PAGE NO.:

NAME - YOGESH SINGH

CLASS - BE IIIyr CSE-A (6th SEM)

SUBJECT - WIRELESS NETWORKS

ROLLNO - 17CG063

ENROLL - DE17 192

ASSIGNMENT-4

Q1.) Explain different Entities and terminologies of Mobile network layer along with their functionalities.

Ans.) • Mobile Node (MN): It is the hand-held communication device that the user carries.
Eg: Cell phone.

• Home Network:
It is a network to which the mobile node originally belongs to as per its assigned IP address (home address).

• Home Agent (HA)
It is a router in home network to which the mobile node was originally connected.

• Home Address: It is the permanent IP address assigned to the mobile node (within its home network)

• Foreign Network: It is the current network to which the mobile node is visiting (away from its home network)

• Foreign Agent (FA):
It is a Router in foreign network to which mobile node is currently connected. The packets from the home agent are sent to the foreign agent which deliver it to the mobile node.

- Correspondent Node (CN): It is the device on the internet communicating to the mobile node.
- Care of Address (COA): It is the temporary address used by a mobile node while it is moving away from its home network.

Q2.) What are the consequences and problems of using IP with standard routing protocols for mobile communication? What are the quick solution and why we cannot use them?

Mobile IP problems and quick solution

→ Protocols were not designed by keeping the things in mind called MOBILITY.
→ Improvement in classical IP concepts, since in computer networks a IP is allocated to system for communication
→ A host needs a topological correct address (129.13.42.1)
→ Solution for Mobility
Assign a new IP address when system moves from one Location to another.
- Problem with above solution is identification of new address
- But DNS can do this ... but it need time.

PAGE NO.:

One more problem with above solution is TCP relies on IP. If IP get changes TCP connection does not survive.

TCP connection is identified by a type (source IP, source port, destination IP, Destination Port)

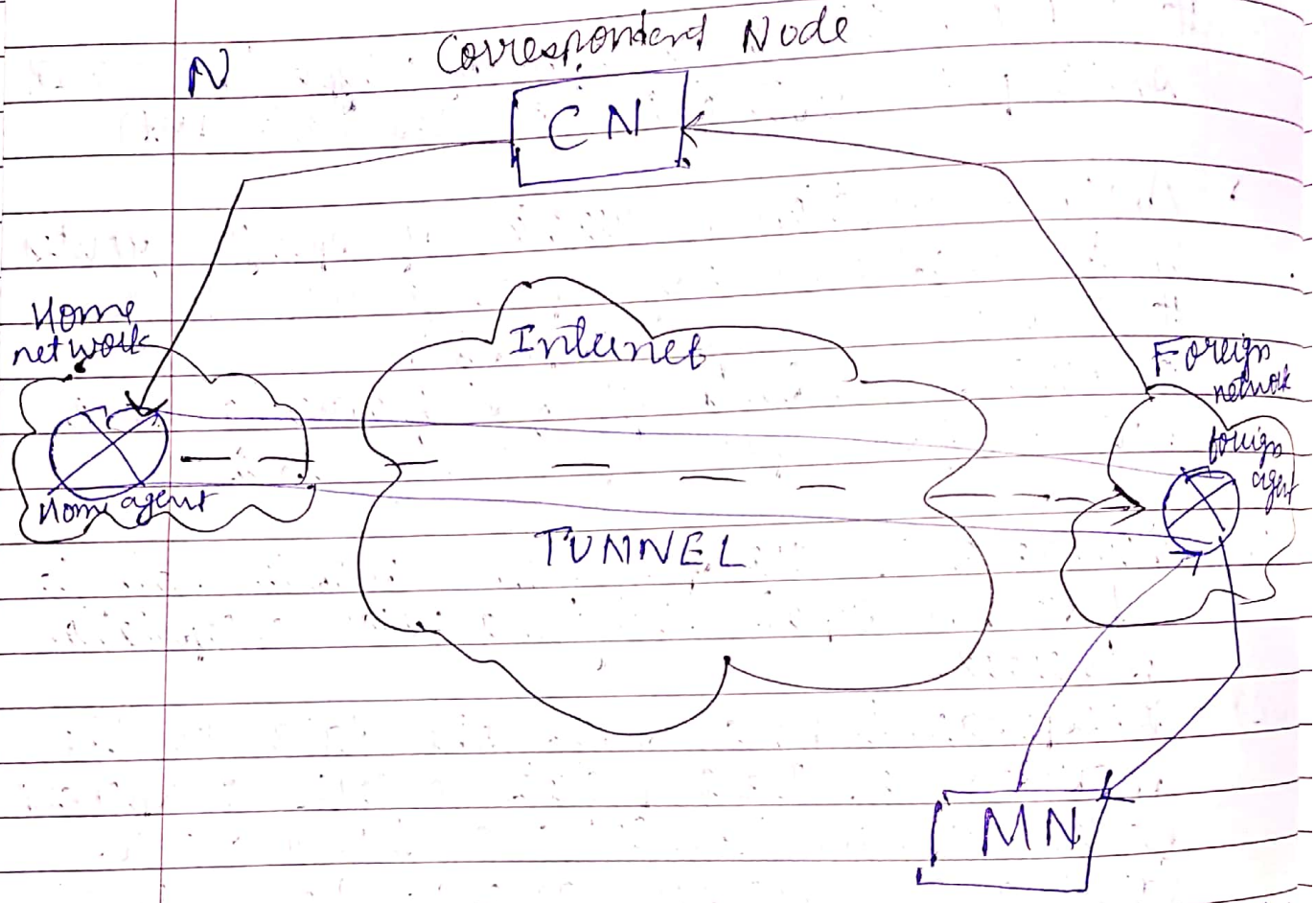
→ Another solution is creation of specific routes to the mobile node by updating the routers.
But it is practically not possible.
Routers are built for fast forwarding but not for fast updates of routing tables.

