CHAPTER 3

Unit III

Mobile Networking

Syllabus

3.1 Mobile Networking : Medium Access Protocol, Internet Protocol and Transport layer

3.2 Medium Access Control : Motivation for specialized MAC, Introduction to multiple Access techniques (MACA)

3.3 Mobile IP: IP Packet Delivery, Agent Advertisement and Discovery, Registration, Tunneling and Encapsulation, Reverse Tunneling, Routing (DSDV,DSR)

3.4 Mobile TCP : Traditional TCP, Classical TCP Improvements like Indirect TCP, Snooping TCP & Mobile TCP, Fast Retransmit/ Fast Recovery, Transmission/Timeout Freezing, Selective Retransmission.

Introduction

With the rapid usage of portable devices, mobility has become an important factor in the success of mobile networks. Existing network protocols that are developed for fixed network do not work well if used directly in wireless networks. This is because the wireless networks impose various challenges like dynamic topology, asymmetric links, frequent disconnections, security, high error rate etc. To support mobility, either new protocols have to be developed or existing protocols need to be modified. This chapter discusses problems with some of the existing MAC, Internet and TCP layer protocol and required modifications to support mobility.

3.1 Mobile Networking

- Now a day, people want to access the services from anywhere, anytime irrespective of their location. This feature of moving anywhere and still be able to access the services is called mobility.
- Making such services mobile, requires modification to existing protocols and at some extent to existing architecture. The following section discusses the improvements or modifications need to be done in Media Access Control, Internet and Transport layer protocols to make a network or services mobile.

3.1.1 Medium Access Protocols

- Medium access protocols basically controls access to the shared medium.
- We know many of the MAC protocols for wired (or fixed) network such as ALOHA, Slotted ALOHA, CSMA, CSMA/CD, Token bus, token ring etc. Since wireless medium is a shared medium MAC protocols become an important design decision for wireless network.
- But all this MAC protocols from wired networks cannot be directly used for wireless networks. Here, we have introduced several **Medium Access Control (MAC)** algorithms which are specifically adapted to the wireless domain.
- Medium access control comprises all mechanisms that regulate user access to a medium using SDM, TDM, FDM, or CDM. MAC is thus similar to traffic regulations in the multiplexing.
- In this chapter we will discuss various MAC protocols specially designed for wireless networks.

3.1.2 Internet Protocols

- In traditional IP routing, IP addresses represent a topology. Routing mechanisms rely on the assumption that each network node will always have the same point of attachment to the Internet. Each node's IP address identifies the network link where it is connected.

- The Internet routers look at the IP address prefix, which identifies a device's network.
- At the network level, routers look at the next few bits to identify the appropriate subnet. Finally, at the subnet level, routers look at the bits identifying a particular device.
- In this routing scheme, if you disconnect a mobile device from the Internet and want to reconnect through a different subnet, you have to configure the device with a new IP address, and the appropriate netmask and default router. Otherwise, routing protocols have no means of delivering packets. This is because the device's IP address doesn't contain the necessary information about the current point of attachment to the Internet.
- The necessity for uninterrupted communication when the mobile device moves from one location to another calls for a new technology.
- This kind of communication can be efficiently implemented using Mobile IP. **Mobile IP** (or MIP) is an IETF standard communications protocol that is designed to allow **mobile** device users to move from one network to another while maintaining a permanent **IP** address.
- Section 3.3 discusses detail Mobile IP protocols and it's functionalities.

3.1.3 Transport Protocols

- Transmission control Protocol (TCP) is typically designed for fixed network.
- If we use the same TCP over mobile network, the performance of the TCP degrades.
- Existing TCP can be modified to support mobility.
- Section 3.5 discusses working of existing TCP, problems with existing TCP if used in mobile network and some modifications to the existing TCP that can be used for mobile networks.

3.2 Medium Access Control

3.2.1 Motivation for Specialized MAC

MU – May 18

Q. Explain the need of specialized MAC in wireless communication. **(May 18, 10 Marks)**

- CSMA/CD is the most commonly used MAC protocol for wired network. The question is, can we use the same CSMA/CD for wireless networks to control the medium access without any modifications?
- Let us consider carrier sense multiple access with collision detection, (CSMA/CD) which works as follows.
- A sender senses the medium (a wire) to see if it is free. If the medium is busy, the sender waits until it is free. If the medium is free, the sender starts transmitting data and continues to listen into the medium. If the sender detects a collision while sending, it stops at once and sends a jamming signal.
- But this scheme fails in wireless networks. This is because, CSMA/CD is not really interested in collisions at the sender, but rather in those at the receiver. The signal should reach the receiver without collisions. But the sender is the one who detects the collisions.
- This is not a problem using a wire, as the same signal strength can be assumed all over the wire if the length of the wire stays within certain standardized limits. If a collision occurs somewhere in the wire, everybody will notice it.
- The situation is different in wireless networks. Two problems hidden terminal and exposed terminal problem occur in wireless network which are discussed on following sections.
- Collision detection is very difficult in wireless scenarios as the transmission power in the area of the transmitting antenna is several magnitudes higher than the receiving power. So, this very common MAC scheme from wired network fails in a wireless scenario.
- The following sections show scenarios where CSMA/CD scheme form fixed networks fail in case of wireless network.

3.2.1(a) Hidden Station Problem and Exposed Station Problem

MU – May 12, Dec. 12, Dec. 13, May 15, May 16, May 17, Dec. 17

Q. What is Hidden and Exposed terminal problem? Discuss solutions to these problems. **(May 12, Dec. 13, 10 Marks)**

Q. What do you mean by Exposed terminal problem ? **(Dec. 12, 5 Marks)**

Q. What do you mean by Hidden terminal problem? **(Dec. 12, May 16, 5 Marks)**

Q. Explain hidden station and exposed station problems in WLAN. **(May 15, May 16, 5 Marks)**

Q. What is hidden and exposed terminal problems? Discuss solution to these problems. **(May 17, 5 Marks)**

Q. Why do hidden terminal and exposed terminal problems arise? How would you propose to solve it? **(Dec. 17, 10 Marks)**

- Wireless medium is an open, shared, and broadcast medium. Multiple nodes may access the medium at the same time.
- Traditional LANs uses CSMA/CD mechanism to control media access. This scheme works for wired network but not for wireless.
- CSMA/CD fails in case of wireless networks due to the following reason.
- In the wired network the signal strength can be assumed to be same all over the wire if the length of the wire stays within certain standardized limits. If a collision occurs somewhere in the wire, each station will notice it. But the situation is different in a wireless LAN. Here, the strength of a signal decreases proportionally to the square of the distance to the sender.
- Due to this reason, MAC schemes for wired networks may fail when used for wireless networks.
- Following two scenarios show where conventional CSMA/CD fails when used in wireless networks.

