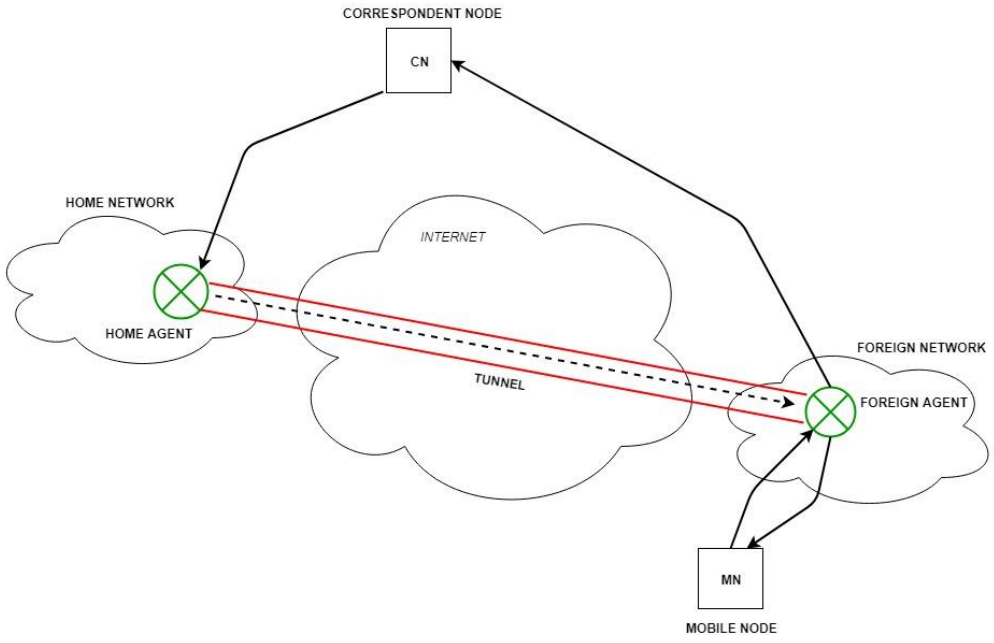
Unit 4

****Mobile IP** is a communication protocol that allows the users to move from one network to another with the same IP address. It ensures that the communication will continue without the user's sessions or connections being dropped.

Terminologies:

1. **Mobile Node (MN)** is the hand-held communication device that the user carries e.g. Cell phone.
2. **Home Network** is a network to which the mobile node originally belongs as per its assigned IP address (home address).
3. **Home Agent (HA)** is a router in-home network to which the mobile node was originally connected
4. **Home Address** is the permanent IP address assigned to the mobile node (within its home network).
5. **Foreign Network** is the current network to which the mobile node is visiting (away from its home network).
6. **Foreign Agent (FA)** is a router in a foreign network to which the mobile node is currently connected. The packets from the home agent are sent to the foreign agent which delivers them to the mobile node.
7. **Correspondent Node (CN)** is a device on the internet communicating to the mobile node.
8. **Care-of Address (COA)** is the temporary address used by a mobile node while it is moving away from its home network.
9. **Foreign agent COA,** the COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as a common COA.
10. **Co-located COA,** the COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.



Working of Mobile IP

The mobile IP process has following three main phases, which are:

1. **Agent Discovery:** Agents advertise their presence by periodically broadcasting their agent advertisement messages. The mobile node receiving the agent advertisement messages observes whether the message is from its own home agent and determines whether it is in the home network or foreign network.

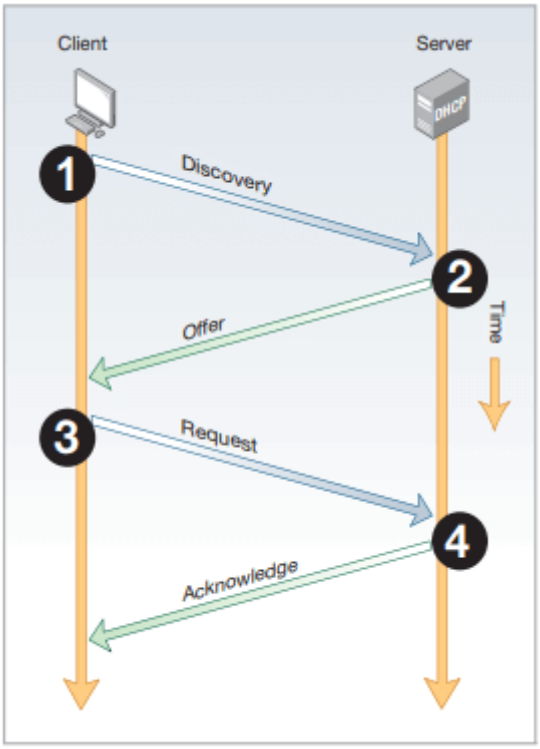
2. **Agent Registration:** Mobile node after discovering the foreign agent sends a registration request (RREQ) to the foreign agent. The foreign agent, in turn, sends the registration request to the home agent with the care-of-address. The home agent sends a registration reply (RREP) to the foreign agent. Then it forwards the registration reply to the mobile node and completes the process of registration.