Q3) How data is transfer from a mobile node to a fixed node explain. Why and where encapsulation is needed.

Ans) Correspondent node sends the data to the mobile node. Data packets contains correspondent node's address (source) and home address (destination). Packets reaches to the home agent. But now mobile node is not in the home network it has moved into the foreign network. Foreign ~~network~~ agent sends the care of address to the home agent to which all the packets should be sent. Now a tunnel will be established b/w the home agent and the foreign agent by the process of Tunneling.

Tunneling establishes a virtual pipe for the packets available b/w a tunnel entry

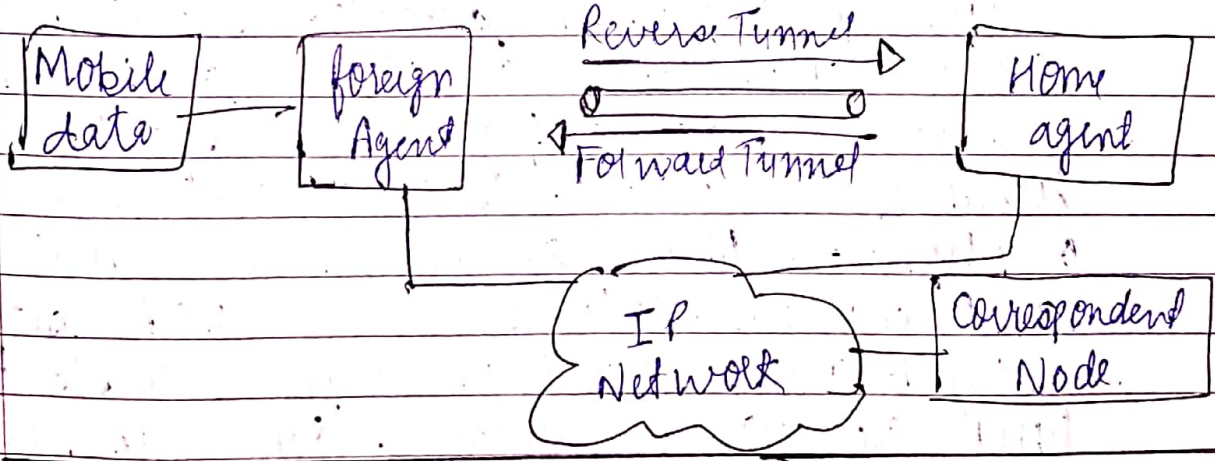
and an entry point. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called Encapsulation



Now, home agent encapsulates the data packet into new packets in which the source address is the home address and destination is care of address and sends it through the tunnel to the foreign agent. Foreign agent, on other side of the tunnel receives the data packet, decapsulates them and sends them to mobile node. Mobile node in response to the data packets received, sends a reply in response to foreign agent. Foreign agent send the reply to correspondent agent

Q4) Explain Packet flow if two mobile nodes communicate with each other and both are in foreign network. What additional routes do packets take if reverse tunneling is required.