1. Hidden Station (or Terminal) Problem

Consider the scenario with three mobile phones A, B and C as shown in Fig. 3.2.1

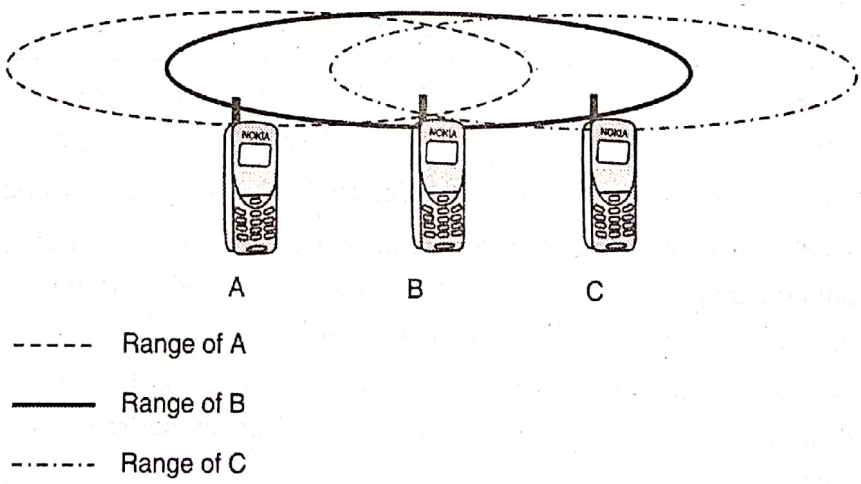


Fig. 3.2.1 : Hidden station problem

- The transmission range of A reaches B, but not C.
- The transmission range of C reaches B, but not A.
- Finally, the transmission range of A reaches both A and C. That is, A cannot detect C and vice versa.

(i) Initially, A senses the channel and since it finds the channel free, A transmits to B.

(ii) While A is transmitting, C also wants to transmit to B and hence senses the channel.

(iii) C does not hear A's transmission (because A is out of range of C).

(iv) C concludes that the channel is free and starts transmitting to B.

(v) Signals from A and C both collide at B.

(vi) "A" is hidden for "C".

2. Exposed Station Problem

Consider the situation shown in Fig. 3.2.2. Along with the previous situation now node D is added which is in the range of C.

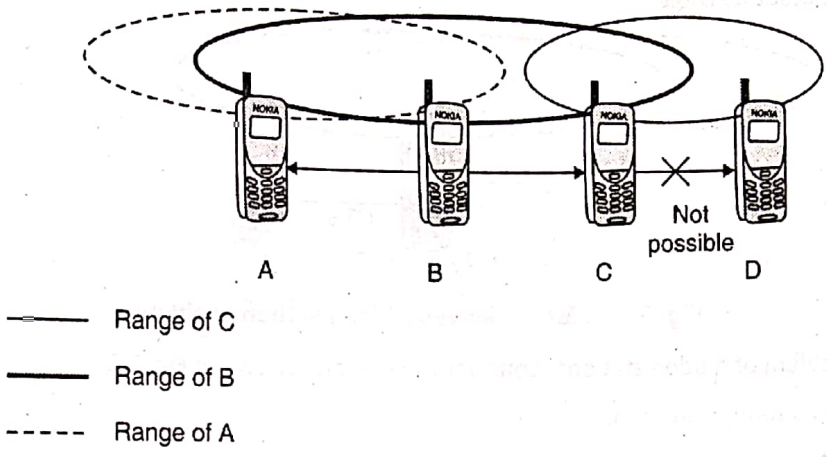


Fig. 3.2.2 : Exposed Station (or Terminal) Problem

(i) B wants to send data to A. B senses the channel and finds it free and hence transmits to A.

(ii) Now C also wants to talk to D.

(iii) C senses the channel and finds it to be busy (C can hear B's transmission since B is in C's range).

(iv) C concludes that the channel is busy and does not transmit (when it could have ideally transmitted to D because A is outside the radio range of C).

(v) "C" is exposed to "B".

The Hidden Terminal problem leads to :

(i) More collisions

(ii) Wastage of resources

On the other hand, Exposed Terminal problem leads to :

(i) Underutilization of channel

(ii) Lower effective throughput

3.2.2 Multiple Access with Collision Avoidance (MACA)

MU - May 16, May 17, Dec. 17

Q. Explain in short how Hidden station problem is avoided in WLAN. **(May 16, 5 Marks)**

Q. What is hidden and exposed terminal problems? Discuss solution to these problems. **(May 17, 5 Marks)**

Q. Why do hidden terminal and exposed terminal problems arise? How would you propose to solve it? **(Dec. 17, 10 Marks)**

- Hidden and exposed terminal problems can be solved by using multiple access with collision avoidance (MACA) protocol.
- We know that, "Absence of carrier does not always mean an idle medium" in the context of hidden terminal problem and "Presence of carrier does not always mean a busy medium" in the context of exposed terminal problem, MACA solves both the problems.

- MACA uses two short signaling packets called RTS and CTS for collision avoidance.
  - (i) **RTS (request to send) :** A sender requests the 'right to send' from a receiver by transmitting RTS packet before data transmission.
  - (ii) **CTS (clear to send) :** The receiver grants the 'right to send' as soon as it is ready to receive by sending back a CTS packet.
- These packets contain sender address, receiver address and length of future transmission.
- MACA solves Hidden Station Problem.

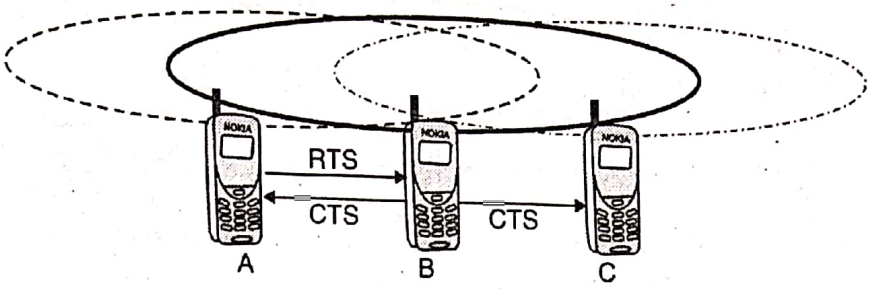


Fig. 3.2.3 : MACA solves Hidden station problem

- MACA avoids the problem of hidden stations. Consider the scenario shown in Fig. 3.2.3.
  1. A and C want to communicate to B.
  2. A sends RTS first.
  3. B receives RTS that contains name of the sender (A), receiver (B) and the length of future transmission. This RTS is not heard by C (Not in C's range).
  4. B responds to RTS by sending CTS. CTS packet contains the sender (A), the receiver (B) and the length of the future transmission. This CTS is received by both A and C (B is in range of both A and C).
  5. C waits after receiving CTS from B and is not allowed to transmit anything for the duration indicated in received CTS.
- Still there are chances of collision during the sending of an RTS. Both A and C could send an RTS at the same time that collides at B. An RTS packet is very small as compared to data packet, so the probability of a collision is much lower.

  In such cases, B resolves this contention and sends CTS to only one station.
- MACA Solves Exposed Terminal Problem
- MACA also avoids the problem of exposed terminals.

