Mobile IP

This is an **IETF (Internet Engineering Task Force)** standard communications protocol designed to allow mobile devices' (such as laptop, PDA, mobile phone, etc.) users to move from one network to another while maintaining their permanent IP (Internet Protocol) address.

Defined in RFC (Request for Comments) 2002, mobile IP is an enhancement of the internet protocol (IP) that adds mechanisms for forwarding internet traffic to mobile devices (known as mobile nodes) when they are connecting through other than their home network.

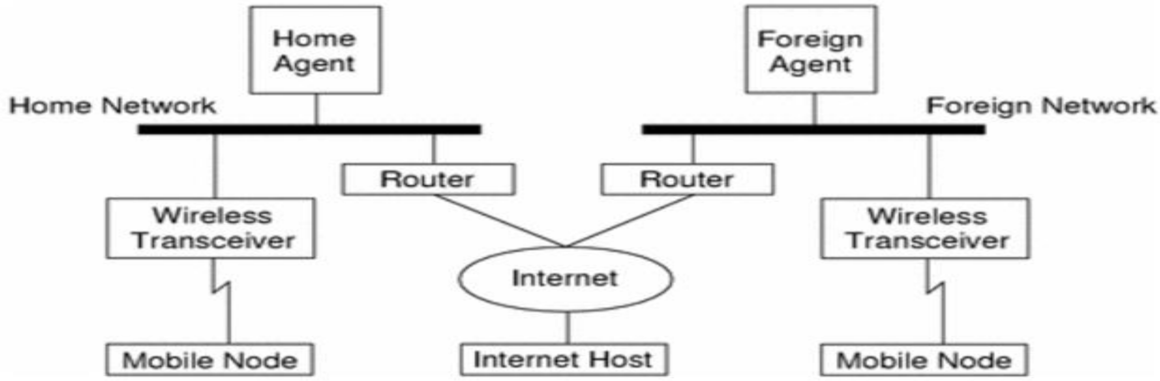


Fig: Mobile IP topology

The following case shows how a datagram moves from one point to another within the Mobile IP framework.

- First of all, the internet host sends a datagram to the mobile node using the mobile node's home address (normal IP routing process).
- If the mobile node (MN) is on its home network, the datagram is delivered through the normal IP (Internet Protocol) process to the mobile node. Otherwise the home agent picks up the datagram.
- If the mobile node (MN) is on foreign network, the home agent (HA) forwards the datagram to the foreign agent.
- The foreign agent (FA) delivers the datagram to the mobile node.
- Datagrams from the MN to the Internet host are sent using normal IP routing procedures. If the mobile node is on a foreign network, the packets are delivered to the foreign agent. The FA forwards the datagram to the Internet host.

In the case of wireless communications, the above illustrations depict the use of wireless transceivers to transmit the datagrams to the mobile node. Also, all datagrams between the Internet host and the MN use the mobile node's home address regardless of whether the mobile node is on a home or foreign network. The care-of address (COA) is used only for communication with mobility agents and is never seen by the Internet host.

Components of Mobile IP

The mobile IP has following three components as follows:

1. Mobile Node (MN)

The mobile node is an end system or device such as a cell phone, PDA (Personal Digital assistant), or laptop whose software enables network roaming capabilities.

2. Home Agent (HA)

The home agent provides several services for the mobile node and is located in the home network. The tunnel for packets towards the mobile node starts at home agent. The home agent maintains a location registry, i.e. it is informed of the mobile node's location by the current COA (care of address). Following alternatives for the implementation of an HA exist.

- Home agent can be implemented on a **router** that is responsible for the home network. This is obviously the best position, because without optimization to mobile IP, all packets for the MN have to go through the router anyway.
- If changing the router's software is not possible, the home agent could also be implemented on an **arbitrary node** in the subset. One biggest disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the mobile node comes in via the router; the HA sends it through the tunnel which again crosses the router.

3. Foreign Agent (FA)

The foreign agent can provide several services to the mobile node during its visit to the foreign network. The FA can have the COA (care or address) acting as a tunnel endpoint and forwarding packets to the MN. The foreign agent can be the default router for the MN.

Foreign agent can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting.

In short, FA is a router that may function as the point of attachment for the mobile node when it roams to a foreign network delivers packets from the home agent to the mobile node.