3. **Tunneling:** It establishes a virtual pipe for the packets available between a tunnel entry and an endpoint. It is the process of sending a packet via a tunnel and it is achieved by a mechanism called encapsulation. It takes place to forward an IP datagram from the home agent to the care-of-address. Whenever the home agent receives a packet from the correspondent node, it encapsulates the packet with source address as home address and destination as care-of-address.

**Dynamic Host Configuration Protocol (DHCP)

DHCP stands for Dynamic Host Configuration Protocol. It is the critical feature on which the users of an enterprise network communicate. DHCP helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as desktops, laptops, cell phones, etc.

DHCP is based on a client-server model and based on discovery, offer, request, and ACK.



WORKING OF DHCP:

DHCP runs at the application layer of the TCP/IP protocol stack to dynamically assign IP addresses to DHCP clients/nodes and to allocate TCP/IP configuration information to the DHCP clients. Information includes subnet mask information, default gateway, IP addresses and domain name system addresses.

- First of all, a client (network device) must be connected to the internet.
- DHCP clients request an IP address. Typically, client broadcasts a query for this information.
- DHCP server responds to the client request by providing IP server address and other configuration information. This configuration information also includes time period, called a lease, for which the allocation is valid.
- When refreshing an assignment, a DHCP clients request the same parameters, but the DHCP server may assign a new IP address. This is based on the policies set by the administrator.

Components of DHCP

The main components of DHCP include:

- **DHCP Server:** DHCP Server is basically a server that holds IP Addresses and other information related to configuration.
- **DHCP Client:** It is basically a device that receives configuration information from the server. It can be a mobile, laptop, computer, or any other electronic device that requires a connection.
- **DHCP Relay:** DHCP relays basically work as a communication channel between DHCP Client and Server.
- **IP Address Pool:** It is the pool or container of IP Addresses possessed by the DHCP Server. It has a range of addresses that can be allocated to devices.
- **Subnets:** Subnets are smaller portions of the IP network partitioned to keep networks under control.
- **Lease:** It is simply the time that how long the information received from the server is valid, in case of expiration of the lease, the tenant must have to re-assign the lease.

**MOBILE TRANSPORT LAYER:

The mobile transport layer is a component of the network stack in mobile devices that provides communication services for applications running on the device. It is responsible for ensuring reliable and efficient transmission of data between applications on the device and the network.

The mobile transport layer uses various protocols such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to provide reliable and efficient data transfer. TCP is a connection-oriented protocol that ensures reliable data transfer by establishing a virtual connection between the sender and receiver, while UDP is a connectionless protocol that provides a faster data transfer but does not guarantee reliability.

**Traditional TCP:

Transmission Control Protocol (TCP) is the transport layer protocol that serves as an interface between client and server. The TCP/IP protocol is used to transfer the data packets between transport layer and network layer. Transport protocol is mainly designed for fixed end systems and fixed, wired

networks. In simple terms, the traditional TCP is defined as a wired network while classical TCP uses wireless approach. Mainly TCP is designed for fixed networks and fixed, wired networks.

The main research activities in TCP are as listed below.

Congestion control

- TCP has been designed for fixed networks with fixed end-systems
- Hardware and software are mature enough to ensure reliability of data
- The probable reason for a packet loss in a fixed network is a temporaryoverloadsome point in the transmission path, i.e., a state of congestion at a node
- The packet buffers of a router are filled and the router cannot forward the packetsfast enough
- The only thing a router can do in this situation is to drop packets
- The sender notices the missing acknowledgement for the lost packet and assumes apacket loss due to congestion
- Retransmitting the missing packet and continuing at full sending rate would now beunwise, as this might only increase the congestion.