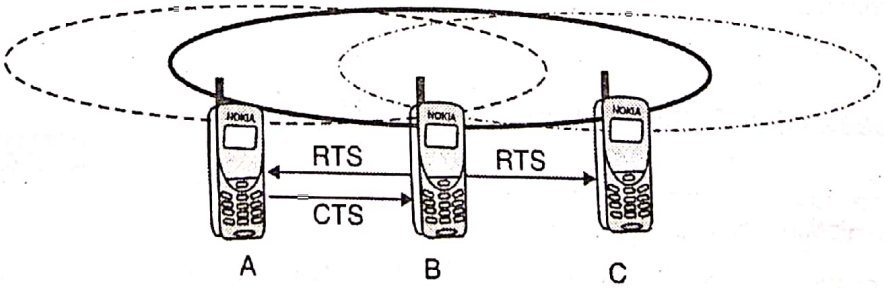


Fig. 3.2.4 : MACA solves exposed terminal problem

- Consider the scenario shown in Fig. 3.2.4.
  1. B wants to send data to A.
  2. C also wants to send data to someone else (Not to A and B)
  3. B sends RTS with sender as B, Receiver as A and length of the data packet. This RTS is received by both A and C.
  4. C does not react to this RTS as it is not the receiver.
  5. A responds to RTS by sending CTS.

6. This CTS is not received by C (A is not in C's range) and C concludes that A is outside the detection range.
7. C can now start its transmission assuming it will not cause a collision at A.

Drawbacks of MACA

1. One problem with MACA is the overheads associated with RTS and CTS transmission for short and time critical data packets.
2. MACA also assumes that the transmission links are symmetrical in both the uplink and the downlink directions. Otherwise a strong sender, directed antenna etc. could contract with the above scheme.

3.3 Mobile IP

3.3.1 Mobile IP : Basic Concept

- Mobile IP (or IP mobility) is a communication protocol developed by Internet Engineering Task Force (IETF) standard.
- In mobile IP, nodes continue to receive packets independent of their location which is achieved by modifying the standard IP in a certain way. It is designed such that mobile users can move from one network to another while maintaining a permanent IP address.

3.3.1(a) Need for Mobile IP

- To understand the need for Mobile IP, let us first understand the problem with the internet protocol (IP).
- In the standard IP, a host's IP address is made up of a network identifier and a host identifier. This network identifier specifies the network the host is attached to.
- A host sends an IP Packet with the header containing a destination address, made up of its network identifier and destination identifier.
- As long as the receiver remains connected to its original network, it can receive packets.
- Now suppose the receiver disconnects itself from its original network and joins another network, the receiver would never receive any packets. This is because, the IP address of the host is now topologically not correct in the new network.
- Hence, a host needs a so-called topologically correct address and Mobile IP standard was developed.

3.3.1(b) Goals/Requirements of Mobile IP

MU – Dec. 18

(Dec. 18, 5 Marks)

Q. What is the goal of Mobile IP?

1. **Flawless Device Mobility Using Existing Device Address**

   Mobile devices can continue to use their existing IP address even while changing their actual location or their original network.

2. **No additional Addressing or Routing Requirements**
   - The same overall scheme for addressing and routing must be maintained as in regular IP. The owner of each device must assign IP addresses in the usual way.
   - New routing requirements must not be placed on the internetwork, like host-specific routes.
3. **Interoperability**

   Mobile IP devices can continue to communicate with other IP devices that have no idea about how Mobile IP works, and vice-versa.

4. **Transparency of Layers**
   - All changes made by Mobile IP must remain confined to the network layer.
   - Other layers like the transport layer and applications must be able to function in the same way as regular IPv4.
5. **Restraining Hardware Changes**
   - A few changes are required to the routers that are used, by the mobile device and the mobile device software for Mobile IP.
   - These changes must be kept to a minimum. Other devices, however, like routers between the ones on the home and visited networks, do not need changes.
6. **Scalability**
   - Mobile IP must allow any device to change from one network to another network, and this must be supported for an arbitrary number of devices.
   - The scope of the connection change must be global. For example, you can use your laptop from an office in London and also use it if you move to Mumbai.
7. **Security**

   Mobile IP must include authentication procedures to prevent unauthorized devices from causing accessing the network and thereby causing problems.

3.3.1(c) Basic Terminology

MU – May 12, Dec. 16

Q. List the entities of mobile IP and describe data transfer from a mobile node to a fixed node and vice versa. **(May 12, Dec. 16, 10 Marks)**

1. **Mobile Node (MN)**

   An end-system or a router (node) that can change its point of connection to the network without changing its IP address.
2. **Correspondent Node (CN)**

   It is the communication partner for the mobile node. The CN can be fixed or mobile.
3. **Home Network (HN)**

   The home network is the subnet to which the MN belongs to with respect to its IP address.
4. **Foreign Network (FN)**

   The foreign network is the current subnet the MN visits and which is not the home network.
5. **Foreign Agent (FA)**
   - The FA is typically a router in the foreign network to which the mobile node is currently attached.
   - The FA usually implements Mobile IP functions like providing security services to the MN during its visit to the FN and forwarding the datagrams received from the home agent to the MN.
   - It also supports the sharing of mobility information so that Mobile IP operates smoothly.

6. **Home Agent (HA)**
   - HA is a system in the home network of the MN.
   - HA can be implemented on router that is responsible for the home network, or alternatively, it can be implemented on a node in a home subnet.
   - HA maintains a location registry i.e. it is informed of the MN's location.
   - The tunnel for packets towards the MN starts at the HA.
7. **Care of Address (COA)**
   - The COA defines the current location of the MN.
   - Packet delivery towards the MN is done using a tunnel.
   - All IP Packets sent to the MN are delivered to the COA.

   There are 2 different possibilities for the location of the COA.

   (i) Foreign Agent COA

   The COA could be the IP address of the FA. In this case, the tunnel endpoint is the FA. The FA forwards packets to the MN.

   (ii) Co- located COA

   If the MN acquires a temporary IP address to act as the COA, the COA is said to be co – located. This address is a topologically correct address and the MN's topologically correct IP address is now the tunnel endpoint.

- In Fig. 3.3.1, an example network is shown.
- A CN connects to the internet via a router. Another router implements the HA, thus connecting the home network and the internet.
- The foreign network's router acts as the FA. Currently, the MN is in the foreign network. The tunnel's start point is at HA and end point is at FA, for the packets directed towards the MN.

