Module – 4

Wireless and Mobile Network

Cellular Internet Access

- Cellular telephony is now ubiquitous in many areas throughout the world as it support not only voice telephony but wireless Internet access as well.
- Ideally, this Internet access would be at a reasonably high speed and would provide for seamless mobility, allowing users to maintain their TCP sessions while traveling, for example, on a bus or a train.

An Overview of Cellular Network Architecture

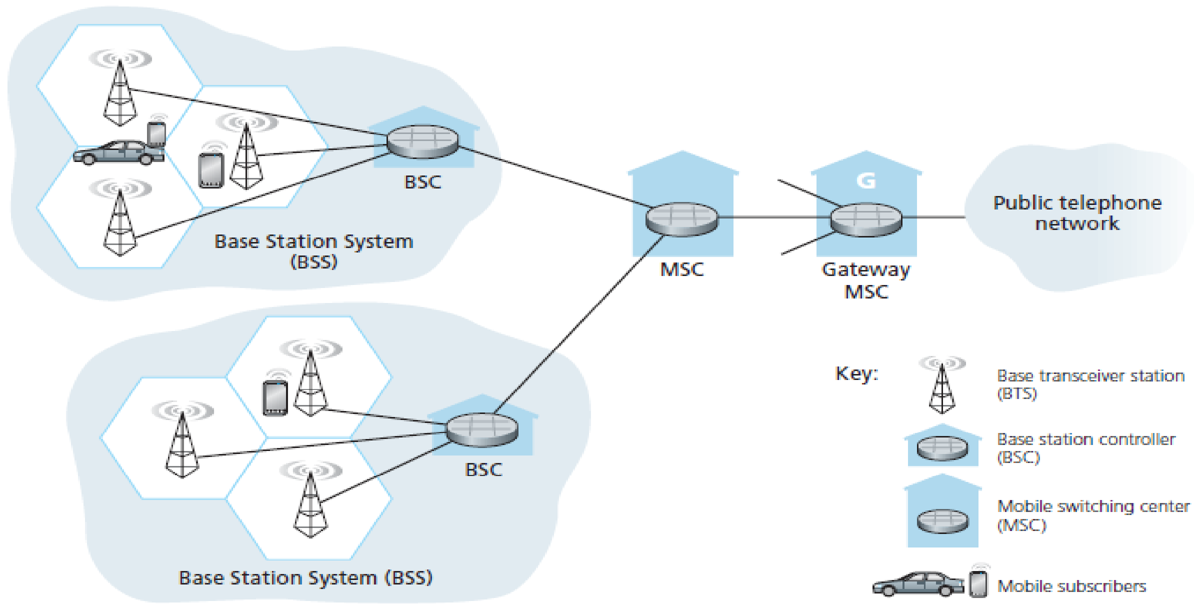
- Nearly 80% of total Cellular network users adopt Global System for Mobile communication (GSM) Standard.
- First generation (1G) systems were analog FDMA systems designed exclusively for voice-only communication. These 1G systems are almost extinct now, having been replaced by digital 2G systems.
- The original 2G systems were also designed for voice, but later extended (2.5G) to support data (i.e., Internet) as well as voice service.
- The 3G systems that currently are being deployed also support voice and data, but with an ever increasing emphasis on data capabilities and higher-speed radio access links.

2G Cellular Network

The term cellular refers to the fact that the region covered by a cellular network is partitioned into a number of geographic coverage areas, known as cells.

Each cell contains a base transceiver station (BTS) that transmits signals to and receives signals from the mobile stations in its cell.

The coverage area of a cell depends on many factors, including the transmitting power of the BTS, the transmitting power of the user devices, obstructing buildings in the cell, and the height of base station antennas.