4. Care of Address (COA)

The Care- of- address defines the current location of the mobile node from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the mobile node is done using a tunnel. To be more precise, the COA marks the endpoint of the tunnel, i.e. the address where packets exit the tunnel.

There are two different possibilities for the location of the care of address:

1. **Foreign Agent COA:** The COA could be located at the foreign agent, i.e. the COA is an IP address of the foreign agent. The foreign agent is the tunnel endpoint and forwards packets to the MN. Many MN using the FA can share this COA as common COA.
2. **Co-located COA:** The COA is co-located if the MN temporarily acquired an additional IP address which acts as a COA. This address is now topologically correct, and the tunnel endpoint is at the mobile node. Co-located address can be acquired using services such as DHCP. One problem associated with this approach is need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

5. Correspondent Node (CN)

At least one partner is needed for communication. The correspondent node represents this partner for the MN. The correspondent node can be a fixed or mobile node.

6. Home Network

The home network is the subset the MN belongs to with respect to its IP address. No mobile IP support is needed within this network.

7. Foreign network

The foreign network is the current subset the MN visits and which is not the home network.

Process of Mobile IP

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

1. Agent Discovery

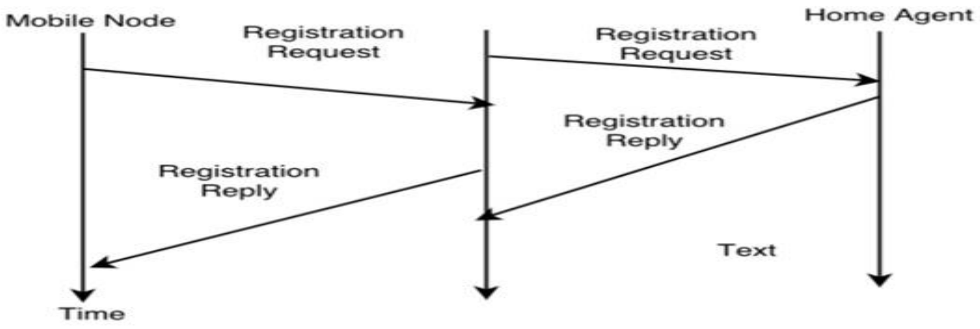
During the agent discovery phase the HA and FA advertise their services on the network by using the ICMP router discovery protocol (IROP).

Mobile IP defines two methods: agent advertisement and agent solicitation which are in fact router discovery methods plus extensions.

- **Agent advertisement:** For the first method, FA and HA advertise their presence periodically using special agent advertisement messages. These messages advertisement can be seen as a beacon broadcast into the subnet. For this advertisement internet control message protocol (ICMP) messages according to RFC 1256, are used with some mobility extensions.
- **Agent solicitation:** If no agent advertisements are present or the inter arrival time is too high, and an MN has not received a COA, the mobile node must send agent solicitations. These solicitations are again bases on RFC 1256 for router solicitations.

2. Registration

The main purpose of the registration is to inform the home agent of the current location for correct forwarding of packets.



Registration can be done in two ways depending on the location of the COA.

- **If the COA is at the FA**, the MN sends its registration request containing the COA to the FA which is forwarding the request to the HA. The HA now set up a **mobility binding** containing the mobile node's home IP address and the current COA.

Additionally, the mobility biding contains the lifetime of the registration which is negotiated during the registration process. Registration expires automatically after the lifetime and is deleted; so a mobile node should register before expiration. After setting up the mobility binding, the HA send a reply message back to the FA which forwards it to the MN.

- **If the COA is co-located**, registration can be very simpler. The mobile node may send the request directly to the HA and vice versa. This by the way is also the registration procedure for MNs returning to their home network.