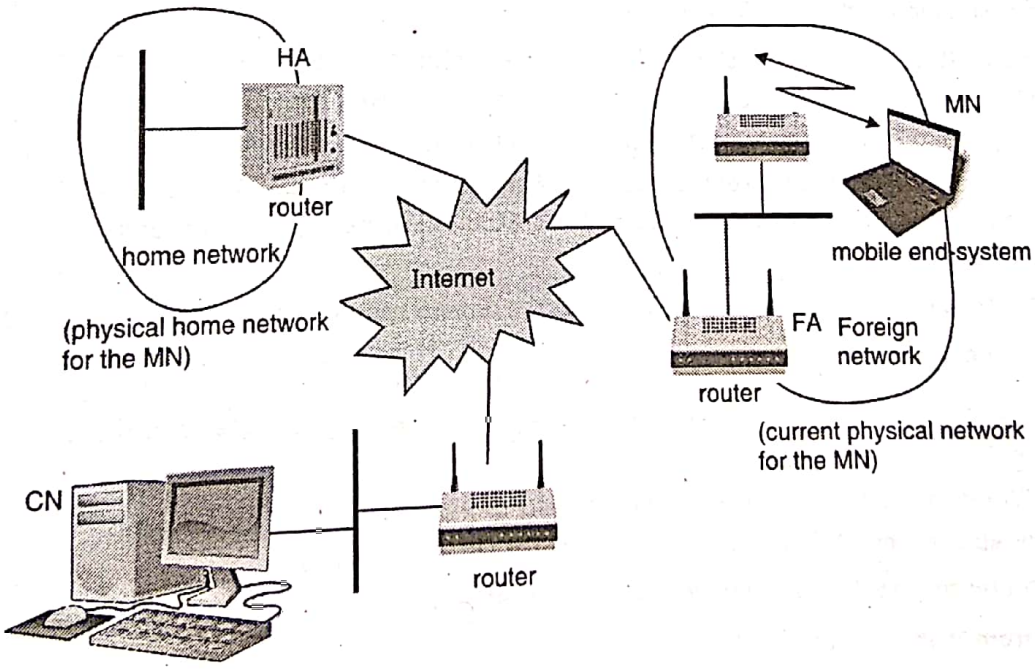


Fig. 3.3.1 : An example mobile IP network

Note : Tunnel for a packet sent to the MN always starts at HA and ends at either FA or MN depending upon the mode of COA. If the COA is foreign agent COA, then the tunnel ends at FA. If the COA is co-located, then the tunnel ends at MN.

3.3.2 IP Packet Delivery

MU – May 12, Dec. 13, Dec. 16, Dec. 18

Q. List the entities of mobile IP and describe data transfer from a mobile node to a fixed node and vice versa. **(May 12, Dec. 16, 10 Marks)**

Q. Explain the IP Packet Delivery with respect to mobile IP. **(Dec. 13, 5 Marks)**

Q. How is packet delivery achieved to and from mobile node? **(Dec. 18, 5 Marks)**

Consider data transmission between CN and MN. There are four scenarios.

1. CN is a fixed node and data is to be transferred from CN to MN.
2. CN is a fixed node and data is to be transferred from MN to CN.
3. CN is a mobile node and data is to be transferred from CN to MN.
4. CN is a mobile node and data is to be transferred from MN to CN.

Fig. 3.3.2 shows the packet delivery to and from MN.

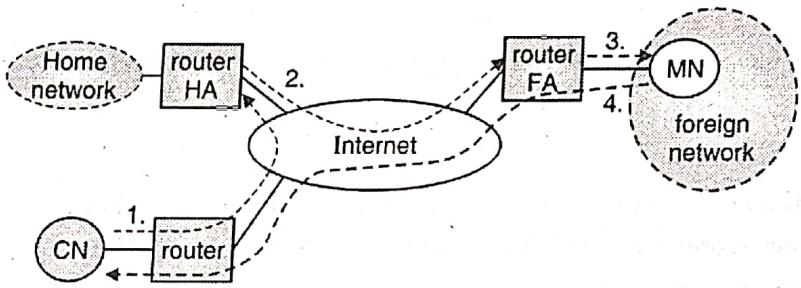


Fig. 3.3.2 : Packet delivery to and from the mobile node

(a) Data transfer from Fixed CN to MN

Step 1 : When the CN wants to send an IP packet to the MN, the CN doesn't know about the MN's current location and sends the packet to the IP address of MN. Here, the source address of the packet is CN's IP address and the destination address is MN's original IP address.

Step 2 : The packet is routed via the standard routing mechanism of the Internet to the router responsible for MN's home network. The home network's router implements the HA.

Step 3 : The HA now detects that the MN is currently not in its home network. Instead of forwarding the packet into the subnet as usual, the packet is encapsulated and is tunneled to the COA of the MN. A new header is added in front of the old IP header indicating MN's COA as the new destination and HA as the source of the encapsulated packet.

Step 4 : FA now decapsulates the packet and forwards the original packet with CN as source and MN as destination.

(b) Data transfer from MN to fixed CN

Step 1 : The packet is sent by the MN with its original IP address as the sender and the CN's IP address as the receiver.

Step 2 : The FA responsible for the foreign network acts as a default router and forwards the packet to the router responsible for the CN (The router is located in CN's home network).

Step 3 : The router responsible for CN then forwards the packet to CN.

(c) Data transfer from Mobile CN to the MN

Step 1 : The CN sends the packet with its original IP address as the source address and MN's original IP address as the destination address.

Step 2 : Since the CN is also in the visiting network, the FA responsible for the CN sends the packet to the router responsible for the home network of MN.

Step 3 : The HA of MN realizes that the MN is not in the home network. It then encapsulate the received packet and forwards it to the COA with source address as HA's IP address and the destination address as COA.

Step 4 : The foreign agent (FA) of the MN receives this packet, decapsulates it and forwards it to the MN.

(d) Data transfer from MN to a mobile CN

Step 1 : The MN sends the packet as usual with its own fixed IP address as a source address and CN's address as destination.

Step 2 : The foreign agent (FA) router responsible for MN sends this packet to the home network of the CN.

Step 3 : The HA responsible for CN receives the packet and realizes that the CN is not in the home network and hence tunnel the packet towards COA of the CN.

Step 4 : The FA responsible for CN receives the packet, decapsulates it and forwards it to the CN.

Some additional mechanisms are needed for mobile IP to work. The following section discusses about these enhancements.

3.3.3 Agent Advertisement and Discovery

MU - May 18

Q. Explain agent advertisement and discovery registration in mobile networks. **(May 18, 5 Marks)**

- When a mobile node is first turned on, it can either be in its home network or a foreign network.
- Hence, the first thing that it must do is to determine where it is, and if it is not at home, must begin the process of setting up datagram forwarding from its home network to the current location.
- This process is accomplished by communicating with a local router serving as an agent (FA), through the process called *agent discovery*.
- Agent discovery process makes it possible for an MN to determine :
  - Whether it is connected to its home network or to a foreign network.
  - Whether it has changed its position.
  - To obtain a COA when it changes to a different foreign network.

After moving to another network one initial problem is how to find a foreign agent. For this purpose, mobile IP describes two messages: ***Agent Advertisement*** and ***Agent Solicitation***.

3.3.3(a) Agent Advertisement

MU – Dec. 15, Dec. 17

Q. Explain Agent advertisement in Mobile IP. **(Dec. 15, 5 Marks)**

Q. How the agent could be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. **(Dec. 17, 10 Marks)**

- How does a mobile node make out that it has changed network recently? This is achieved by messages from home agents and foreign agents.
- Home agents and foreign agents advertise their presence and services using messages called ***agent advertisement***.
- Agent advertisement messages are periodically broadcast and contain the following details
  - List of COAs available for the MN.
  - Special features and services provided by FA such as different types of encapsulation available. For example, minimal encapsulation or generic encapsulation.
  - Allows MN to detect the network number and congestion details of a link to the Internet.