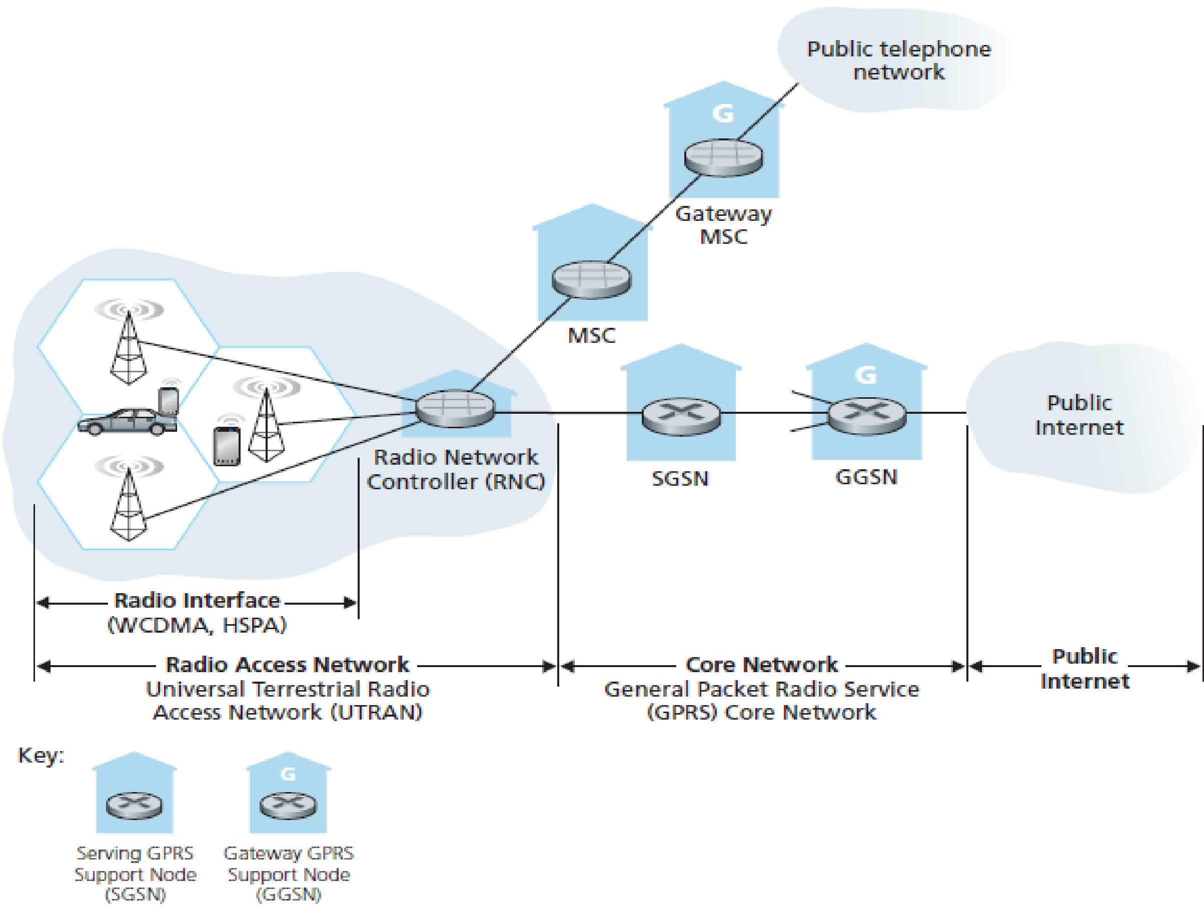


- The GSM standard for 2G cellular systems uses combined FDM/TDM (radio) for the air interface. In combined FDM/TDM systems, the channel is partitioned into a number of frequency sub-bands; within each sub-band, time is partitioned into frames and slots.
- GSM systems consist of 200-kHz frequency bands with each band supporting eight TDM calls. GSM encodes speech at 13 kbps and 12.2 kbps.
- A GSM network's base station controller (BSC) will typically service several tens of base transceiver stations. The role of the BSC is to allocate BTS radio channels to mobile subscribers, perform paging (finding the cell in which a mobile user is resident), and perform handoff of mobile users.
- The base station controller and its controlled base transceiver stations collectively constitute a GSM base station system (BSS).
- The mobile switching center (MSC) plays the central role in user authorization and accounting (e.g., determining whether a mobile device is allowed to connect to the cellular network), call establishment and teardown, and handoff.
- A single MSC will typically contain up to five BSCs, resulting in approximately 200K subscribers per MSC.
- A cellular provider's network will have a number of MSCs, with special MSCs known as gateway MSCs connecting the provider's cellular network to the larger public telephone network.

Abhijith

3G Cellular Data Networks

- The 3G core cellular data network connects radio access networks to the public Internet.
- Principle adapted in 3G: leave the existing core GSM cellular voice network untouched, adding additional cellular data functionality in parallel to the existing cellular voice network.



- There are two types of nodes in the 3G core network: Serving GPRS Support Nodes (SGSNs) and Gateway GPRS Support Nodes (GGSNs). (GPRS stands for Generalized Packet Radio Service)
- An SGSN is responsible for delivering datagrams to/from the mobile nodes in the radio access network to which the SGSN is attached.
- The SGSN interacts with the cellular voice network's MSC for that area, providing user authorization and handoff, maintaining location (cell) information about active mobile nodes, and performing datagram forwarding between mobile nodes in the radio access network and a GGSN.
- The GGSN acts as a gateway, connecting multiple SGSNs into the larger Internet.

3G Radio Access Network: The Wireless Edge

- The Radio Network Controller (RNC) typically controls several cell base transceiver stations.
- The RNC connects to both the circuit-switched cellular voice network via an MSC, and to the packet-switched Internet via an SGSN.
- It uses a CDMA technique known as Direct Sequence Wideband CDMA (DS-WCDMA) within TDMA slots.
- The data service associated with the WCDMA specification is known as HSP (High Speed Packet Access) and promises downlink data rates of up to 14 Mbps.

4G Networks: Long Term Evaluation (LTE)

The 4G Long-Term Evolution (LTE) standards has two important innovations over 3G systems:

1. **Evolved Packet Core (EPC)**

- The EPC is a simplified all-IP core network that unifies the separate circuit-switched cellular voice network and the packet-switched cellular data network.
- It is an "all-IP" network in that both voice and data will be carried in IP datagrams.
- A key task of the EPC is to manage network resources to provide this high quality of service. The EPC also makes a clear separation between the network control and user data planes, with many of the mobility support features.
- The EPC allows multiple types of radio access networks, including legacy 2G and 3G radio access networks, to attach to the core network.

2. **LTE Radio Access Network.**

- LTE uses a combination of frequency division multiplexing and time division multiplexing on the downstream channel, known as orthogonal frequency division multiplexing (OFDM).
- In LTE, each active mobile node is allocated one or more 0.5 ms time slots in one or more of the channel frequencies. By being allocated increasingly more time slots a mobile node is able to achieve increasingly higher transmission rates.
- The maximum data rate for an LTE user is 100 Mbps in the downstream direction and 50 Mbps in the upstream direction, when using 20 MHz worth of wireless spectrum.

Abhijith H V

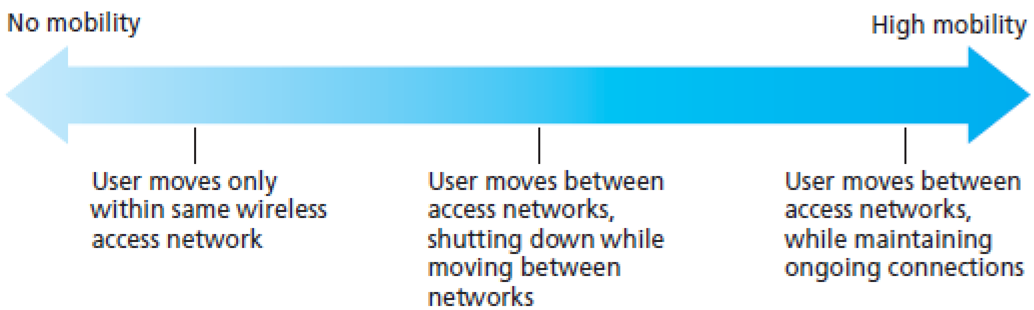
Mobility Management: Principles

A mobile node is one that changes its point of attachment into the network over time.

Several dimensions of mobility:

1. From the network layer's standpoint, how mobile is a user?

- A physically mobile user will present a very different set of challenges to the network layer, depending on how he or she moves between points of attachment to the network. Below figure shows various level of mobility.



