INTERNET CONTROL MESSAGE PROTOCOL

- Since IP does not have a inbuilt mechanism for sending error and control messages, it depends upon ICMP (Internet Control Message Protocol) to provide an error control.
- It is a supporting protocol and used by network devices like routers for sending the ~~editor~~ error messages, and managenet queries or operations information.
- The messages are divided into following:

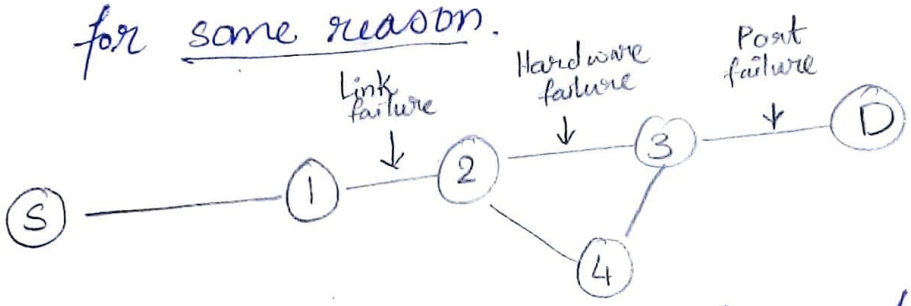
ICMP

Error Reporting Messages	Query Messages
– Destination Unreachable	– Echo Request & Reply
– Source Quench	– Time Stamp request & Reply
– Time Exeeds	– Address mask Request & Reply
– Parameter Problem	
– Redirection	

Error Reporting Messages

#1. Destination Un-Reachable

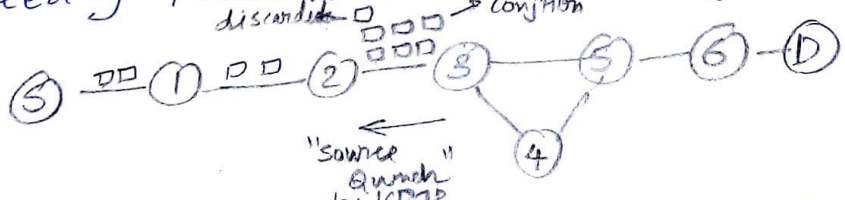
- Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.



- This failure can be of any form: Link, Hardware, Port. etc.

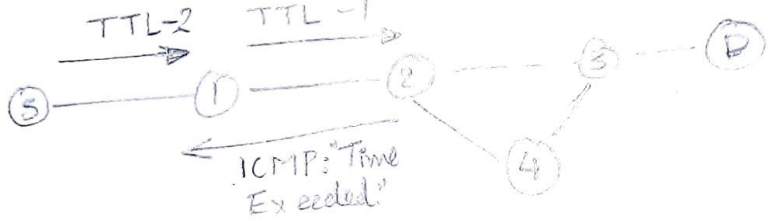
#2. Source Quench

- Source quench messages is a request to decrease traffic rate for messages sent to the destination.
- When the rate of packets sent is high, there is either packet loss or conjestion occurs.
- When conjestion routers far away, ICMP will send hop by hop source quench to reduce the speed of transmission at every router.



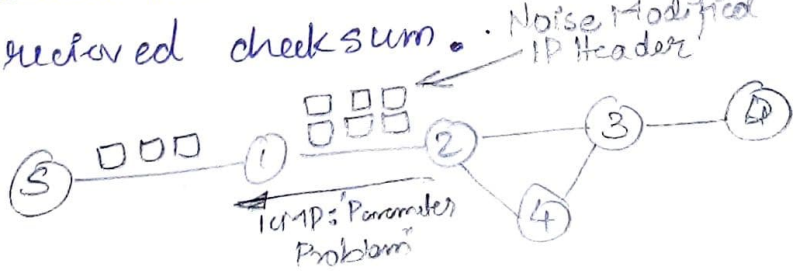
#3. Time Exeeds

- Each packeat in the headerd is embedded with a time to live (TTL) counter.
- When some fragments are lost in a network then the ~~holding~~ fragment held by the router will be dropped.
- ICMP takes the source IP address from the dropped packet and sends it back to the soure ~~with~~ a message "Time Exeeds".



