1. Static Mapping :-

* In this, we create a table that associates a logical address with a physical address and store in each machine.

* Static IP address does not change any time, is less secure, is difficult to designate but is more stable than dynamic address.

* The cost to maintain static address is high and is used where computational data is less confidential.

Dynamic Mapping =

* In this, we use a protocol to find another address.

ARP - map a logical address to physical address

RARP - map physical address to logical address.

* Dynamic IP address change any time and is easy to designate. It is less stable than static IP address and cost maintenance is comparatively less. It is used where data is more confidential and needs more security.

2. Time stamp request & time stamp reply messages in ICMP are used to determine the round trip time needed for an IP datagram to travel between them. It can be used to calculate round trip time and synchronize two clocks in 2 machines if the exact one-way time duration is known.

sending time = receive timestamp − original timestamp

receiving time = returned time − transmit timestamp

round trip time = sending + receiving time.

3. 3-way handshake TCP.
   - Clients establish connection with server − SYN
   - Server responds to client request with SYN-ACK signal bits set.
   - Final step is client acknowledgment of server response and connection established.

4-way handshake TCP.
   - When client/server closes connection, TCP sends FIN. Then next FIN segment which performs passive close.
   - The application will close the socket and TCP sends a FIN.
   - Finally, TCP receives a final FIN [the end which initiated the active close] acknowledges the FIN.

Four packets required to close connection so it is 4 way handshake.

4. **ICMP**

It is a supporting protocol used by network devices like routers for sending error messages and operations information.

Need of ICMP in error scenario:

i) **Source quench message:**

When receiving host detects that the rate of sending packets (traffic rate) to it is too fast, it sends source quench message, a request to the source to decrease traffic rate and slow down the pace so that no packet is lost and congestion is reduced at a particular router.

ii) **Parameter problem:**

The calculated leader checksum should be equal to the received leader checksum when packets come to the router. The router discards the packet in case of mismatch so ICMP will take source IP from discarded packet and informs to the source by sending a parameter problem message.

iii) Time exceeded message :
        When some fragments are lost
in a network, then the holding
fragment by the router will be
dropped then ICMP will take source
IP from discarded packet and informs
the source, of discarded datagram
due to time to live field reaches
zero, by sending time exceeded message.

iv) Destination unreachable :
        This message comes into play
in case of link, hardware or
port failure.

v) Redirection message :
        This comes into play if there
is a shorter route to the
intended destination or intermediate
router. The message informs a host
to update its routing information
and send packets to an alternate
route.

5. Multicasting and Multiple Unicasting:
In this, one nodes sends the same information (maybe a combination of incoming flows) to multiple successors. This is how it is broadcasted.

In multiple unicast, there are several sources and each source needs to communicate to its relative sink and each node can send different combination to its neighbours.

In multicasting, single packet travels between 2 routers. eg:- Teleconferencing.

In multiple unicasting, multiple copies are sent between 2 routers like eg:- a group e-mail.

ABHINAV RANJAN

RA 1911003010003

CSE A1

SRMIST, KTR