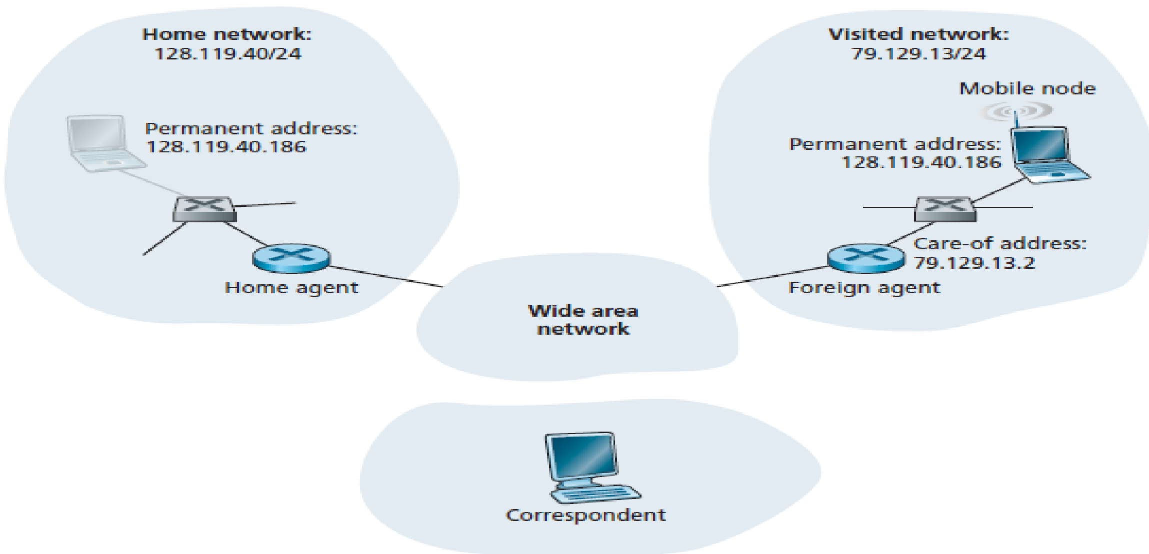
2. How important is it for the mobile node's address to always remain the same?

- With mobile telephony the network-layer address of phone remains the same as you travel from one provider's mobile phone network to another.
- If a mobile entity is able to maintain its IP address as it moves, mobility becomes invisible from the application standpoint. There is great value to this transparency—an application need not be concerned with a potentially changing IP address, and the same application code serves mobile and nonmobile connections alike.
- A less frequent mobile user might simply want to turn off an office laptop, bring that laptop home, power up, and work from home. If the laptop functions primarily as a client in client-server applications (e.g., send/read e-mail, browse the Web, Telnet to a remote host) from home, the particular IP address used by the laptop is not that important.

3. What supporting wired infrastructure is available?

- It is assumed that there is a fixed infrastructure to which the mobile user can connect—for example, the home's ISP network, the wireless access network in the office, or the wireless access networks lining the autobahn. What if no such infrastructure exists? If two users are within communication proximity of each other, can they establish a network connection in the absence of any other network-layer infrastructure?

Elements of Mobile Network Architecture



- In a network setting, the permanent home of a mobile node is known as the **home network**, and the entity within the home network that performs the mobility management functions of the mobile node is known as the **home agent**.
- The network in which the mobile node is currently residing is known as the **foreign (or visited) network**, and the entity within the foreign network that helps the mobile node with the mobility management functions discussed below is known as a **foreign agent**.
- A correspondent is the entity wishing to communicate with the mobile node.

Addressing

In order for user mobility to be transparent to network applications, it is desirable for a mobile node to keep its address as it moves from one network to another.

When a mobile node is resident in a foreign network, all traffic addressed to the node's permanent address now needs to be routed to the foreign network.

One option is for the foreign network to advertise to all other networks that the mobile node is resident in its network.

- The foreign network could simply advertise to its neighbors that it has a highly specific route to the mobile node's permanent address.
- These neighbors would then propagate this routing information throughout the network as part of the normal procedure of updating routing information and forwarding tables.

Abhijith

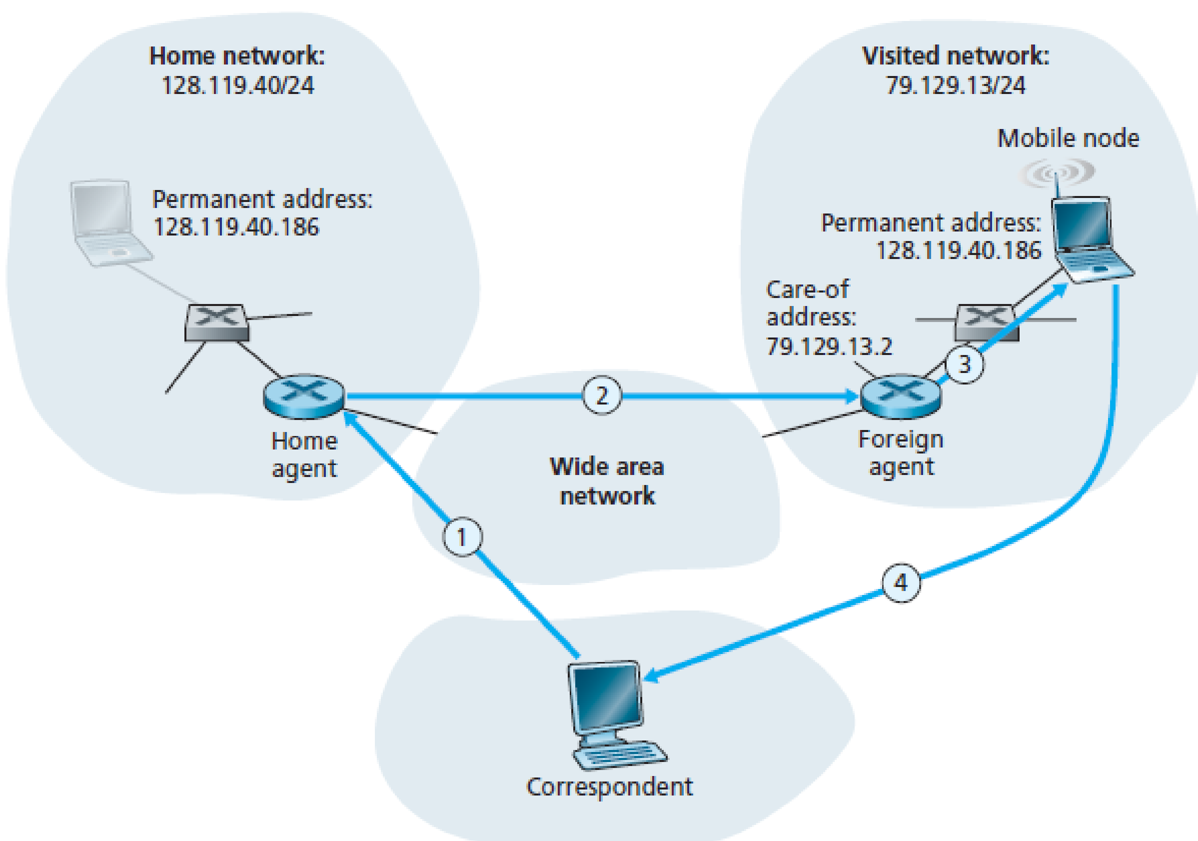
- When the mobile node leaves one foreign network and joins another, the new foreign network would advertise a new, highly specific route to the mobile node, and the old foreign network would withdraw its routing information regarding the mobile node.
- Limitation: Scalability