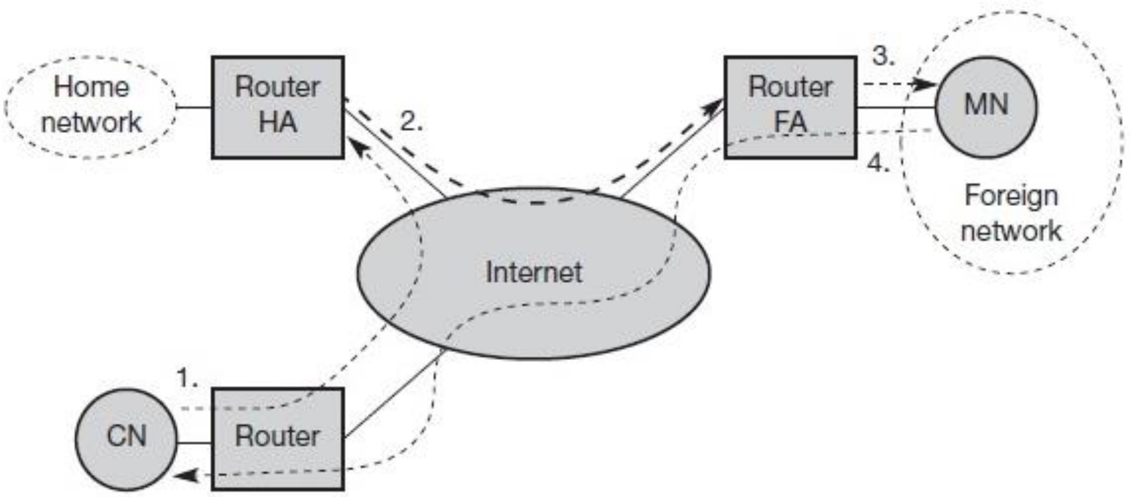
3. Tunneling

A tunnel is used to establish a virtual pipe for data packets between a tunnel entry and a tunnel endpoint. Packets which are entering in a tunnel are forwarded inside the tunnel and leave the tunnel unchanged. Tunneling, i.e., sending a packet through a tunnel is achieved with the help of encapsulation.

Tunneling is also known as "**port forwarding**" is the transmission and data intended for use only within a private, usually corporate network through a public network.

Packet Delivery

The mobile i.e movement of MN from one location to another has to be hidden as per the requirement of mobile IP. CN may not know the exact location of MN



STEP 1: CN sends the packet as usual to the IP address of MN. With Source address as CN and Destination address as MN .The internet, which does not have any information of the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet.

STEP 2: The HA now diverts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet.

STEP 3: The foreign agent (FA) now decapsulates the packet, i.e., removes the additional header(newly added as COA as destination and HA as source), and forwards the original packet with CN as source and MN as destination to the MN. Again, for the MN mobility is not visible.

Finally the MN Receives the packet with the Source address as CN and Destination address as MN.

STEP 4: The MN sends the packet MN as Source Address and CN as Destination Address. The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. Simple mechanism works if CN is Fixed at a location if it has got mobility then the above Steps 1 to 3 are to be followed to deliver the packet from MN to CN.

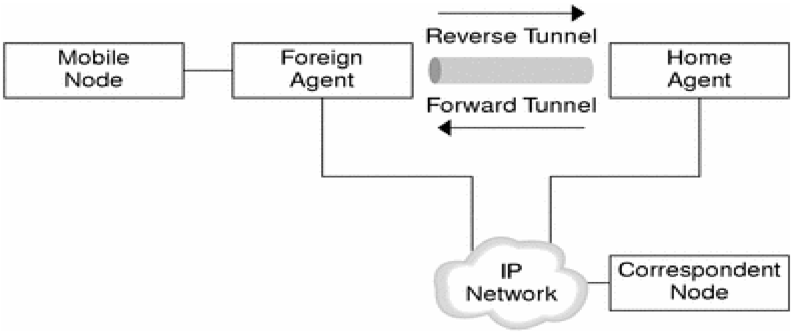
Route Optimization in Mobile IP:
The route optimization adds a conceptual data structure, the binding cache, to the correspondent node.

The binding cache contains bindings for mobile node’s home address and its current care-of-address. Every time the home agent receives a IP datagram that is destined to a mobile node currently away from the home network, it sends a binding update to the correspondent node to update the information in the correspondent node’s binding cache. After this the correspondent node can directly tunnel packets to the mobile node.