Ans:) If HN_a and HN_b are both in foreign network attached to FA_a and FA_b the packet flow is as follows: HN_a sends packet to HN_b via the internet to HA_b (actually, HN_a sends to HN_b's address, the packets are only intercepted by HA_b). HA_b encapsulates the packet to FA_b, which then forwards the packet to HN_b. If reverse tunneling is required, the packet flow is as follows: HN_a send its packet via FA_a through the reverse tunnel via HA_a and the internet to HA_b, HA_b then forwards the packet through the tunnel to FA_b which in turn forwards the packet to HN_b.



Q5 What is DHCP? What is its purpose? Name the entities of DHCP. How can DHCP be used for mobility and support of mobile IP?

DHCP (Dynamic Host Configuration Protocol) is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.
It will assign new IP address in each location when device are moved from place to place, which means network administrators do not have manually configure each device with a valid IP address or reconfigure the device with a new IP address if it moves to a new location on the network.

Components –
DHCP is made up of numerous components, such as the DHCP server, client and relay. The DHCP server – typically either a server or router – is a networked device that runs on the DHCP service. The DHCP server hold IP addresses, as well as related information pertaining to configuration. The DHCP client is a device – such as a computer or phone – that can connect to a network and communicate with a DHCP server. The DHCP relay will manage requests b/w DHCP clients and servers. Typically, relays are used when an organization has to handle large and complex networks. Other components include the IP address pool, subnet, lease and DHCP communication protocol.

How can DHCP be used for mobility and support of Mobile IP?

DHCP is a good candidate for support the acquisition of COA for mobile nodes. The same holds for all other parameter needed, such as address of the default router, DNS servers etc. A DHCP server should be located in the subnet of the access point of the mobile node, or at least a DHCP relay should provide forwarding of the messages.

Q6.) Compare different type transmission error that can occur in wireless and wired networks.

Ans) Packet Loss due to Congestion –

Congestion may appear from time to time even in carefully designed networks. The packet buffers of a router are filled and the router cannot forward the packets fast enough because the sum of input rates of packets destined for one output link is higher than the capacity of the output link. The only thing a router can do in this situation is to drop packet. This kind of packet loss can occur in both wireless and wired networks.

Packet loss due to Random Loss –

The random loss is due to bit corruption and link errors. In wired networks, the transmission error rate (10-10 – 10-12) is

generally very low so that it can be neglected however it is not true for the wireless network (10-2-10-4).

Packet loss due to burst loss:
The burst loss may be initiated by signal fading. Prolonged uncontrolled channel interference can lead to correlated packet losses. Yet it generally occur over a very short duration, leading a loss of several consecutive segment at a time. In an infrastructure network, when a mobile host is moved from the coverage of a base station to another, all subsequent communication are routed via the new base station and the handoff process is completed. However the packet may be lost as they are routed to the old station during the process of the handoff. Therefore a handoff event can initiate a burst loss event. In ad hoc network, same situation can happen. During to the mobility of the mobile host, the network connectivity and the network topology can change. The transmission path for a traffic flow may be affected. Some time is necessary to complete the rerouting process for the traffic flow. Thus some packets belong to the same traffic flow may be lost during the process. As a result, a burst loss event occurs in this case.