Another Approach is through care-of-address

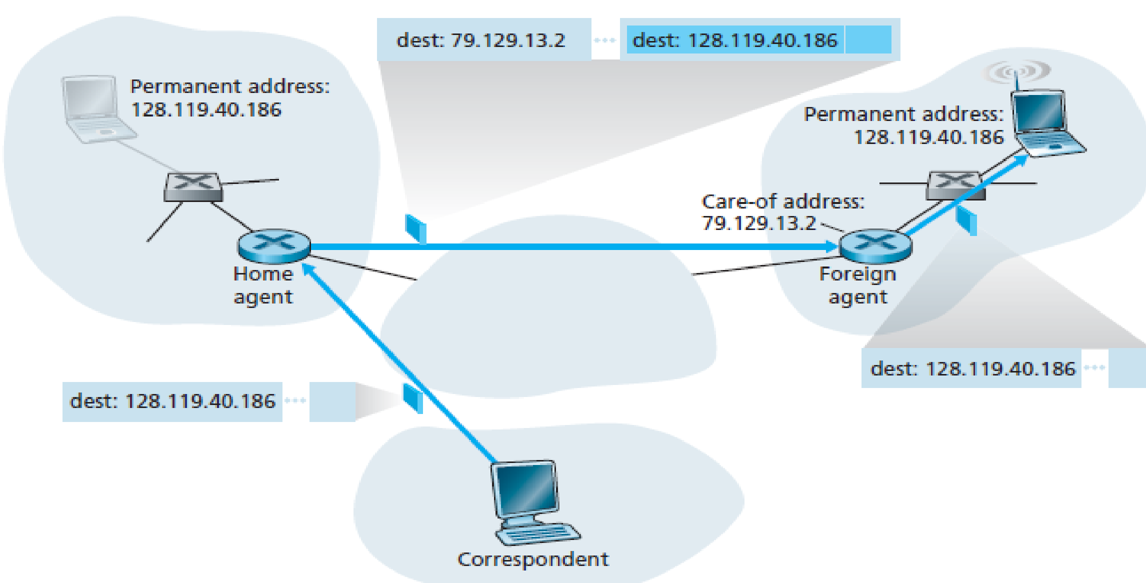
- The conceptually simplest approach is to locate foreign agents at the edge routers in the foreign network. One role of the foreign agent is to create care-of address (COA) for the mobile node, with the network portion of the COA matching that of the foreign network.
- There are thus two addresses associated with a mobile node, its permanent address and its COA, sometimes known as a foreign address.
- A second role of the foreign agent is to inform the home agent that the mobile node is resident in its network and has the given COA.

Routing to a Mobile Node

1) Indirect Routing to a Mobile Node



- In the indirect routing approach, the correspondent simply addresses the datagram to the mobile node's permanent address and sends the datagram into the network, blissfully unaware of whether the mobile node is resident in its home network or is visiting a foreign network; mobility is thus completely transparent to the correspondent.
- Home agent is responsible for interacting with a foreign agent to track the mobile node's COA.
- Home agent second job is to be on the lookout for arriving datagrams addressed to nodes whose home network is that of the home agent but that are currently resident in a foreign network. The home agent intercepts these datagrams and then forwards them to a mobile node in a two-step process.
- The datagram is first forwarded to the foreign agent, using the mobile node's COA, and then forwarded from the foreign agent to the mobile node.
- Home agent encapsulate the correspondent's original complete datagram within a new (larger) datagram. This larger datagram is addressed and delivered to the mobile node's COA.
- The foreign agent, who "owns" the COA, will receive and decapsulate the datagram—that is, remove the correspondent's original datagram from within the larger encapsulating datagram and forward the original datagram to the mobile node.
- Since the mobile node knows the correspondent's address, there is no need to route the datagram back through the home agent.



Indirect routing requires:

- **A mobile-node–to–foreign-agent protocol:** The mobile node will register with the foreign agent when attaching to the foreign network. Similarly, a mobile node will deregister with the foreign agent when it leaves the foreign network.
- **A foreign-agent–to–home-agent registration protocol:** The foreign agent will register the mobile node's COA with the home agent. A foreign agent need not explicitly deregister a COA when a mobile node leaves its network, because the subsequent registration of a new COA, when the mobile node moves to a new network, will take care of this.
- **A home-agent datagram encapsulation protocol:** Encapsulation and forwarding of the correspondent's original datagram within a datagram addressed to the COA.
- **A foreign-agent decapsulation protocol:** Extraction of the correspondent's original datagram from the encapsulating datagram, and the forwarding of the original datagram to the mobile node.

2) Direct Routing to a Mobile Node

Limitation of indirect routing:

The indirect routing approach suffers from an inefficiency known as the **triangle routing problem**—datagrams addressed to the mobile node must be routed first to the home agent and then to the foreign network, even when a much more efficient route exists between the correspondent and the mobile node.

In the worst case, imagine a mobile user who is visiting the foreign network of a colleague.

The two are sitting side by side and exchanging data over the network. Datagrams from the correspondent (in this case the colleague of the visitor) are routed to the mobile user's home agent and then back again to the foreign network.