Slow start

- The behavior TCP shows after the detection of congestion is called slow start
- The sender always calculates a congestion window for a receiver.
- The start size of the congestion window is one segment (TCP packet).
- This scheme doubles the congestion window every time the acknowledgementscome back, which takes one round trip time (RTT) like 1, 2, 4, 8 etc.
- This is called the exponential growth of the congestion window in the slow startmechanism.
- The exponential growth stops at the congestion threshold.
- As soon as the congestion window reaches the congestion threshold, further increase of the transmission rate is only linear by adding 1 to the congestion window each time the acknowledgements come back
- Linear increase continues until a time-out at the sender occurs due to a missingacknowledgement, or until the sender detects a gap in transmitted data

- the sender sets the congestion threshold to half of the current congestion window
- The congestion window itself is set to one segment

Fast retransmit/fast recovery

Fast Retransmit

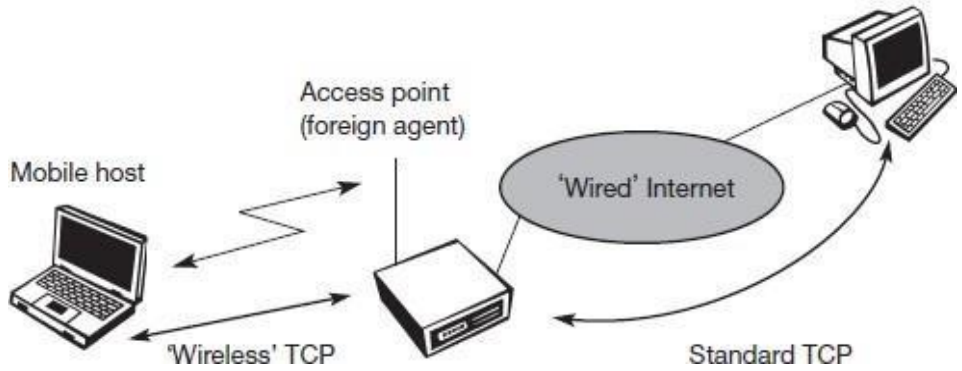
- a receiver sends acknowledgements only if it receives any packets from the sender.
- Receiving acknowledgements from a receiver also shows that the receivercontinuously receives something from the sender.
- The gap in the packet stream is not due to severe congestion, but asimple packet loss due to a transmission error.
- The sender can now retransmit the missing packet(s) before the timer expires.
- This behavior is called fast retransmit

Fast Recovery

- The receipt of acknowledgements shows that there is no congestion to justify a slowstart.
- The sender can continue with the current congestion window.
- The sender performs a fast recovery from the packet loss
- This mechanism can improve the efficiency of TCP dramatically

****INDIRECT TCP:**

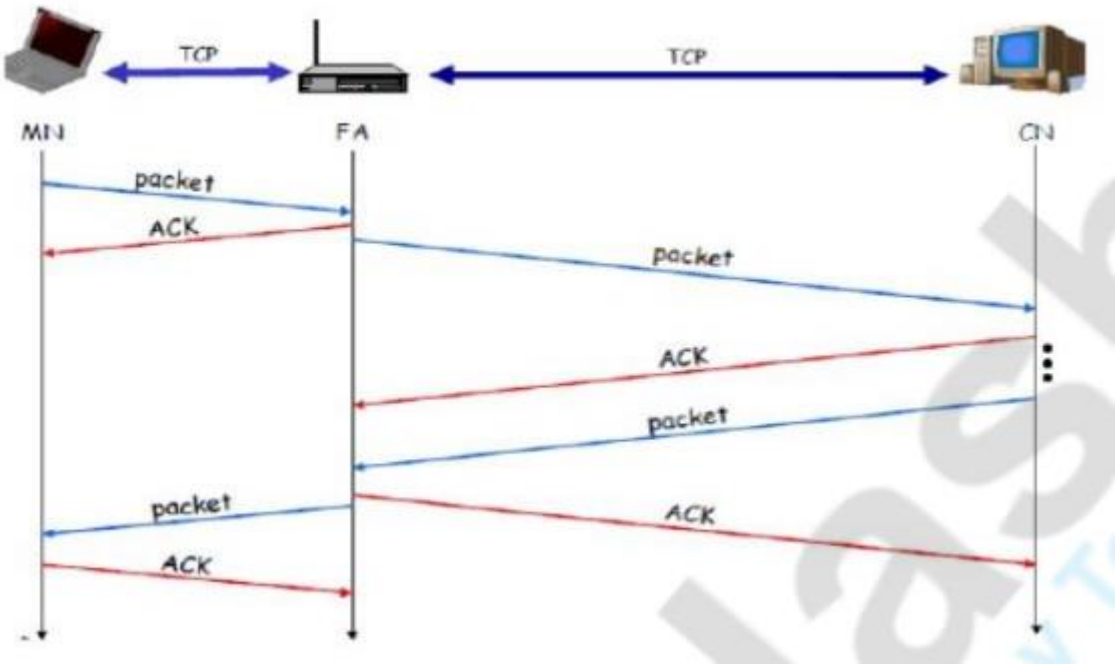
Indirect TCP Two competing insights led to the development of indirect TCP (I-TCP). One is that TCP performs poorly together with wireless links; the other is that TCP within the fixed network cannot be changed. I-TCP segments a TCP connection into a fixed part and a wireless part.