- For agent advertisement ICMP messages with some mobility extension are used. The agent advertisement packet is shown in Fig. 3.3.3.

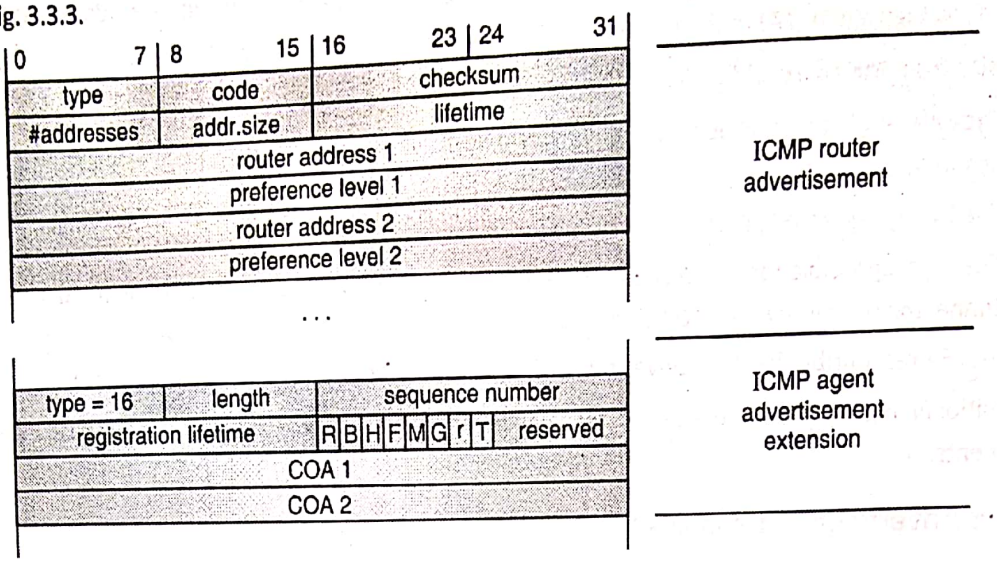


Fig. 3.3.3 : Agent advertisement message

- The various fields of ICMP part of the packet are :
  - **Type :** It is set to 9 for ICMP.
  - **Code :** Set to 0, if the agent also routes traffic from non-mobile node. And set to 16 if the agent only routes mobile traffic.
  - **#addresses :** Indicates the number of addresses advertised with this packet. The actual addresses follow as shown in Fig. 3.3.3.
  - **Lifetime :** Denotes the length of time for which the advertisement is valid
  - **Preference level :** Preference for each router address is specified. It helps a node to choose the router. The chosen router will act as an FA for the MN.
- The various fields of mobility extension part are :
  - **Type :** It is set to 16 for routing only mobile packets.
  - **Length :** Length depends on the number of COAs provided with the message and it is equal to 6 + 4 * (number of addresses).
  - **Sequence number :** It indicates the total number of advertisements set since initialization.
  - **Registration lifetime :** Specifies the maximum lifetime in seconds a node can request during registration.
- The following bits specify the characteristics of an agent :
  - **R bit :** It is the registration bit and indicates if a registration with this agent is required even when using co-located COA at the MN.
  - **B bit :** This bit is set if the agent is currently too busy to accept new registration.
  - **H bit :** This bit is set if the agent offers services as a home agent.
  - **F bit :** This bit is set if the agent offers services as foreign agent on the link where the advertisement has been sent.
  - **M and G bit :** M and G bits specify the method of encapsulation used for the tunnel. M for minimal encapsulation and G for generic routing encapsulation.
  - **r bit :** This is reserved and set to zero.
  - **T bit :** It indicates that reverse tunnelling is supported by the FA.

3.3.3(b) Agent Solicitation

Q. Explain Agent advertisement in Mobile IP. **MU – Dec. 15, Dec. 17**

Q. How the agent could be discovered using Mobile IP? Give the overlay of agent advertisement packet which includes mobility extension. **(Dec. 15, 5 Marks)** **(Dec. 17, 10 Marks)**

- Agent solicitation messages are sent by MN itself to search an FA in one of the following conditions.
  - When no agent advertisements are present or
  - The inter-arrival time of advertisement message is too high or,
  - An MN has not received a COA by other means.
- To reduce the congestion on the link the MN can send out three solicitations, per second, as soon as it enters a new network.
- Any agent that receives the solicitation message, transmits a single agent advertisement in response. If a node does not receive an answer to its solicitations, it must decrease the rate of solicitations exponentially to avoid flooding the network.
- After these steps of advertisements and solicitations, the MN can now receive COA, either one for an FA or a co-located COA.
- Now the next step is, the MN has to register with the HA if the MN is in a foreign network.

3.3.4 Registration

Q. Explain registration with respect to mobile IP. **MU – Dec. 13** **(Dec. 13, 5 Marks)**

- After agent discovery is done by a mobile node, it knows whether it is in its home network or in a foreign network. If it is in its home network, it communicates like a regular IP device, but if it has moved to a foreign network, it must activate Mobile IP.
- For activating Mobile IP, a process called home agent registration, or simply registration is used. For registration, the MN exchanges information and instructions with the home agent. The main purpose of registration is to get the Mobile IP working. The mobile node must inform the home that it is on a foreign network so that all datagrams must be forwarded to its foreign network.
- It also must inform the home agent about its care of address (COA) so the home agent can send the forwarded datagrams appropriately.
- When registration is performed, the home agent, in turn, needs to communicate various types of information back to the mobile node.
- Registration can be done in two different ways depending on the location of the COA.

1. **COA at the FA :** In this case, registration is done as shown in Fig. 3.3.4.
   - The MN sends its registration request to the FA (containing COA).
   - The FA forwards the request to the HA.
   - The HA now setup a mobility binding containing the mobile node's home IP address, the current COA and the lifetime of the registration.
   - The registration expires automatically after the lifetime and is deleted. So the MN should reregister before expiration.
   - After mobility binding, the HA sends reply message back to the FA which forwards it to MN.