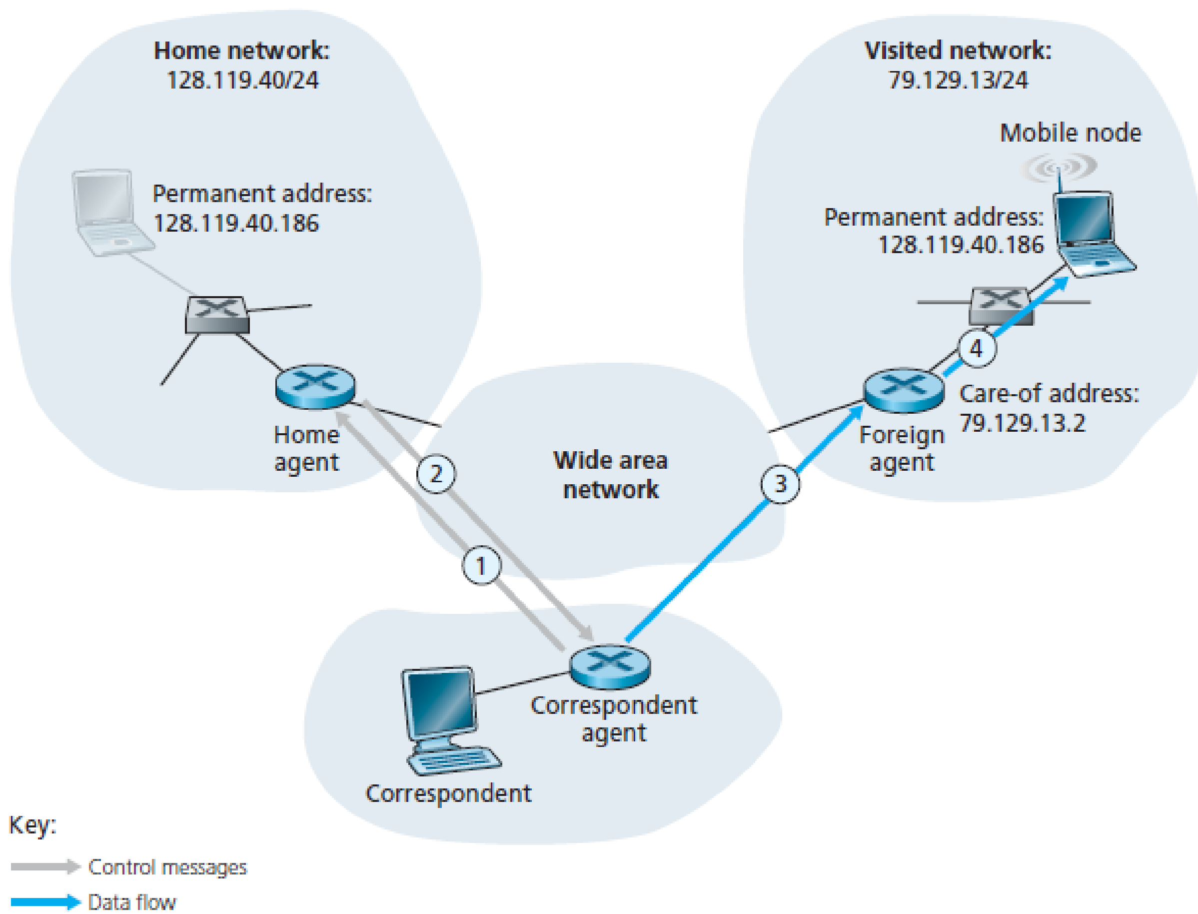
Solution:

- Direct routing overcomes the inefficiency of triangle routing, but does so at the cost of additional complexity.
- In the direct routing approach, a correspondent agent in the correspondent's network first learns the COA of the mobile node. This can be done by having the correspondent agent

Abhijith H V

query the home agent, assuming that the mobile node has an up-to-date value for its COA registered with its home agent.

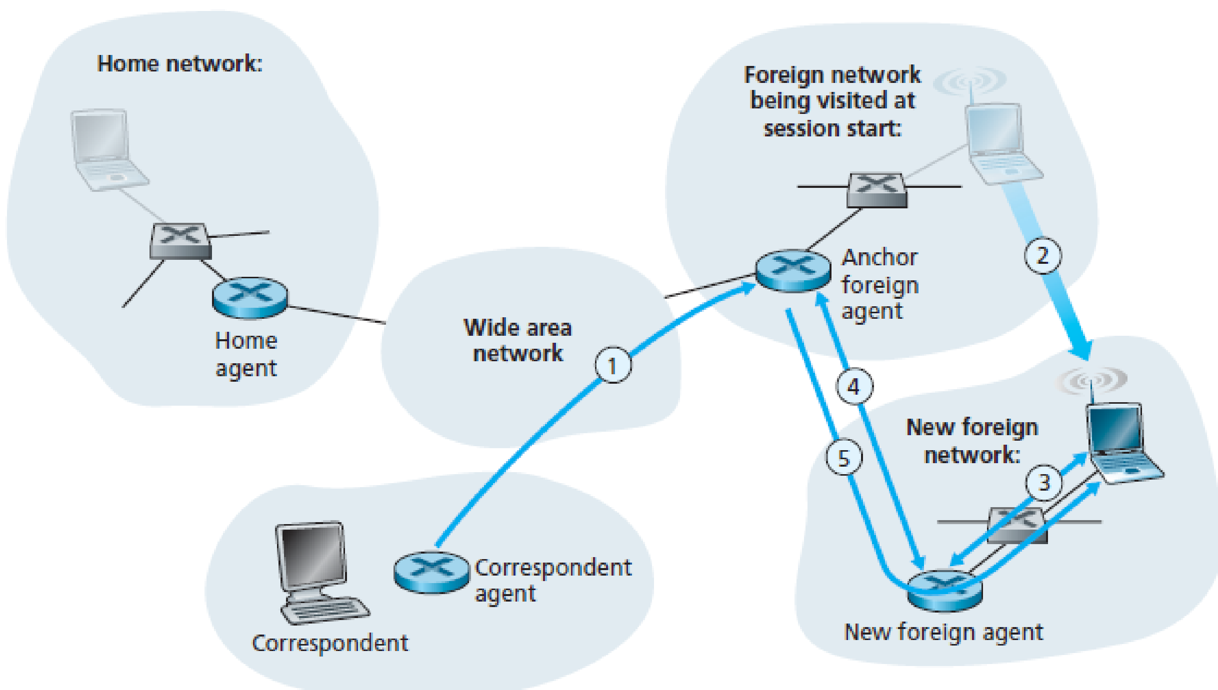
- It is also possible for the correspondent itself to perform the function of the correspondent agent, just as a mobile node could perform the function of the foreign agent. (step 1 and step 2 of below figure).
- The correspondent agent then tunnels datagrams directly to the mobile node's COA, in a manner analogous to the tunneling performed by the home agent, (steps 3 and 4)



While direct routing overcomes the triangle routing problem, it introduces two important additional challenges:

- A mobile-user location protocol is needed for the correspondent agent to query the home agent to obtain the mobile node's COA
- Suppose data is currently being forwarded to the mobile node in the foreign network where the mobile node was located when the session first started (Step 1).We'll identify the foreign agent in that foreign network where the mobile node was first found as the anchor foreign

agent. When the mobile node moves to a new foreign network (step 2), the mobile node registers with the new foreign agent (step 3), and the new foreign agent provides the anchor foreign agent with the mobile node's new COA (step 4). When the anchor foreign agent receives an encapsulated datagram for a departed mobile node, it can then re-encapsulate the datagram and forward it to the mobile node (step 5) using the new COA. If the mobile node later moves yet again to a new foreign network, the foreign agent in that new visited network would then contact the anchor foreign agent in order to set up forwarding to this new foreign network.



Mobile IP

Mobile IP is a flexible standard, supporting many different modes of operation (for example, operation with or without a foreign agent), multiple ways for agents and mobile nodes to discover each other, use of single or multiple COAs, and multiple forms of encapsulation.