WORKING:

- A good place for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP.

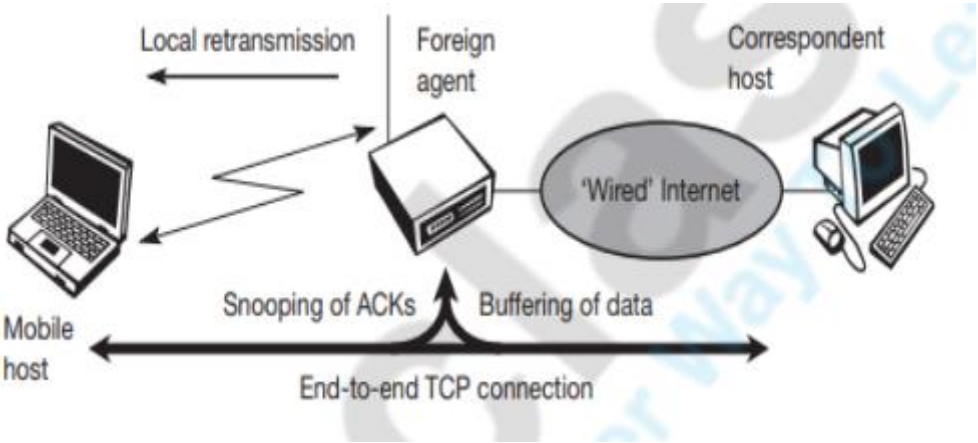
- The foreign agent controls the mobility of the mobile host anyway and can also
- hand over the connection to the next foreign agent when the mobile host moves
- on.
- The foreign agent acts as a proxy and relays all data in both directions.
- If the correspondent host sends a packet, the foreign agent acknowledges this packet and tries to forward the packet to the mobile host.
- If the mobile host receives the packet, it acknowledges the packet.
- However, this acknowledgement is only used by the foreign agent.
- If a packet is lost on the wireless link due to a transmission error, the correspondent host would not notice this.
- In this case, the foreign agent tries to retransmit this packet locally to maintain reliable data transport.
- Similarly, if the mobile host sends a packet, the foreign agent acknowledges this packet and tries to forward it to the correspondent host.
- If the packet is lost on the wireless link, the mobile hosts notice this much faster due to the lower round trip time and can directly retransmit the packet.
- Packet loss in the wired network is now handled by the foreign agent.
- During handover, the buffered packets, as well as the system state (packet sequence number, acknowledgements, ports, etc.), must migrate to the new agent.
- No new connection may be established for the mobile host, and the correspondent host must not see any changes in connection state.



