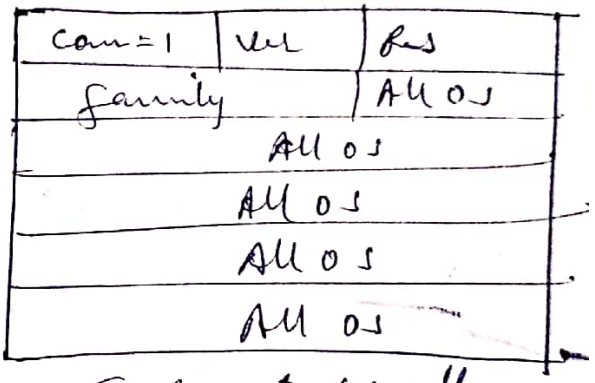


fig: RIP Message format (Also Response Msg format)

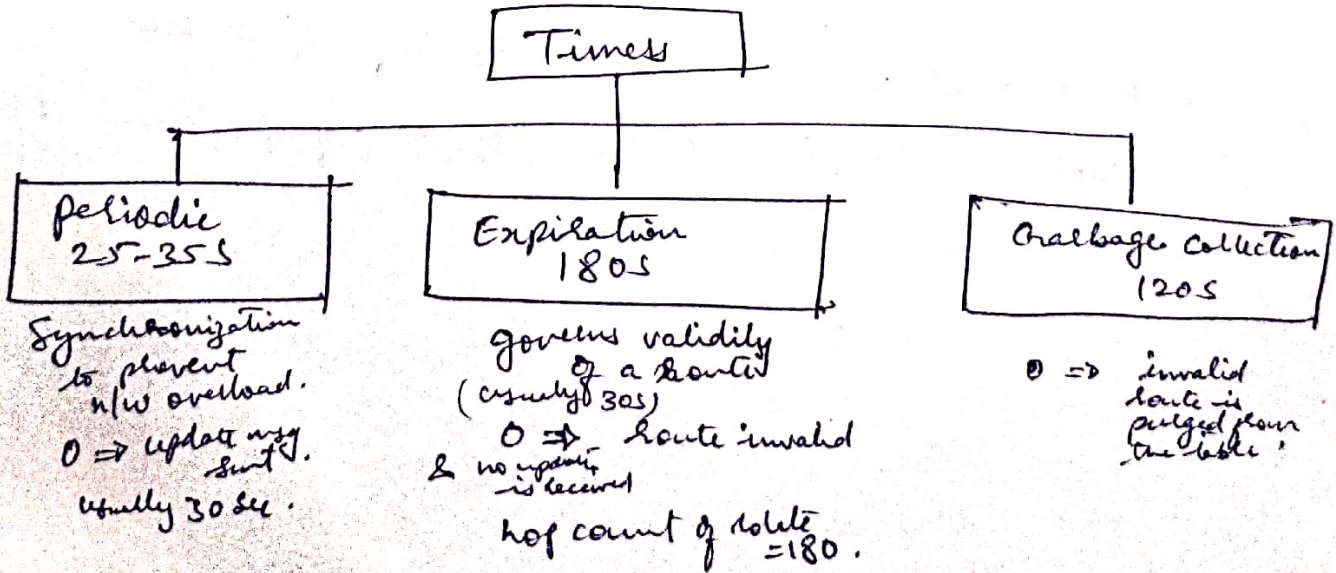


(a) Request for some.



(b) Request for all.

Times in RIP.



BGP – The Exterior Gateway Routing Protocol

- OSPF is used within a single AS.
- BGP is used between different ASes.
- Three types of n/w's →
  - Stub n/w's → • Single connection to the BGP Graph. • not used for transit traffic
  - multiconnected n/w's → • Multiple connections to the BGP Graph. • used for transit traffic
  - Transit n/w's → • Such as backbones. • willing to handle 3rd party packets.
- pairs of BGP routers communicate with each other by establishing a TCP connection thereby providing reliable communication.
- BGP is a DV protocol ~~but~~ diff from RIP.
- In addition to cost BGP routers advertise the routing path updates to other routers. (unlike RIP).

e.g.

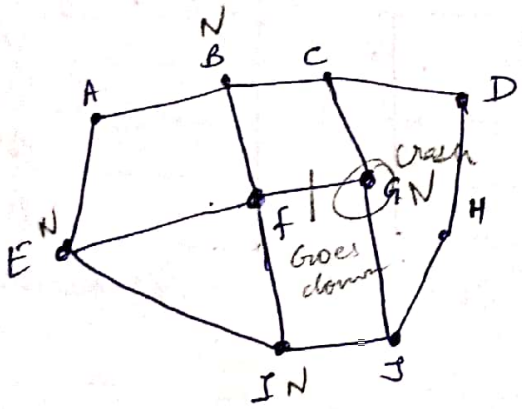


fig @ A Set of BGP routers

Information f receives from its neighbors about D

From B: "I use BCD"
From G: "I use GCD"
From I: "I use IfGCD" } decided by f.
From E: "I use EfGCD" }
N => neighbor.

f runs routing algo

- BGP easily solves the count to infinity problem.
- final shortest path to D is BCD (if G is crashed if G goes down)

	RIP	OSPF	EIGRP
Nature	Distance Vector	Link State	Hybrid
Scale	Small networks	Enterprise networks	Medium
Routing	Classful routing, loop counter mechanism	Classless	Classless 100% loop free
Metrics	Number of hops	The inverse of BW of links	Available BW, delay, load MTU & the link Reliability
updates	Periodic (Broadcast)	Incremental	Incremental updates (multicasts)
Failure Recovery	Slow convergence	Generally faster than RIP	DUAL Algorithm
Load Balancing	only supported on equal-cost paths	Support six equal cost paths, but difficult to implement	Support six equal cost paths but commonly ignored due to its complexity & instability

Features	RIP		OSPF
	Version 1	Version 2	
Algorithm	Bellman Ford		Dijkstra
path selection	Hop based		Shortest Path
Routing	Classful	classless	classless
Transmission	Broadcast	Multicast	Multicast
Administrative Distance	120		110
Hop count Limitation	15		No Limitation
Authetication	No	MD5	MD5
Protocol	UDP		IP
Convergence Time	More		Less