Mobile IP With Reverse Tunneling

The previous description of Mobile IP assumes that the routing within the Internet is independent of the data packet's source address. However, intermediate routers might check for a topologically correct source address. If an intermediate router does check, you should set up a reverse tunnel. By setting up a reverse tunnel from the mobile node's care-of address to the home agent, you ensure a topologically correct source address for the IP data packet. A mobile node can request a **reverse tunnel** between its foreign agent and its home agent when the mobile node registers. A reverse tunnel is a tunnel that starts at the mobile node's care-of address and terminates at the home agent. The following illustration shows the Mobile IP topology that uses a reverse tunnel.

Figure 1–4 Mobile IP With a Reverse Tunnel



Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to dynamically assign an IP address to nay device, or node, on a network so they can communicate using IP (Internet Protocol). DHCP automates and centrally manages these configurations. There is no need to manually assign IP addresses to new devices. Therefore, there is no requirement for any user configuration to connect to a DHCP based network.

DHCP can be implemented on local networks as well as large enterprise networks. DHCP is the default protocol used by the most routers and networking equipment. DHCP is also called RFC (Request for comments) 2131.

DHCP does the following:

- DHCP manages the provision of all the nodes or devices added or dropped from the network.
- DHCP maintains the unique IP address of the host using a DHCP server.
- It sends a request to the DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to a network. The server acknowledges by providing an IP address to the client/node/device.

DHCP is also used to configure the proper subnet mask, default gateway and DNS server information on the node or device.

There are many versions of DCHP are available for use in IPV4 (Internet Protocol Version 4) and IPV6 (Internet Protocol Version 6).

How DHCP works

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.

DHCP is based on client-server protocol in which servers manage a pool of unique IP addresses, as well as information about client configuration parameters, and assign addresses out of those address pools.

The DHCP lease process works as follows:

- 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

When working with DHCP, it is important to understand all of the components. Following are the list of components:

- **DHCP Server:** DHCP server is a networked device running the DCHP service that holds IP addresses and related configuration information. This is typically a server or a router but could be anything that acts as a host, such as an SD-WAN appliance.
- **DHCP client:** DHCP client is the endpoint that receives configuration information from a DHCP server. This can be any device like computer, laptop, IoT endpoint or anything else that requires connectivity to the network. Most of the devices are configured to receive DHCP information by default.
- **IP address pool:** IP address pool is the range of addresses that are available to DHCP clients. IP addresses are typically handed out sequentially from lowest to the highest.
- **Subnet:** Subnet is the partitioned segments of the IP networks. Subnet is used to keep networks manageable.
- **Lease:** Lease is the length of time for which a DHCP client holds the IP address information. When a lease expires, the client has to renew it.
- **DHCP relay:** A host or router that listens for client messages being broadcast on that network and then forwards them to a configured server. The server then sends responses back to the relay agent that passes them along to the client. DHCP relay can be used to centralize DHCP servers instead of having a server on each subnet.

Benefits of DHCP

There are following benefits of DHCP:

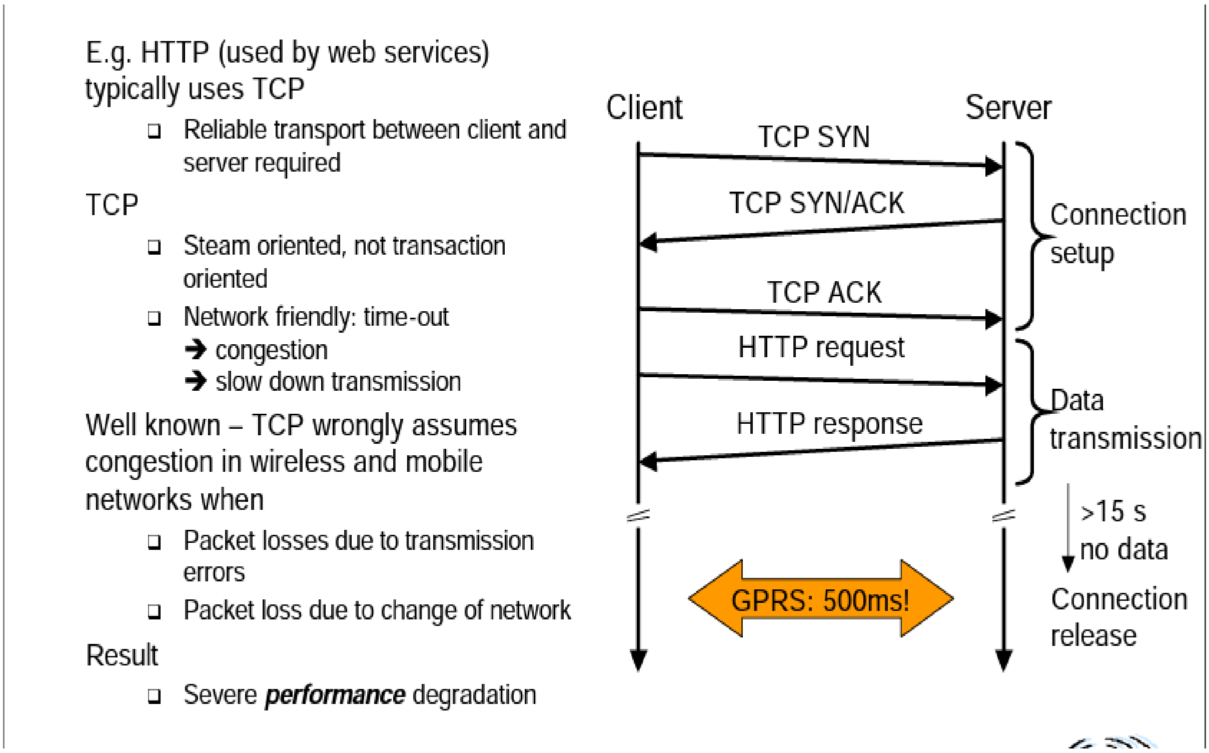
Centralized administration of IP configuration: DHCP IP configuration information can be stored in a single location and enables that administrator to centrally manage all IP address configuration information.

Dynamic host configuration: DHCP automates the host configuration process and eliminates the need to manually configure individual host. When TCP/IP (Transmission control protocol/Internet protocol) is first deployed or when IP infrastructure changes are required.

Seamless IP host configuration: The use of DHCP ensures that DHCP clients get accurate and timely IP configuration IP configuration parameter such as IP address, subnet mask, default gateway, IP address of DND server and so on without user intervention.

Flexibility and scalability: Using DHCP gives the administrator increased flexibility, allowing the administrator to move easily change IP configuration when the infrastructure changes.

Transport Layer



E.g. HTTP (used by web services) typically uses TCP

- ❑ Reliable transport between client and server required

TCP

- ❑ Steam oriented, not transaction oriented
- ❑ Network friendly: time-out
  ➔ congestion
  ➔ slow down transmission

Well known – TCP wrongly assumes congestion in wireless and mobile networks when

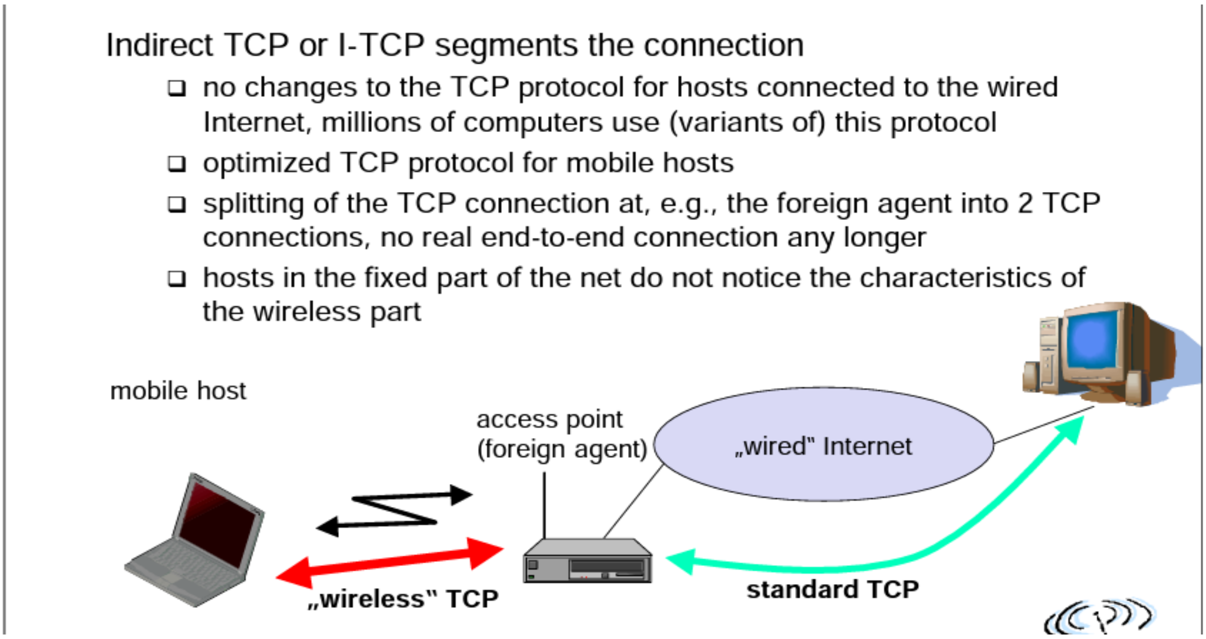
- ❑ Packet losses due to transmission errors
- ❑ Packet loss due to change of network