#4. Parameter Problem

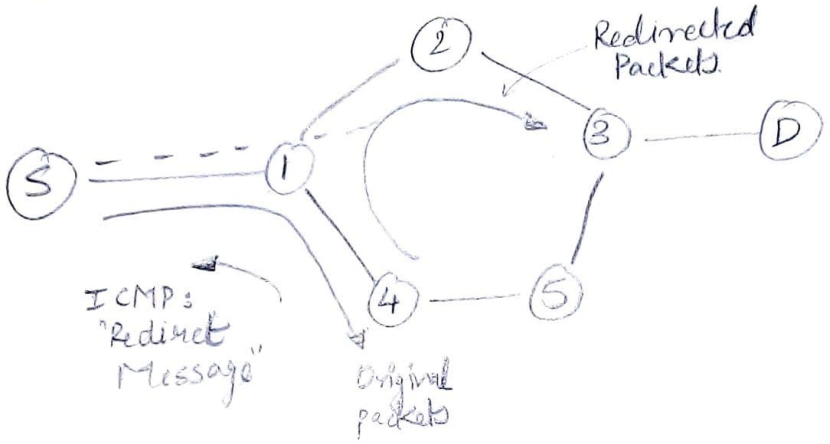
- Whenever packets come to the router then the calculated header checksum must be equal to the recieved checksum.



- If there is a mismatch packet will be dropped by the router, and so again ICMP will take the source IP from the discarded packet and send "Parameter Problem" to the source.

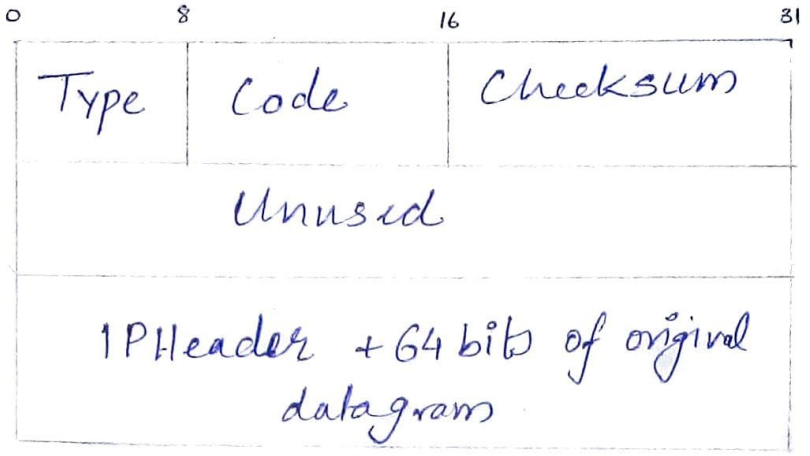
#5. Redirection

- When a host tries to send data through a particular router, it send back a "Redirect" notice to the host.
- This can happen because the router is aware of a better alternate route to duction and asks the host to update its routing information.

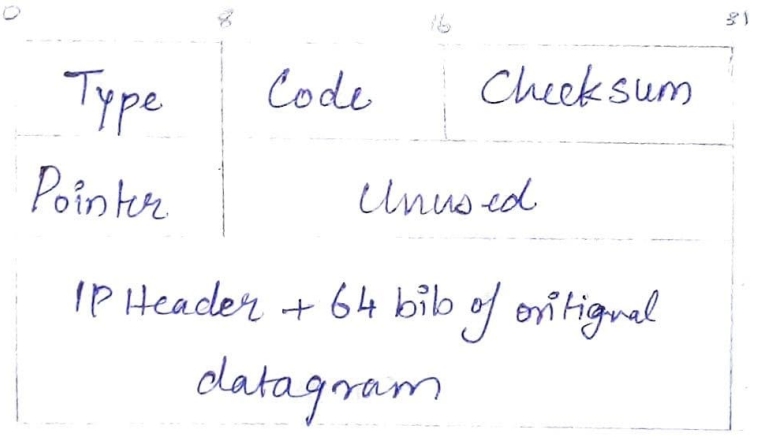


- ICPM obtains the source IP from the dropped packets and sends the Redirect notice and subsequently the routes are updated.