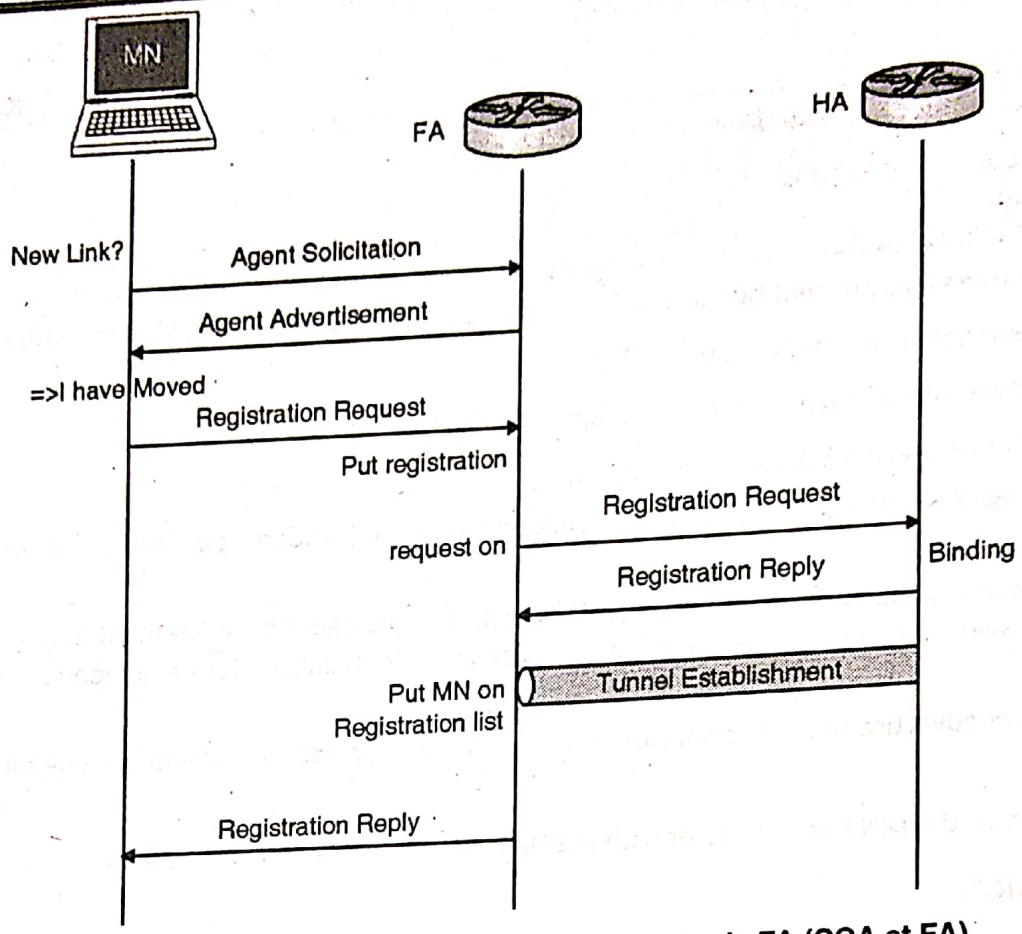


Fig. 3.3.4 : Registration procedure of mobile node via FA (COA at FA)

2. **COA is co-located :** In this case, the registration is very simple and shown in Fig. 3.3.5

– The MN may send registration request directly to the HA and vice versa.

– If the MN received an agent advertisement from the FA, it should register via this FA if the R bit is set in the advertisement.

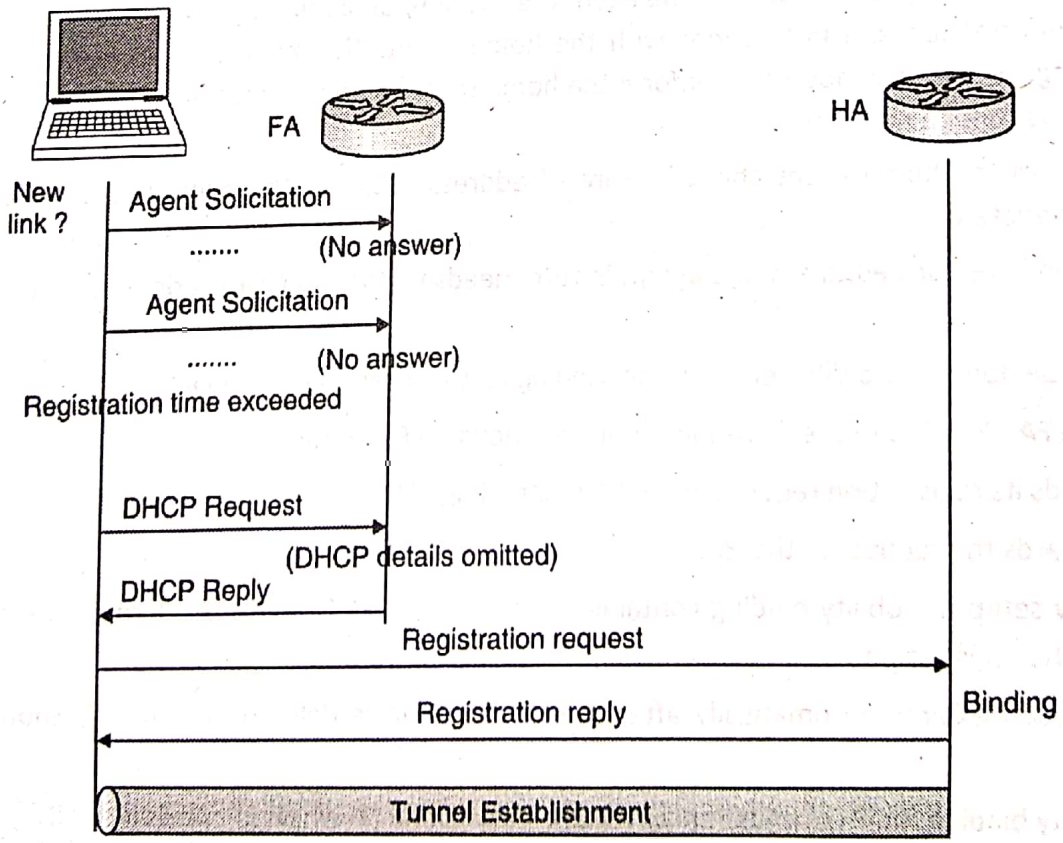


Fig. 3.3.5 : Registration procedure of mobile node via HA (Co- located COA)

1. Registration request message

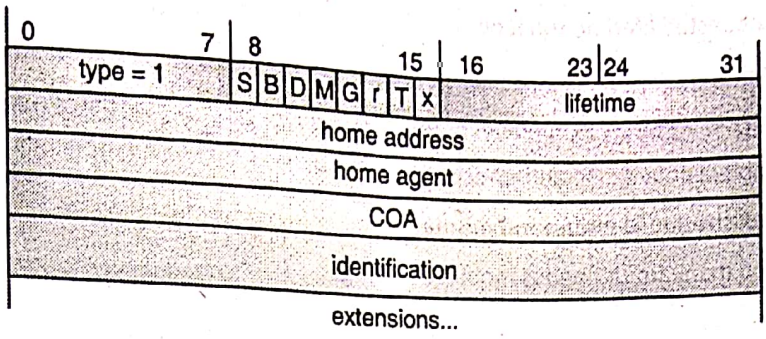


Fig. 3.3.6 : Registration request message

The registration request message is shown in Fig. 3.3.6 and various fields are described as follows :

- **Type :** It is set to 1 for registration request.
- **S bit :** If set, indicates that the MN also wants the FA to retain priority binding.
- **B bit :** If set, indicates that an MN also wants to receive the broadcast packets which have been received by the HA in home network.
- **D bit :** If set, it indicates that the de-capsulation of packets is performed by the MN.
- **Lifetime :** Denotes the validity of the registration in seconds.
- **Home address :** The home address is the fixed IP address of the MN.
- **Home agent :** It is the IP address of the home agent.
- **Identifications :** 64 bit identification is generated by MN to identify a request and match it with registration replies.