Result

- ❑ Severe ***performance*** degradation

- Transport protocols typically designed for
  - Fixed end-systems
  - Fixed, wired networks
- Research activities
  - How to improve TCP performance in wireless networks
  - Maintain congestion control behavior
  - Efficient retransmissions
- TCP congestion control in fixed networks
  - Timeouts/Packet loss typically due to (temporary) overload
  - Routers discard packets when buffers are full
  - TCP recognizes congestion only indirectly via missing ACKs, retransmissions unwise, since they increase congestion
  - slow-start algorithm as reaction

Indirect TCP



Indirect TCP or I-TCP segments the connection

- ❑ no changes to the TCP protocol for hosts connected to the wired Internet, millions of computers use (variants of) this protocol
- ❑ optimized TCP protocol for mobile hosts
- ❑ splitting of the TCP connection at, e.g., the foreign agent into 2 TCP connections, no real end-to-end connection any longer
- ❑ hosts in the fixed part of the net do not notice the characteristics of the wireless part

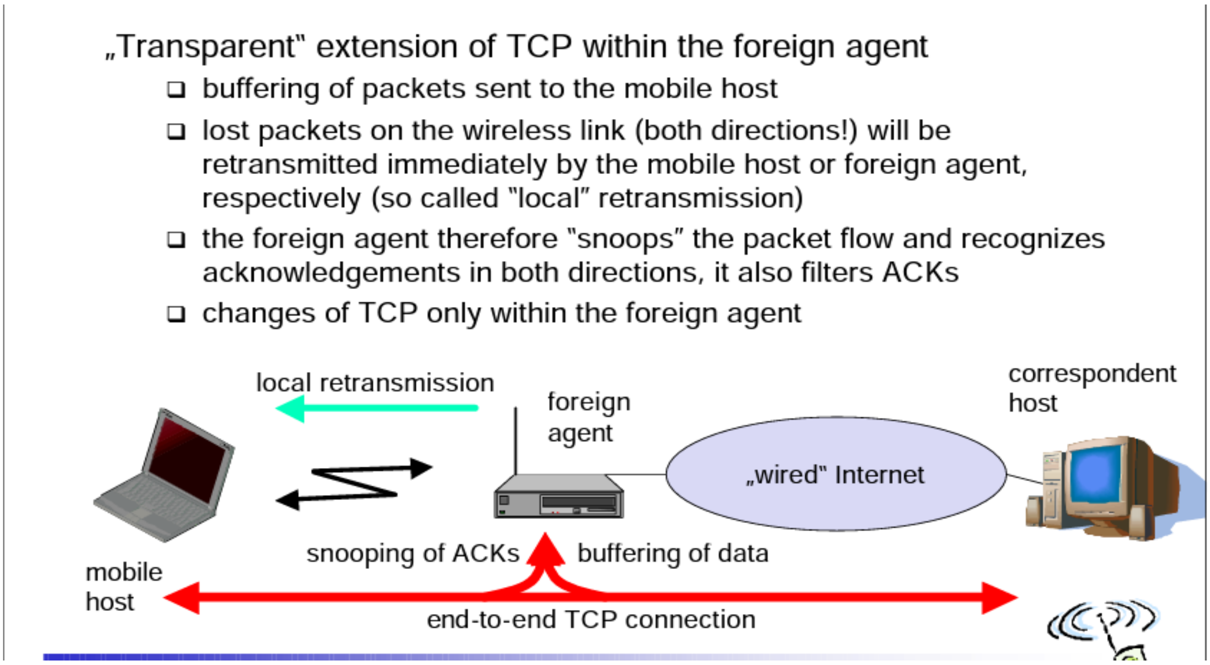
Advantages:

- No changes in the fixed network necessary, no changes for the hosts (TCP protocol) necessary, all current optimizations to TCP still work
- Wireless link transmission errors isolated from those in fixed network
- simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host
- therefore, a very fast retransmission of packets is possible, the short delay on the mobile hop is known

Disadvantages:

- loss of end-to-end semantics, an acknowledgement to a sender does now not any longer mean that a receiver really got a packet, foreign agents might crash
- higher latency possible due to buffering of data within the foreign agent and forwarding to a new foreign agent

Snooping TCP



„Transparent" extension of TCP within the foreign agent

- ❑ buffering of packets sent to the mobile host
- ❑ lost packets on the wireless link (both directions!) will be retransmitted immediately by the mobile host or foreign agent, respectively (so called "local" retransmission)
- ❑ the foreign agent therefore "snoops" the packet flow and recognizes acknowledgements in both directions, it also filters ACKs
- ❑ changes of TCP only within the foreign agent

Data transfer to the mobile host

- FA buffers data until it receives ACK of the MH, FA detects packet loss via duplicated ACKs or time-out
- fast retransmission possible, transparent for the fixed network

Data transfer from the mobile host

- FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a NACK to the MH
- MH can now retransmit data with only a very short delay

Integration with MAC layer

- MAC layer often has similar mechanisms to those of TCP
- thus, the MAC layer can already detect duplicated packets due to retransmissions and discard them

Problems

- snooping TCP does not isolate the wireless link as good as I-TCP
- snooping might be tough if packets are encrypted

<u>Mobile TCP</u>

Special handling of lengthy and/or frequent disconnections M-TCP splits as I-TCP does

- unmodified TCP fixed network to supervisory host (SH)
- optimized TCP SH to MH

Supervisory host

- no caching, no retransmission
- monitors all packets, if disconnection detected
  - set sender window size to
  - sender automatically goes into persistent mode
- old or new SH reopen the window

Advantages:

- maintains semantics, supports disconnection, no buffer forwarding

Disadvantages:

- loss on wireless link propagated into fixed network
- adapted TCP on wireless link

<u>Fast retransmit/fast recovery</u>

Change of foreign agent often results in packet loss

- TCP reacts with slow-start although there is no congestion

Forced fast retransmit

- as soon as the mobile host has registered with a new foreign agent, the MH sends duplicated acknowledgements on purpose
- this forces the fast retransmit mode at the communication partners

- additionally, the TCP on the MH is forced to continue sending with the actual window size and not to go into slow-start after registration

Advantage

- simple changes result in significant higher performance

Disadvantage

- Cooperation required between IP and TCP, no transparent approach

Transmission/time-out freezing

Mobile hosts can be disconnected for a longer time

- no packet exchange possible, e.g., in a tunnel, disconnection due to overloaded cells or mux. with higher priority traffic
- TCP disconnects after time-out completely

TCP freezing

- MAC layer is often able to detect interruption in advance
- MAC can inform TCP layer of upcoming loss of connection
- TCP stops sending, but does now not assume a congested link
- MAC layer signals again if reconnected

Advantage:

- scheme is independent of data

Disadvantage:

- TCP on mobile host has to be changed, mechanism depends on MAC layer

Selective retransmission

TCP acknowledgements are often cumulative

- ACK n acknowledges correct and in-sequence receipt of packets up to n
- if single packets are missing quite often a whole packet sequence beginning at the gap has to be retransmitted (go-back-n), thus wasting bandwidth

Selective retransmission as one solution

- RFC2018 allows for acknowledgements of single packets, not only acknowledgements of in-sequence packet streams without gaps
- sender can now retransmit only the missing packets

Advantage:

- much higher efficiency

Disadvantage:

- more complex software in a receiver, more buffer needed at the receiver

Transaction oriented TCP

TCP phases

- connection setup, data transmission, connection release
- using 3-way-handshake needs 3 packets for setup and release, respectively
- thus, even short messages need a minimum of 7 packets!