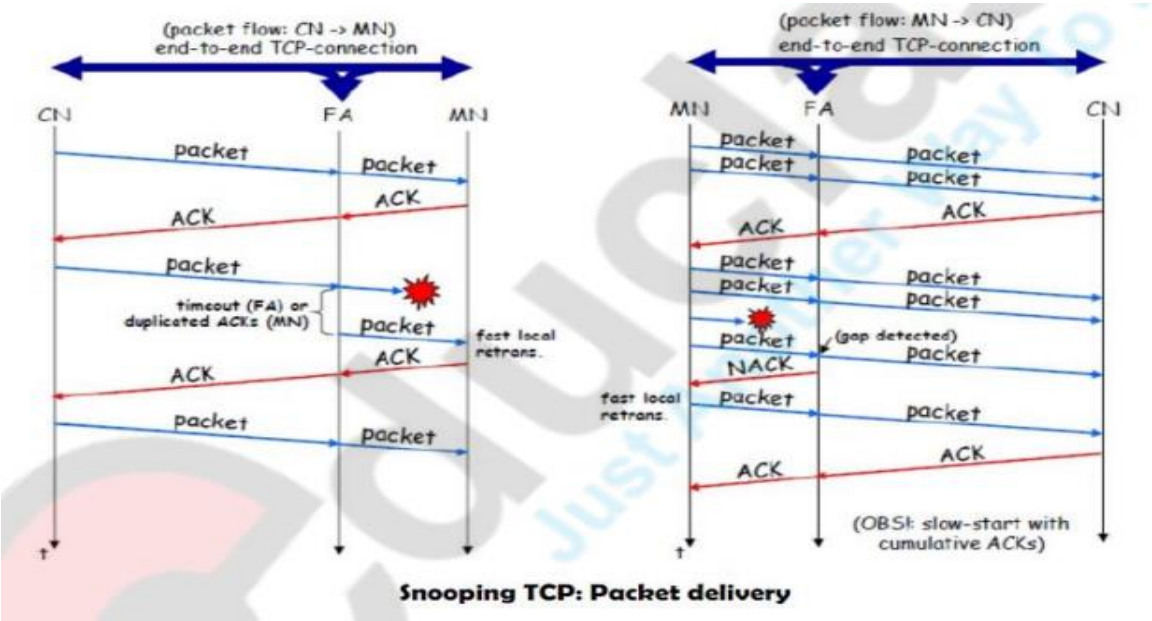
**Snooping TCP:

- The main drawbacks of I-TCP is the segmentation of the single TCP connection into two TCP connections. This loses the original end-to-end TCP semantic.
- A new TCP enhancement, which leaves the TCP end-to-end connection intact and is completely transparent, is Snooping TCP.
- The main function of the enhancement is to buffer data close to the mobile host to perform fast local retransmission in case of packet loss.

- A good place for the enhancement of TCP could be the foreign agent in the Mobile IP context.



- In this approach, the foreign agent buffers all packets with destination mobile host and additionally 'snoops' the packet flow in both directions to recognize acknowledgements.
- The foreign agent buffers every packet until it receives an acknowledgement from the mobile host.
- If the foreign agent does not receive an acknowledgement from the mobile host within a certain amount of time, either the packet or the acknowledgement has been lost.
- Alternatively, the foreign agent could receive a duplicate ACK which also shows the loss of a packet.
- Now the foreign agent retransmits the packet directly from the buffer, performing a much faster retransmission compared to the correspondent host.
- For transparency, the foreign agent does not acknowledge data to the correspondent host which would violate end-to-end semantic in case of a FA failure.
- However, the foreign agent can filter the duplicate acknowledgements to avoid unnecessary retransmissions of data from the correspondent host.
- If the foreign agent now crashes, the time-out of the correspondent host still works and triggers a retransmission.

