2.2 : ICMP (Internet Control Message Protocol)

⇒ A protocol works at network layer and is generally used for sending.

1) Error Messeges
2) Query Messages.

⇒

1) Error Messages : This messages are generally send to the sender to intimate the sender that the packet send are discarded and will not be delivered further to Receiver.

* Types of Error Reporting Messages :

i) Destination Unreachable formate : (refer notes. page 23)

ii) Source Quench : (Header. Refer note. page 23).

⇒ Sender is on a fast n/w and receiver is on a slow network, due to this Rate of sending the packet is very fast as compare to rate of receiving the packet.

⇒ As shown in diag. the packets are colliding due to conjection (Bottolenack problem).

⇒ So, to avoid this situation source quench message send to the sender. and now sender will sbw down.
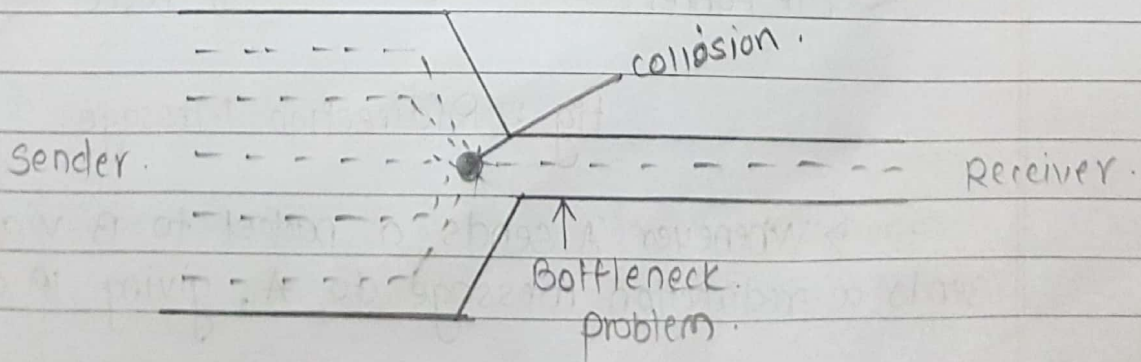
iii) Time Exceeded Message: (Header. Refer notes f...

→ Code 0: the value of TTL bec...
0 & router discards the packet. This tells se...
that packet is discarded since TTL becomes '0'.

→ Code 1: sender sends fragment...
but receiver did't receive all fragments & hence
discards the packet. This tells sender that rece...
didn't receive all fragments & hence discarded.

iv) Parameter Problem Message: (Refer note; page...

→ Code 0: It tells there was a prob...
in IP Header part & pointer tells which part of Head...
had the problem.

→ Code 1: It tells there was a proble...
in IP option part & pointer tells wich part of op...
had the problem.

v) Redirection Message: (Header Refer note page 24)
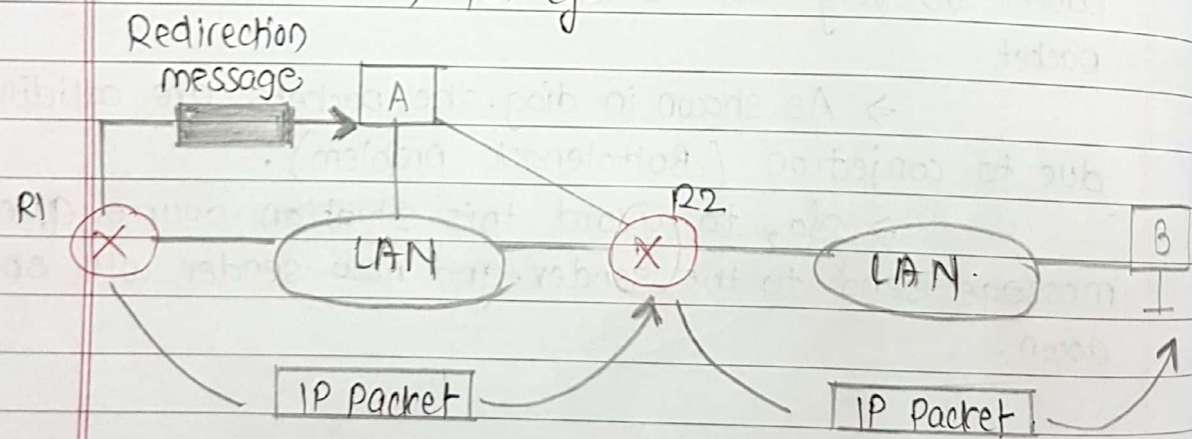
→ for eg:

Redirection
message

fig: Ridirection Message.

→ Whenever A sends a packet to B via R1, R1
sends a redirection message to A, giving IP address of...

and telling A Henceforth send packet to R2 for B.

✗ QUERY MESSAGES :

→ Query messages also require a response message & their are following types of query messages.

1) Echo Request & Reply : (Header. Refer notes : page 25)

→ It is used for checking n/w integrity when client sends echo reques message "hi" server receives the same message & should reply with the same message back the client.

→ If the sending & receiving message is different then the n/w is not safe & cannot maintain integrity.

2) Timestamp Request & Reply : (Header. Refer notes : page 25)

→ This is used for calculating RTT (Round Trip Time).

→ When the packet is sent, sender enters original time stamt.

→ Receiver after receiving enters Receiving Time stamp & sends back the packet at that time enters transmit timestamp

→ Finally Receiver receive back the packet & can easily calculate Round Trip Time (RTT).

3) Mask Request - Reply :

17 : Request
18 : Reply

Type : 17 or 18	Code : 0	checksum
Identifier		Sequence Number
Address Mask		

⇒ Whenever client sends this request packet, server (ISP server) sends the mask of n/w to which client belongs.

4) **Router - Solicitation & Advertisement Message.**
   ⇒ Routers keep on giving some periodic information to neighbors.

for eg :

R1 → ⇄ R2

⇒ For some reason, R1 is not getting any msg from R2. So R1 feels whether R2 is alive or dead.
⇒ So, now R1 sends "Solicitation" to R2 & if R2 is alive it sends back advertisement message to R1.
   10: Solicitation
   9 : Advertisment

Type :10,9	Code : 0	Checksum
Identifier		Sequence number