2. Registration reply message

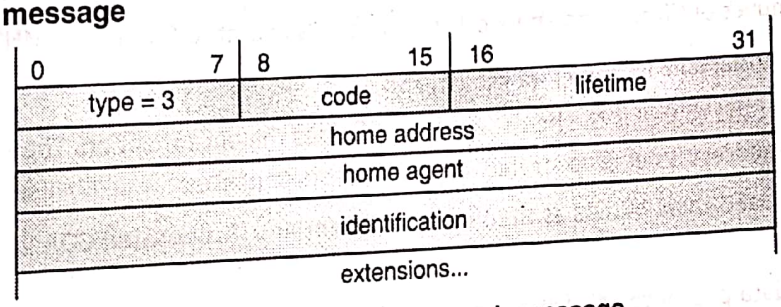


Fig. 3.3.7 : Registration reply message

The registration reply message is shown in Fig. 3.3.7 and various fields are described as follows :

- **Type :** It is set to 3.
- **Code :** Code indicates the result of the registration request. It specifies whether the registration request was successful or denied by the HA, or denied by the FA.

Example codes are :

- Registration successful
  - Code = 0; registration is accepted
  - Code =1; registration is accepted, but simultaneous mobility bindings unsupported
- Registration denied by FA
  - Code = 65; administratively prohibited
  - Code = 66; insufficient resources
  - Code = 67; mobile node failed authentication

- Code = 68; home agent failed authentication
- Code = 69; requested lifetime too long

– Registration denied by HA

- Code = 129; administratively prohibited
- Code = 131; mobile node failed authentication
- Code = 133; registration identification mismatch
- Code = 135; too many simultaneous mobility bindings

Extensions

It contains the parameters for authentication and may also contain other information as required.

3.3.5 Tunnelling and Encapsulation

MU – May 12, Dec. 13, May 14, May 15, Dec. 15, May 16, May 17, Dec. 17

Q. Explain how tunnelling works for mobile IP using IP-in-IP, minimal and generic routing encapsulation respectively. Discuss the advantages and disadvantages of these three methods. **(May 12, 10 Marks)**

Q. Explain encapsulation with respect to mobile IP. **(Dec. 13, 5 Marks)**

Q. Describe tunnelling and encapsulation in Mobile IP. **(May 14, 5 Marks)**

Q. Why is Mobile IP packet required to be forwarded through a tunnel ? **(May 15, 5 Marks)**

Q. Why is mobile IP packet required to be forwarded through tunnel? Explain minimal and generic technique of encapsulation of mobile IP. **(May 15, Dec. 15, May 16, May 17, 10 Marks)**

Q. Discuss how tunnelling work for mobile IP using IP-In-IP encapsulation. **(Dec. 17, 5 Marks)**

What is tunneling ?

– When a mobile node moves out from home network, the HA sends packet to COA of the MN via a tunnel.

– A tunnel establishes a virtual pipe for data packet.

– In Mobile IP, the start of the tunnel is the home agent, which does the encapsulation. The end of the tunnel depends on what sort of care of address is being used which decapsulates data packet.

– If foreign agent COA is used then FA acts as the tunnel end point and if co-located COA is used then MN acts as the tunnel end point.

– If a CN wants to send data packet to MN (currently not in home network) the data packet is first encapsulated at HA and sent via a tunnel and then decapsulated at FA and finally forwarded to the MN.

– The encapsulation process is shown in the Fig. 3.3.8.

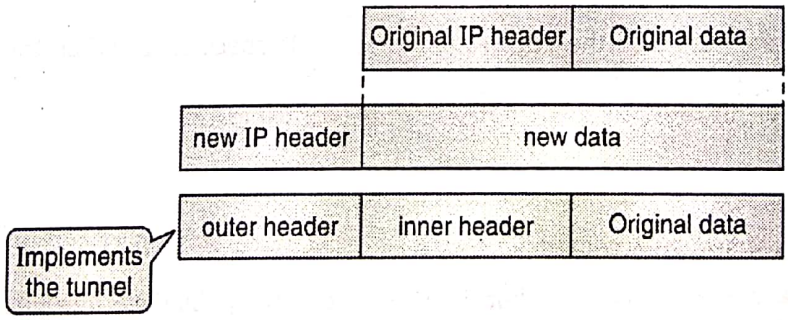


Fig. 3.3.8 : IP encapsulation

- **Encapsulation** means putting a packet made up of a packet header and data into the data field of a new packet.
- **Decapsulation** is the reverse process of encapsulation, that is removing the packet from the data part of another packet.

- The disadvantages of encapsulation are :
  - Packet size is larger than the original packet.
  - Encapsulation can be done only when there is an entity at the tunnel end that decapsulates the IP datagram.
  - After a CN's IP datagrams are captured, datagrams tunneled to the FA for delivery to the MN. The tunneling can be done by one of three encapsulation techniques. These are discussed below.

Why Tunneling is required?

Why does the Mobile IP packet required to be forwarded through a tunnel ?

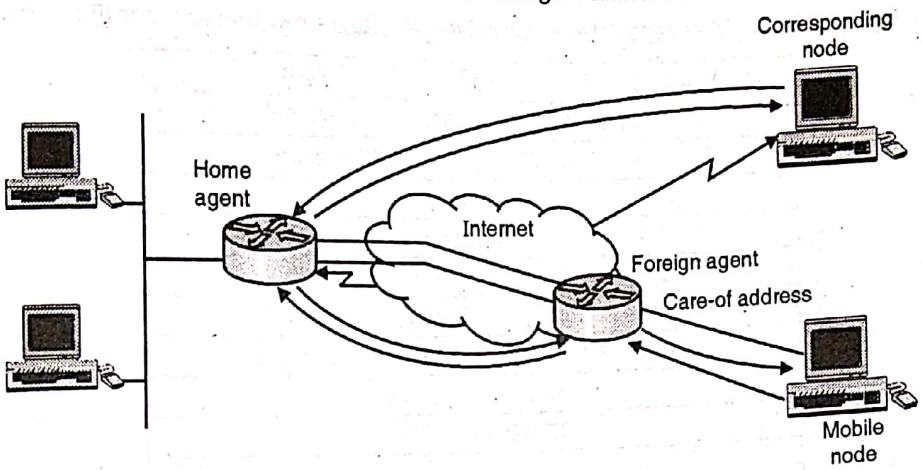


Fig. 3.3.9 : Mobile IP

- Consider a situation when a Correspondent Node (CN) wants to send an IP packet to a Mobile Node (MN). All the CN knows about this MN is, its IP address.
- The CN is totally unaware of the MN's location and so sends it as usual to MN's IP address.
- The internet, routes this packet to the Home router of the MN also called as Home Agent (HA).
- The HA now knowing that the MN is not in its home network encapsulates and tunnels the packet to the COA.
- The Care-of-address (COA) defines the current location of the MN from an IP point of view.
- Since internet routes are created based on the header contents of an IP packet, to route it from HA to COA, we need a new header for the packet to be transmitted.
- The new header on top of the original header is made (Fig. 3.3.10). Now this will enable us to set a new direct route (a tunnel) to the MN from the HA as it is roaming.