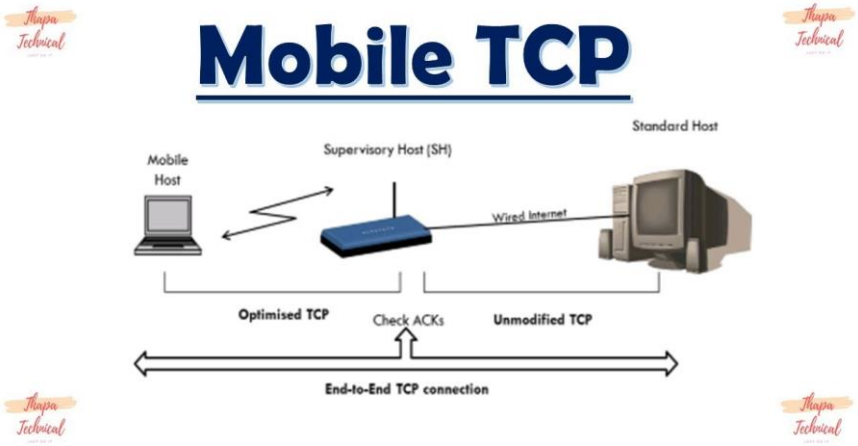


Snooping TCP: Packet delivery

- The foreign agent may discard duplicates of packets already retransmitted locally and acknowledged by the mobile host. This avoids unnecessary traffic on the wireless link.
- Data transfer from the mobile host with destination correspondent host works as follows.
- The foreign agent snoops into the packet stream to detect gaps in the sequence numbers of TCP.
- As soon as the foreign agent detects a missing packet, it returns a negative acknowledgement (NACK) to the mobile host.
- The mobile host can now retransmit the missing packet immediately. Reordering of packets is done automatically at the correspondent host by TCP.

**Mobile TCP:

- Both I-TCP and Snooping TCP does not help much, if a mobile hosts get disconnected.
- The M-TCP (mobile TCP) approach has the same goals as I-TCP and snooping TCP: to prevent the sender window from shrinking if bit errors or disconnection but not congestion cause current problems.
- M-TCP wants to improve overall throughput, to lower the delay, to maintain end-to-end semantics of TCP, and to provide a more efficient handover.



- Additionally, M-TCP is especially adapted to the problems arising from lengthy or frequent disconnections.
- M-TCP splits the TCP connection into two parts as I-TCP does.
- An unmodified TCP is used on the standard host-supervisory host (SH) connection, while an optimized TCP is used on the SH-MH connection.
- The supervisory host is responsible for exchanging data between both parts similar to the proxy in ITCP.
- The M-TCP approach assumes a relatively low bit error rate on the wireless link.
- Therefore, it does not perform caching/retransmission of data via the SH.
- If a packet is lost on the wireless link, it has to be retransmitted by the original sender. This maintains the TCP end-to-end semantics.
- The SH monitors all packets sent to the MH and ACKs returned from the MH.
- If the SH does not receive an ACK for some time, it assumes that the MH is disconnected.
- It then chokes the sender by setting the sender's window size to 0.
- Setting the window size to 0 forces the sender to go into persistent mode, i.e., the state of the sender will not change no matter how long the receiver is disconnected.
- This means that the sender will not try to retransmit data.
- As soon as the SH (either the old SH or a new SH) detects connectivity again, it reopens the window of the sender to the old value.
- The sender can continue sending at full speed. This mechanism does not require changes to

the sender's TCP.

- The wireless side uses an adapted TCP that can recover from packet loss much faster.
- This modified TCP does not use slow start, thus, M-TCP needs a bandwidth manager to implement fair sharing over the wireless link

**Fast retransmit/fast recovery:

- The congestion threshold can be reduced because of two reasons.
- First one is if the sender receives continuous acknowledgements for the same packet.
- It informs the sender that the receiver has got all the packets upto the acknowledged packet in the sequence and also the receiver is receiving something continuously from the sender.
- The gap in the packet stream is not due to congestion, but a simple packet loss due to a transmission error.
- The sender can now retransmit the missing packet(s) before the timer expires. This behavior is called fast retransmit.
- It is an early enhancement for preventing slow-start to trigger on losses not caused by congestion.
- The receipt of acknowledgements shows that there is no congestion to justify a slow start.
- The sender can continue with the current congestion window. The sender performs a fast recovery from the packet loss.
- This mechanism can improve the efficiency of TCP dramatically.
- The other reason for activating slow start is a time-out due to a missing acknowledgement.
- TCP using fast retransmit/fast recovery interprets this congestion in the network and activates the slow start mechanism.
- The advantage of this approach is its simplicity. Only minor changes in the mobile host's software result in a performance increase. No changes are required in foreign agent or correspondent host.
- The main disadvantage of this scheme is the insufficient isolation of packet losses. This approach mainly focuses on loss due to handover. Also it effects the efficiency when a CH transmits already delivered packets.