Transaction oriented TCP

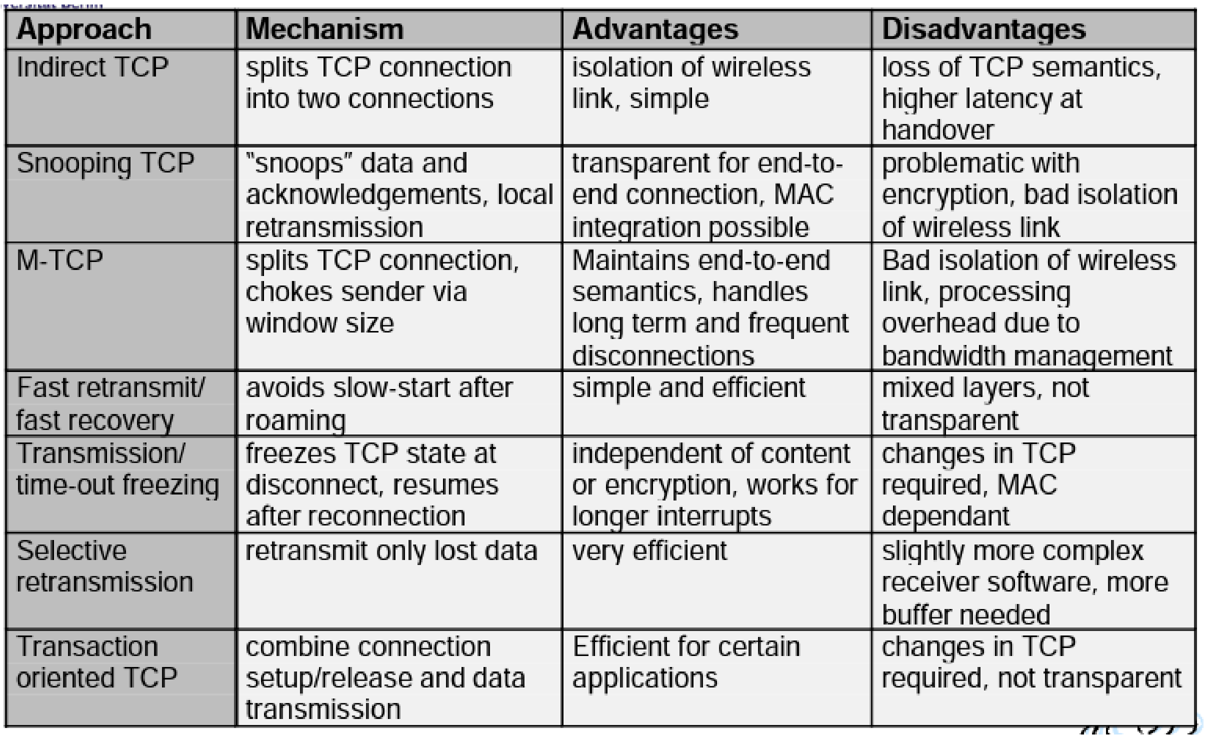
- RFC1644, T-TCP, describes a TCP version to avoid this overhead
- connection setup, data transfer and connection release can be combined
- thus, only 2 or 3 packets are needed

Advantage:

- efficiency

Disadvantage:

- requires changed TCP
- mobility not longer transparent



Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	isolation of wireless link, simple	loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data and acknowledgements, local retransmission	transparent for end-to-end connection, MAC integration possible	problematic with encryption, bad isolation of wireless link
M-TCP	splits TCP connection, chokes sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast retransmit/ fast recovery	avoids slow-start after roaming	simple and efficient	mixed layers, not transparent
Transmission/ time-out freezing	freezes TCP state at disconnect, resumes after reconnection	independent of content or encryption, works for longer interrupts	changes in TCP required, MAC dependant
Selective retransmission	retransmit only lost data	very efficient	slightly more complex receiver software, more buffer needed
Transaction oriented TCP	combine connection setup/release and data transmission	Efficient for certain applications	changes in TCP required, not transparent