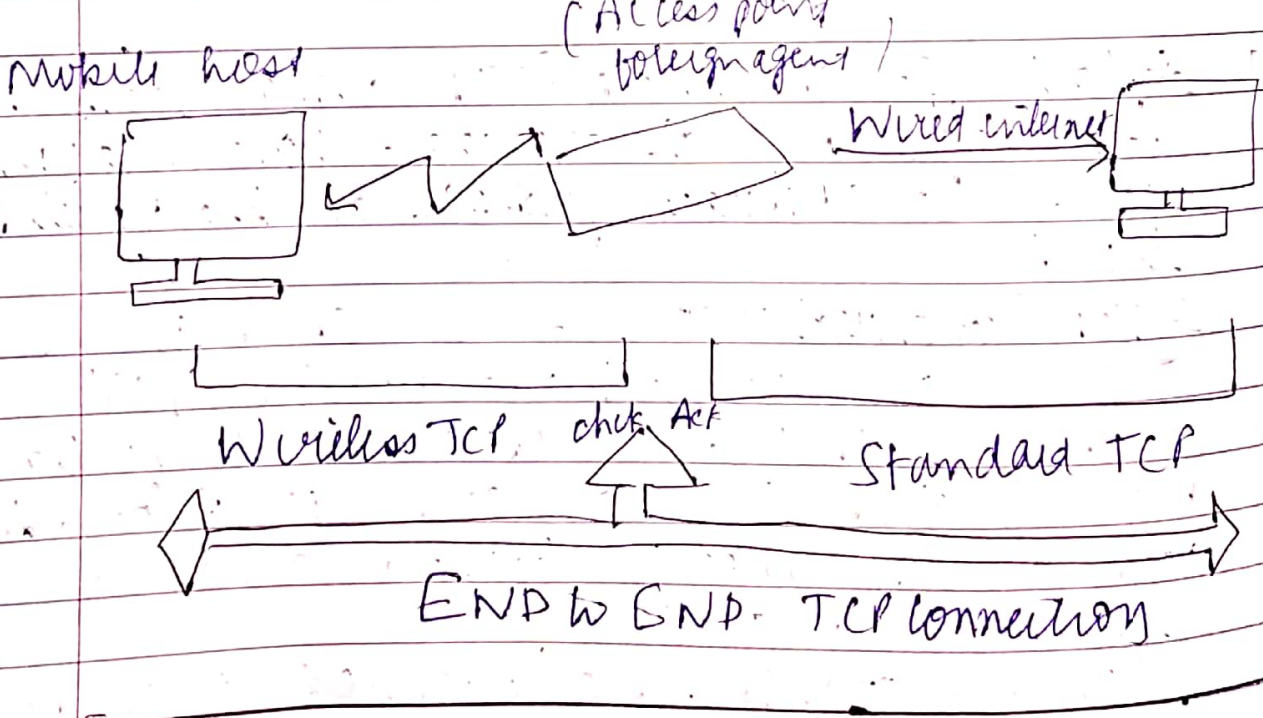
Q8) Can we solve the problem of using TCP by replacing it with UDP. Where could this be useful and why is it quite often dangerous for network stability.

Ans) Using UDP, a better throughput can be achieved. But it only works for a few users doing so. If a higher no. of users would transmit data over UDP, the missing congestion control would be lead to high packet loss rate. Furthermore, UDP does not provide reliable data transfer. This, for only small number of users, using UDP brings advantage, if the application layer takes over control functionality for reliable data transfer.
Mobility support in IP (such as mobile IP) is already enough for UDP to work.

Q9) Explain I-TCP and M-TCP along with their advantages and disadvantages. How and why does I-TCP isolate problems on the wireless link.

Ans) I-TCP (Indirect TCP) — I-TCP segments a TCP onto fixed part and wireless part
→ The example shows a mobile host connected via a wireless link to an access point (AP). Also access node is connected to the internet via the wired internet
→ standard TCP is used to connect to the AP from fixed computer. No computer over the internet recognizes any change to the TCP

→ The AP act as a proxy of mobile host and terminates the TCP connection.
→ Therefore, the fixed computer now sees the AP as mobile host; on the other hand the mobile host sees AP as the fixed computer.
→ In b/w AP and mobile host a special TCP adapted to wireless link is used.
→ A FCP change in TCP is not needed as even as unchanged TCP produces the same round trip time.
→ Such segmentation method can be used in connection b/w mobile host and correspondent host when host is at the FA, so during handover control transfer from one FA to another FA in nearby cell.