**Transmission/time-out freezing :

- Quite often, the MAC layer has noticed connection problems, before the connection is actually interrupted from a TCP point of view.
- Additionally, the MAC layer knows the real reason for the interruption and does not assume congestion, as TCP would.
- The MAC layer can inform the TCP layer of an upcoming loss of connection or that the current interruption is not caused by congestion.
- TCP can now stop sending and 'freezes' the current state of its congestion window and further timers.
- If the MAC layer notices the upcoming interruption early enough, both the mobile and correspondent host can be informed.
- With a fast interruption of the wireless link, additional mechanisms in the access point are needed to inform the correspondent host of the reason for interruption.
- Otherwise, the correspondent host goes into slow start assuming congestion and finally breaks the connection.
- As soon as the MAC layer detects connectivity again, it signals TCP that it can resume operation at exactly the same point where it had been forced to stop.
- For TCP time simply does not advance, so no timers expire.
- The advantage of this approach is that it offers a way to resume TCP connections even after

longer interruptions of the connection.

- It is independent of any other TCP mechanism, such as acknowledgements or sequence numbers, so it can be used together with encrypted data.
- However, this scheme has some severe disadvantages.
- Lots of changes have to be made in software of MH, CH and FA. Freezing the state of TCP does not help in case of some encryption schemes that use time-dependent random numbers. These schemes need resynchronization after interruption.

**Selective retransmission:

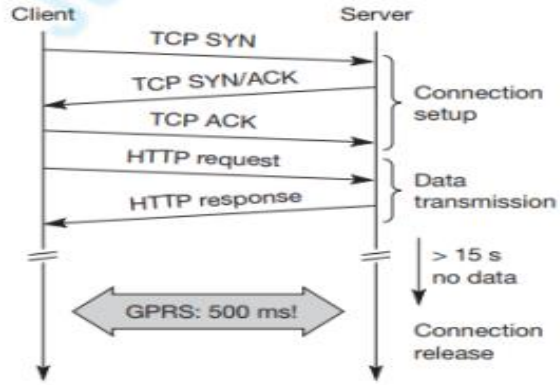
- A very useful extension of TCP is the use of selective retransmission.
- TCP acknowledgements are cumulative, i.e., they acknowledge in-order receipt of packets up to a certain packet.
- If a single packet is lost, the sender has to retransmit everything starting from the lost packet (go-back-n retransmission).
- This obviously wastes bandwidth, not just in the case of a mobile network, but for any network.
- Using RFC 2018, TCP can indirectly request a selective retransmission of packets.
- The receiver can acknowledge single packets, not only trains of in-sequence packets.
- The sender can now determine precisely which packet is needed and can retransmit it.
- The advantage of this approach is obvious: a sender retransmits only the lost packets.
- This lowers bandwidth requirements and is extremely helpful in slow wireless links.
- The gain in efficiency is not restricted to wireless links and mobile environments.
- Using selective retransmission is also beneficial in all other networks.
- However, there might be the minor disadvantage of more complex software on the receiver side, because now more buffer is necessary to resequence data and to wait for gaps to be filled.
- But while memory sizes and CPU performance permanently increase, the bandwidth of the air interface remains almost the same.
- Therefore, the higher complexity is no real disadvantage any longer as it was in the early days of TCP.

**Transaction-oriented TCP:

- Assume an application running on the mobile host that sends a short request to a server from time to time, which responds with a short message.
- If the application requires reliable transport of the packets, it may use TCP (many applications of this kind use UDP and solve reliability on a higher, application oriented layer).
- Using TCP now requires several packets over the wireless link.
- First, TCP uses a three-way handshake to establish the connection.
- At least one additional packet is usually needed for transmission of the request, and requires three more packets to close the connection via a three-way handshake.
- Assuming connections with a lot of traffic or with a long duration, this overhead is minimal.
- But in an example of only one data packet, TCP may need seven packets altogether.
- Figure 9.4 shows an example for the overhead introduced by using TCP over GPRS in a web scenario.
- Web services are based on HTTP which requires a reliable transport system.

- In the internet, TCP is used for this purpose. Before a HTTP request can be transmitted the TCP connection has to be established. This already requires three messages.
- If GPRS is used as wide area transport system, one-way delays of 500 ms and more are quite common. The setup of a TCP connection already takes far more than a second.
- This led to the development of a transaction-oriented TCP.

Figure 9.4
Example TCP connection setup overhead



- T/TCP can combine packets for connection establishment and connection release with user data packets.
- This can reduce the number of packets down to two instead of seven.
- The obvious advantage for certain applications is the reduction in the overhead which standard TCP has for connection setup and connection release.
- Disadvantage is that it requires changes in the software in mobile host and all correspondent hosts. • This solution does not hide mobility anymore.
- Also, T/TCP exhibits several security problems