* Message formats for
"Error Reporting Messages"



Destination Un-Reachable; Time Exceeded; Source Quench



2 Qaury Messages

#1. Echo Request and Reply

- Echo Request or Reply is the first step towards checking in the destination device is alive or not.
- To check it, the source device sends an ICMP Echo message to the destination to which the destination responds with "Echo Reply".
- Once this round about transaction is completed the source is aware of the state of destination.

Type	Code	Checksum
Identifier		Sequence Number
Optional Data		

#2. Timestamp request or reply

- It basically serves two purposes
- One is to check the performance of the network.

~ Second is to sync up the timings between networks that vary by time zones.

Type	Code	Checksum
Identifier		Sequence Number
Originate time stamp		
Recieve time stamp		
Transmit time stamp		

#3 Address Mask Request or Reply

~ It is used to found out the subnet address of the destination network where the packet hast to be sent.

Type	Code	Checksum
Identifier		Sequence Number

Type	Code	Checksum
Identifier		Sequence Number
Address Mask		

ADDRESS RESOLUTION PROTOCOL

- Any time a host or a router has an IP datagram to send to another host or router, it has the logical (IP) address of the reciever.
- The sander needs the physical address of the reciever, so it send an ARP query packet.
- ARP is a mechanism which enables mapping logical address to physical address.
- The intended reciever accepts the ARP broadcast and sends back the ARP response packet.
- The reponse packet contains the recipient's IP and physical Address.

Packet Format

Hardware Type		Protocol Type
Hardware Length	Protocol Length	Operation Request (1), Reply (2)
Sender hardware Address		
Sender protocol Addres		
Target Hardware Address		
Target Protocol Address		

Static ARP

- A MAC/IP table is maintained and so each device with unique MAC can provide corresponding IP.
- But this method is not feasible as IP address tend to change frequently.
- The MAC (48 bit) address is a unique vendor IP provided to each network card.

Dynamic ARP

- Multiple methods are used to perform dynamic ARP.
- The sender broadcasts the ARP - packet as sender IP, reciever IP & sender MAC.
- The reciever / destination responds to this broad cast.

REVERSE AUTOMATIC ~~REQUEST~~ ADDRESS RESOLUTION PROTOCOL

- Reverse automatic address resolution protocol by which a physical machine in a local area network can request to learn it IP address from a gateway server's ARP table or cache.
- Network devices like switches don't have additional memory hence an IP loopup is necessary.
- Network administrator creates a table in a local area network's gateway router that maps the physical machine address (MAC) to the corresponding IP.
- When a new machine is set up RARP client program requests from RARP server.
- Server answer request by filling in the target protocol addrs field, changing the message type from request to reply.

* Demerits

- Since it operates at a low level, it requires direct address to the network which makes it difficult for an application programmer to build a server.
- It does not fully utilize the scalability of a network like ethernet which is enforced by a minimum packet size.
- RARP depends heavily on MAC protocol hence it cannot be used in networks that dynamically assign hardware address.
- RARP just supplies the IP address corresponding to a MAC address, it does not support respond with any more data.

BOOTP

~ The BOOTP uses UDP/IP. It is run when the machine boots.

~ The protocol allows diskless machine to discover their IP addres and addres of the server host.

~ BOOTP doesn't use the MAC layer broadcast but uses UDP/IP.

* Events in BOOTP

1. The client broadcast it MAC addres (or other unique hardware identity number)
2. The BOOTP server responds with the data that specifies how the client should be configured (pre-configured for specific client).

DYNAMIC HOST CONFIGURATION PROTOCOL

- DHCP (Dynamic Host Configuration Protocol) is a protocol that lets network administrators manage centrally and automate the assignment of internet protocol.
- DHCP lets a network-administrator supervise and distribute IP addrss from a central point.
- DHCP is based on a client-server model and based on discovery, offer, request and ACK.