PAGE NO.:

Advantages of I-TCP:-

→ Does not require any change in TCP
→ Due to Partitioning into two connection the lost packet does not propogate to fixed network.

Disadvantages of I-TCP:-

→ Dependency on FA
- If it get failed
- All packets will buffered on FA
- Trusting FA.

☆ Mobile TCP (M-TCP):-

- The M-TCP splits up the connection into 2parts.
  → An unmodified TCP is used on the standard host - supervisory host section.
  → An optimised T.CP is used on the Supervisory Host - Mobile Host section.
- The supervisory Host (SH) adopts the same role as the proxy (Foreign agent) in I-TCP
- The SH is responsible for exchanging data to both the standard Host and the mobile host.
- Here in this approach, we assume that wired bit rate is less as compared to air the wireless links.
- So if any packet is lost, the retransmission has to occur from the original sender and not by SFH
- The SH monitors the Ack's being sent by MH. If for a long period Ack have not been received, then thySH assumes that

the MH has been disconnected.
- If so the SH chokes the sender by setting its window size to 0.
- Because of this the sender goes into persist mode i.e. the sender's state will not change no matter how long receiver is disconnected.
- This means that sender will not try to retransmit data.
- Now when the SH detects a connection established again with the MH, the window of the sender is restored to original value.

Advantages of M-TCP :-
→ Maintains the TCP end to end semantics
→ If the MH is disconnected, it avoids useless retransmission, slow starts or breaking connection by simply shrinking the sender window too.

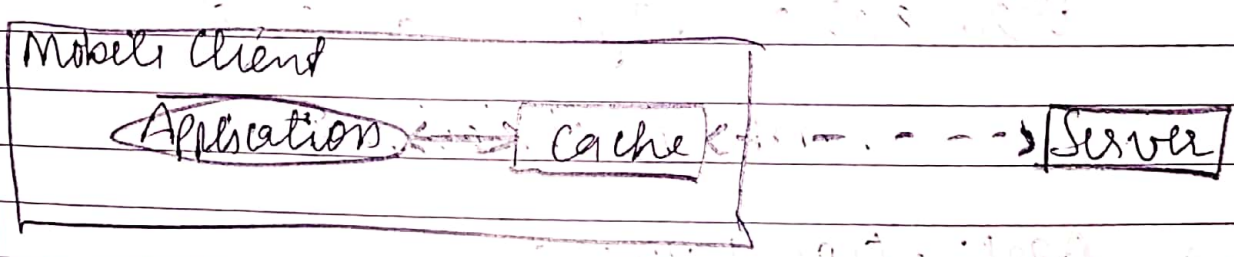
Disadvantages of M-TCP -
→ As the SH does not act as proxy as in I-TCP packet loss on the wireless link due to bit errors is propagated to the sender.
→ A modified TCP on the wireless link requires modification.

I-TCP isolates problem on wireless link from the fixed network. However, this also requires the intermediate systems are able to look into IP packets to split the connection. This

prevents the usage of IP sec - end to end security and E-TCP (Confidentiality solution in general) do not go together.

Q10) Explain :-

(a) CODA file system :-
CODA is an advanced networked file system for a large scale distributed computing environment. It is composed of UNIX work stations & operate on linux environment. It provides resiliency to server and network failures through the use of two mechanism
→ Server Replication
:- It stores copies of file at multiple servers
→ Caching on clients



features of CODA :-
1) disconnected operations for mobile computing
2) It is freely available under GPL
3) High performance through client side persistent caching
4) Server replications
5) Security model authentication, encryption and access control