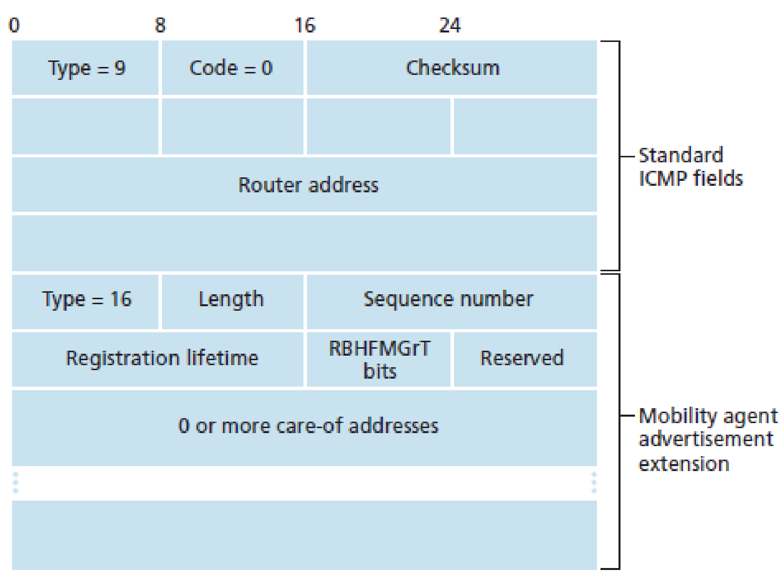
The mobile IP standard consists of three main pieces:

- **Agent discovery:** Mobile IP defines the protocols used by a home or foreign agent to advertise its services to mobile nodes, and protocols for mobile nodes to solicit the services of a foreign or home agent.

- **Registration with the home agent:** Mobile IP defines the protocols used by the mobile node and/or foreign agent to register and deregister COAs with a mobile node's home agent.
- **Indirect routing of datagrams**: The standard also defines the manner in which datagrams are forwarded to mobile nodes by a home agent, including rules for forwarding datagrams, rules for handling error conditions, and several forms of encapsulation

Agent Discovery

- A mobile IP node arriving to a new network, whether attaching to a foreign network or returning to its home network, must learn the identity of the corresponding foreign or home agent. Indeed it is the discovery of a new foreign agent, with a new network address, that allows the network layer in a mobile node to learn that it has moved into a new foreign network. This process is known as **agent discovery.**
- Agent discovery can be accomplished in one of two ways: via **agent advertisement** or via **agent solicitation**.
- With **agent solicitation**, a mobile node wanting to learn about agents without waiting to receive an agent advertisement can broadcast an agent solicitation message, which is simply an ICMP message with type value 10. An agent receiving the solicitation will unicast an agent advertisement directly to the mobile node.
- With **agent advertisement**, a foreign or home agent advertises its services using an ICMP type=9 and code=0 message.



Important fields in agent advertisement are:

- **Home agent bit (H):** Indicates that the agent is a home agent for the network in which it resides.
- **Foreign agent bit (F):** Indicates that the agent is a foreign agent for the network in which it resides.
- **Registration required bit (R):** Indicates that a mobile user in this network must register with a foreign agent.
- **M, G encapsulation bits:** Indicate whether a form of encapsulation will be used.
- **Care-of address (COA) fields:** A list of one or more care-of addresses provided by the foreign agent.

Registration with the Home Agent

Once a mobile IP node has received a COA, that address must be registered with the home agent. This involves following four steps.

Step 1:

- Following the receipt of a foreign agent advertisement, a mobile node sends a mobile IP registration message to the foreign agent.
- The registration message is carried within a UDP datagram and sent to port 434.
- The registration message carries a COA advertised by the foreign agent, the address of the home agent (HA), the permanent address of the mobile node (MA), the requested lifetime of the registration, and a 64-bit registration identification.
- The requested registration lifetime is the number of seconds that the registration is to be valid. If the registration is not renewed at the home agent within the specified lifetime, the registration will become invalid.

Step 2:

- The foreign agent receives the registration message and records the mobile node's permanent IP address.
- The foreign agent then sends a mobile IP registration message to home agent.

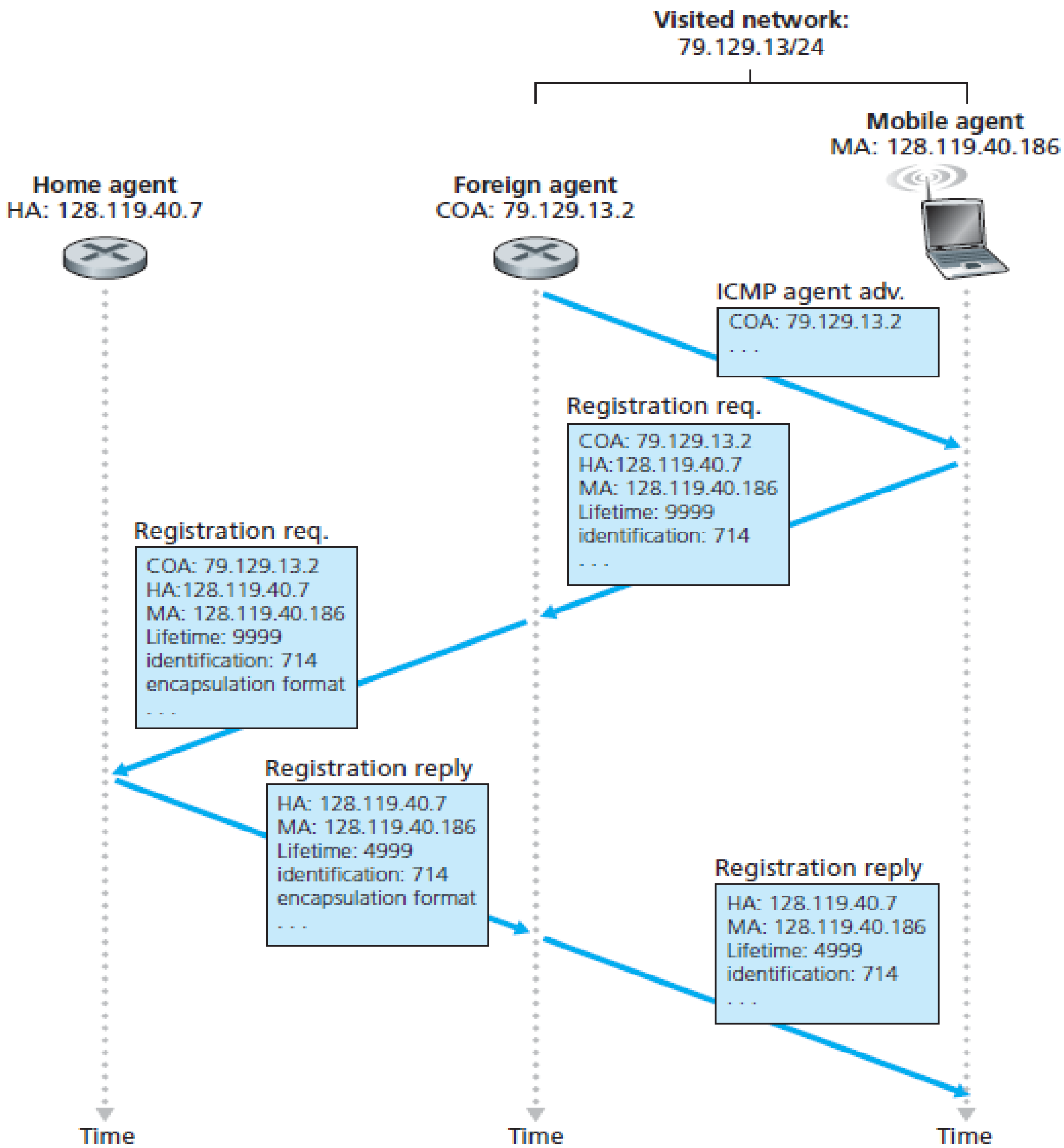
Step 3:

- The home agent receives the registration request and checks for authenticity and correctness.

- The home agent binds the mobile node's permanent IP address with the COA; in the future, datagrams arriving at the home agent and addressed to the mobile node will now be encapsulated and tunneled to the COA.
- The home agent sends a mobile IP registration reply containing the HA, MA, actual registration lifetime, and the registration identification of the request that is being satisfied with this reply.

Step 4:

The foreign agent receives the registration reply and then forwards it to the mobile node.



Indirect Routing:

Correspondent sends data to home agent. Home agent encapsulates the data and forwards it to foreign agent using COA. Foreign agent delivers the data to mobile node.

Managing Mobility in Cellular Networks

Like mobile IP, GSM adopts an indirect routing approach, first routing the correspondent's call to the mobile user's home network and from there to the visited network.

In GSM terminology, the mobile users's home network is referred to as the mobile user's **home public land mobile network** (home PLMN) or **home network**.

The home network is the cellular provider with which the mobile user has a subscription.

The **visited PLMN**, which will be refered as the **visited network**, is the network in which the mobile user is currently residing.

Home network has **home MSC (home agent)** and MSC in visited network is **visited MSC (visited agent).**

Each MSC maintain two databases:

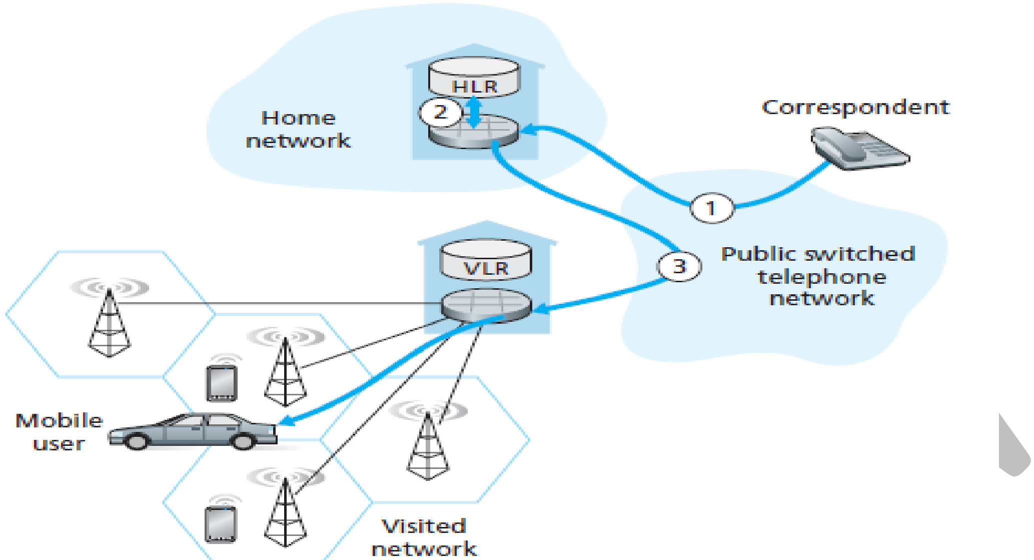
1. **Home location register (HLR):** HLR contains the permanent cell phone number and subscriber profile information for each of its subscribers. Importantly, the HLR also contains information about the current locations of these subscribers.
2. **Visitor location register (VLR):** The VLR contains an entry for each mobile user that is currently in the portion of the network served by the VLR. VLR entries thus come and go as mobile users enter and leave the network.

Routing Calls to a Mobile User

1. The correspondent dials the mobile user's phone number. The leading digits in the number are sufficient to globally identify the mobile's home network. The call is routed from the correspondent through the PSTN to the home MSC in the mobile's home network.
2. The home MSC receives the call and interrogates the HLR to determine the location of the mobile user. In the simplest case, the HLR returns the **mobile station roaming number (MSRN)**, or **roaming number**.

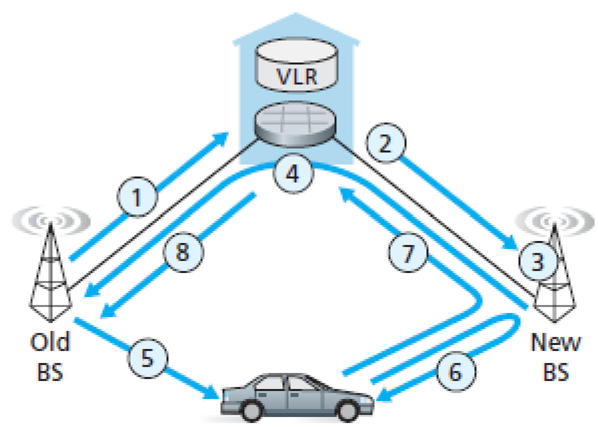
Abhijith H V

3. The call is completed, being routed from the correspondent to the home MSC, and from there to the visited MSC, and from there to the base station serving the mobile user.



Handoffs in GSM

- A handoff occurs when a mobile station changes its association from one base station to another during a call.
- There may be several reasons for handoff to occur, including
  1. The signal between the current base station and the mobile may have deteriorated to such an extent that the call is in danger of being dropped
  2. A cell may have become overloaded, handling a large number of calls.