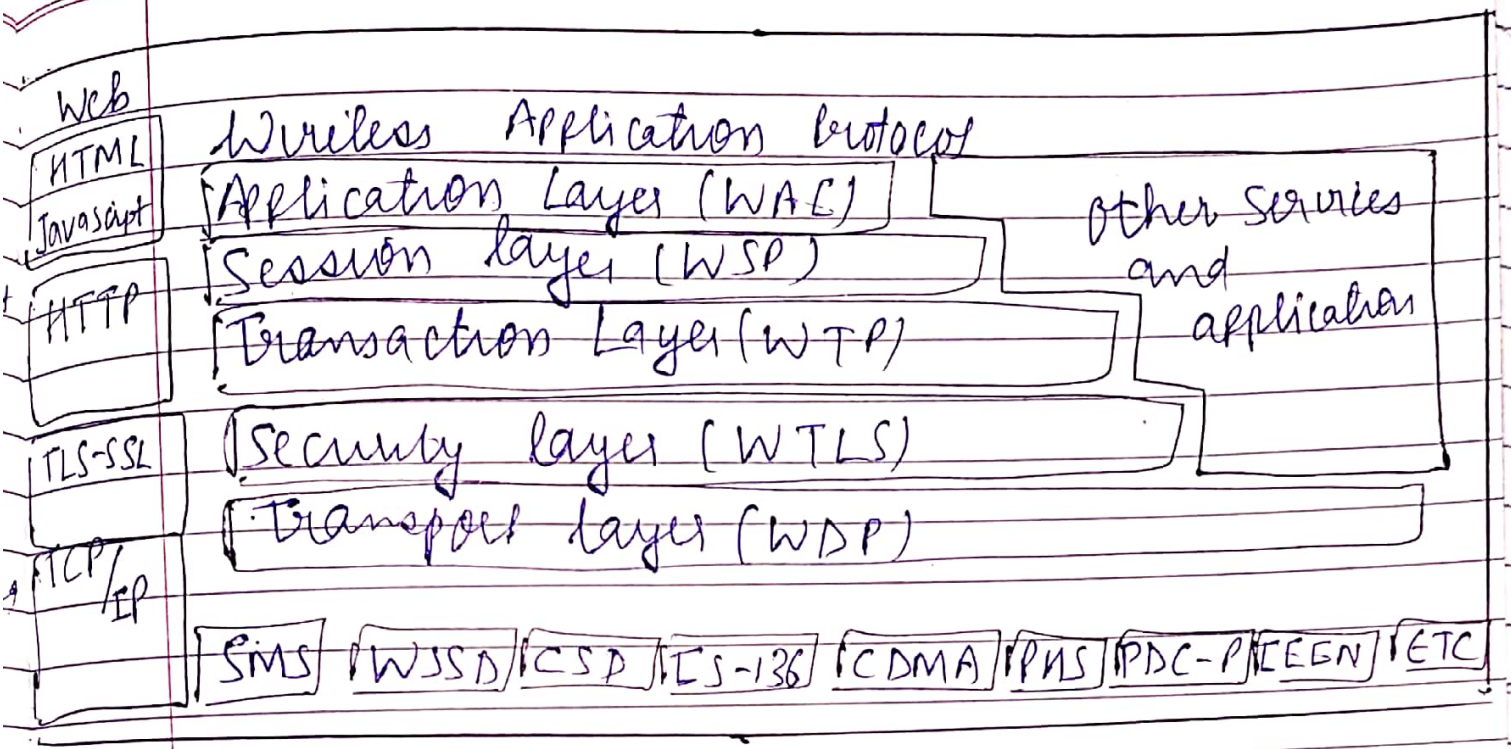
6) Continued operation during partial network failures in server network.
7) Network bandwidth adaption
8) Good scalability
9) Well defined semantics of sharing, even in the presence of network failures.

(b) WAP Architecture :-
It provides scalable and extensible environment for application development of mobile.
→ It is achieved using layered design of protocol stack. The layers resembles the layers of OSI model. Each layer is accessible by layers above as well as by other services and application through a set of well defined interface.
→ External applications may access session, transaction layers directly.

WAP Architecture

→ Application Layer :-
This layer contains wireless application environment (WAE). It contain mobile device specifications and content development programming languages like WML.

→ Session Layer -
It contain wireless session protocol (WSP). It provides fast connections suspension and reconnection



→ Transaction Layer —
This layer contains wireless Transaction protocol (WTP). It runs on top of UDP and is part of TCP/IP and offer transaction support.

→ Security layer:-
This layer contains wireless Transaction layer security (WTLS). It offers data integrity, privacy and authentication

→ Transport layer.
This layer contain wireless Datagram protocol (WDP). It presents consistent data format to higher layers of WAP protocol stack.