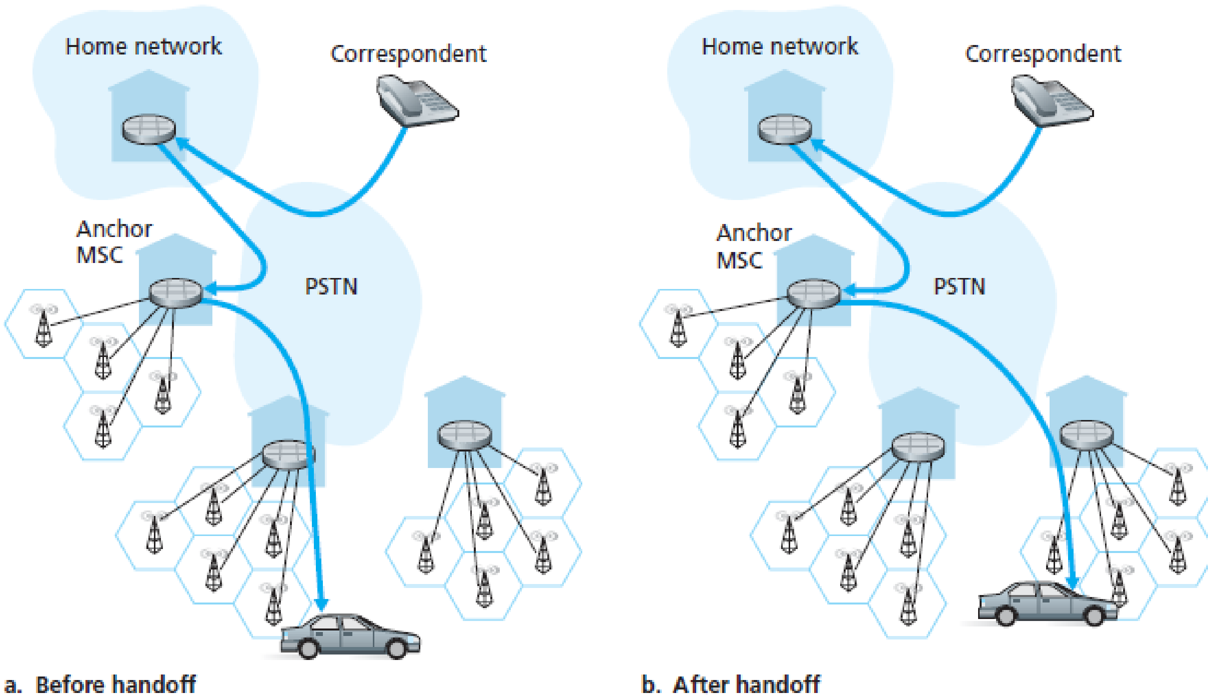
Steps:

1. The old base station (BS) informs the visited MSC that a handoff is to be performed and the BS (or possible set of BSs) to which the mobile is to be handed off.
2. The visited MSC initiates path setup to the new BS, allocating the resources needed to carry the rerouted call, and signaling the new BS that a handoff is about to occur.
3. The new BS allocates and activates a radio channel for use by the mobile.
4. The new BS signals back to the visited MSC and the old BS that the visited-MSC-to-new-BS path has been established and that the mobile should be informed of the impending handoff. The new BS provides all of the information that the mobile will need to associate with the new BS.
5. The mobile is informed that it should perform a handoff. Note that up until this point, the mobile has been blissfully unaware that the network has been laying the groundwork (e.g., allocating a channel in the new BS and allocating a path from the visited MSC to the new BS) for a handoff.
6. The mobile and the new BS exchange one or more messages to fully activate the new channel in the new BS.
7. The mobile sends a handoff complete message to the new BS, which is forwarded up to the visited MSC. The visited MSC then reroutes the ongoing call to the mobile via the new BS.
8. The resources allocated along the path to the old BS are then released.

Inter-MSC handoff

- The anchor MSC is the MSC visited by the mobile when a call first begins; the anchor MSC thus remains unchanged during the call.
- Throughout the call's duration and regardless of the number of inter-MSC transfers performed by the mobile, the call is routed from the home MSC to the anchor MSC, and then from the anchor MSC to the visited MSC where the mobile is currently located.
- When a mobile moves from the coverage area of one MSC to another, the ongoing call is rerouted from the anchor MSC to the new visited MSC containing the new base station.
- Thus, at all times there are at most three MSCs (the home MSC, the anchor MSC, and the visited MSC) between the correspondent and the mobile.

- Rather than maintaining a single MSC hop from the anchor MSC to the current MSC, an alternative approach would have been to simply chain the MSCs visited by the mobile, having an old MSC forward the ongoing call to the new MSC each time the mobile moves to a new MSC.



Wireless and Mobility: Impact on Higher- Layer Protocols

- Network layer provides the same best-effort delivery service model to upper layers in both wired and wireless networks.
- Similarly, if protocols such as TCP or UDP are used to provide transport-layer services to applications in both wired and wireless networks, then the application layer should remain unchanged as well.
- The TCP and UDP can operate in networks with wireless links. On the other hand, transport protocols in general, and TCP in particular, can sometimes have very different performance in wired and wireless networks.
- TCP retransmits a segment that is either lost or corrupted on the path between sender and receiver. In the case of mobile users, loss can result from either network congestion or from handoff. In all cases, TCP's receiver-to-sender ACK indicates only that a segment was not

received intact; the sender is unaware of whether the segment was lost due to congestion, during handoff, or due to detected bit errors. In all cases, the sender's response is the same—to retransmit the segment.

- Bit errors are much more common in wireless networks than in wired networks.
- Given high bit error rates on wireless links and the possibility of handoff loss, TCP's congestion-control response could be problematic in a wireless setting. Three broad classes of approaches are possible for dealing with this problem:
  1. **Local recovery:** Local recovery protocols recover from bit errors when and where they occur.
  2. **TCP sender awareness of wireless links:** In the local recovery approaches, the TCP sender is blissfully unaware that its segments are traversing a wireless link. An alternative approach is for the TCP sender and receiver to be aware of the existence of a wireless link, to distinguish between congestive losses occurring in the wired network and corruption/loss occurring at the wireless link, and to invoke congestion control only in response to congestive wired-network losses.
  3. **Split-connection approaches:** In a split-connection approach the end-to-end connection between the mobile user and the other end point is broken into two transport-layer connections: one from the mobile host to the wireless access point, and one from the wireless access point to the other communication end point. The end-to-end connection is thus formed by the concatenation of a wireless part and a wired part.
- Wireless links often have relatively low bandwidth. As a result, applications that operate over wireless links, particularly over cellular wireless links, must treat bandwidth as a scarce commodity.

Abhijith HV