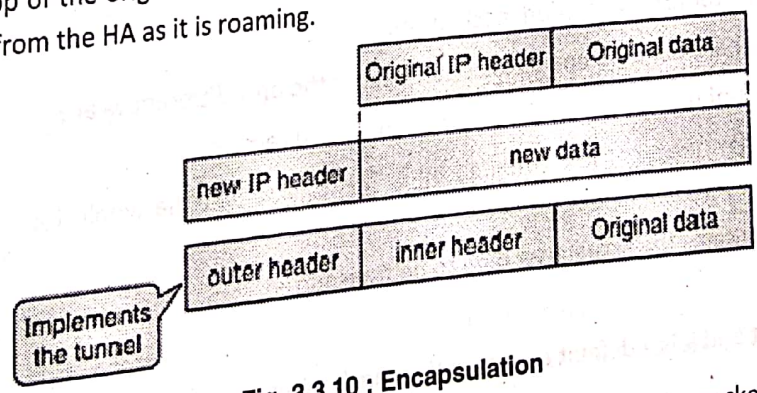


Fig. 3.3.10 : Encapsulation

Thus tunnelling is the process of creating a tunnel by the HA to the COA to route packets to the Mobile Node as it roams. It establishes a pipe (a data stream between two connected ends) wherein the data is inserted and moves in FIFO order.

3.3.5(a) IP-in-IP Encapsulation

MU - May 16, Dec. 17

Q. Explain IP-in-IP technique of encapsulation of mobile IP. **(May 16, 5 Marks)**

Q. Discuss how tunneling work for mobile IP using IP-In-IP encapsulation. **(Dec. 17, 5 Marks)**

- IP-in-IP encapsulation is defined in RFC 2003. It is the simplest approach and must always be supported.
- In this type of encapsulation, the entire IP datagram sent by the internet host is inserted in a new IP datagram as the payload.
- As shown in the Fig. 3.3.11 the HA encapsulates the received IP datagram within another IP datagram.

ver.	IHL	DS(TOS)	length	
IP identification			flags	fragment offset
TTL		IP-in-IP	IP checksum	
IP address of HA				
Care-of address COA				
ver.	IHL	DS(TOS)	length	
IP identification			flags	fragment offset
TTL		lay. 4 prot.	IP checksum	
IP address of CN				
IP address of MN				
TCP/UDP/ ...payload				

Fig. 3.3.11 : IP-in-IP encapsulation

The various fields in the outer header are :

1. **ver. (Version) :** Version field denotes the version number and set to 4 for IPv4.
2. **IHL (Internet header length) :** IHL indicates the length of the outer header.
3. **DS (TOS) :** It is just copied from the inner header.
4. **Length :** It denotes the complete length of the encapsulated packet.
5. **TTL (time to live) :** It indicates the period of validity of the packet. TTL should be high enough so the packet can reach the tunnel endpoint.
6. **IP-in-IP :** This denotes the type of protocol used in the IP payload.
7. **IP checksum :** This is used for error detection mechanism.

The fields of inner header are almost same as the outer header the only differences are :

- The address fields consist of the address of the original sender and receiver.
- The TTL value of the inner header is decremented by 1. This means that the whole tunnel considered a single hop from the original packet's point of view.

The TCP/UDP payload contains the actual user data to be transmitted.

Advantage

It is simple to implement and it is a default encapsulation mechanism.

Disadvantage

Most of the outer header fields are same as inner header so this method increases redundancy.

3.3.5(b) Minimal Encapsulation

Q. Explain minimal encapsulation. Also discuss merits and demerits. **MU – May 12, May 15, May 17**
Q. Explain minimal techniques of encapsulation of Mobile IP packet. **(May 12, 5 Marks)** **(May 15, May 17, 5 Marks)**

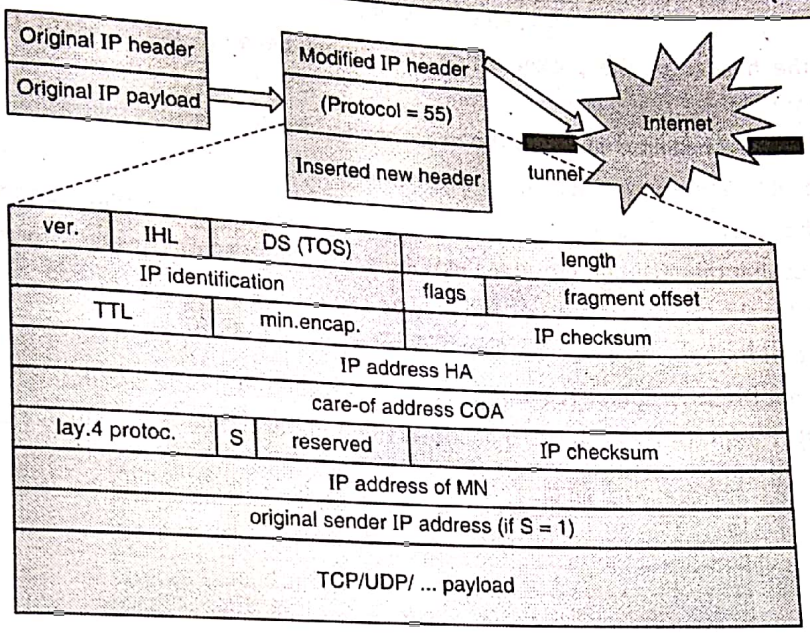


Fig. 3.3.12 : Minimal encapsulation

- Minimal encapsulation is defined in RFC 2004. It involves fewer fields in IP packet. It can be used if the HA, MN, and FA all agree to use. Fig. 3.3.12 shows the minimal encapsulation.
- The outer header fields are almost same as for IP encapsulation; the only difference is in the **Type** field. It is set to 55.
- The inner header is much smaller than IP encapsulation packet.
- The **S bit** indicates whether the original sender's IP address is included in the header or not. Value 0 indicates sender's IP address can be omitted.
- **Advantage :** Lower overhead as compared to IP-in-IP encapsulation as it avoids redundancy.
- **Disadvantage :** It does not support fragmentation to deal with tunnel with smaller path maximum transmission units (MTU).

3.3.5(c) Generic Routing Encapsulation (GRE)

Q. Explain Generic encapsulation. Also discuss merits and demerits. **MU – May 12, Dec. 15**
Q. Explain Generic technique of encapsulation of mobile IP. **(May 12, 5 Marks)** **(Dec. 15, 10 Marks)**

- GRE is defined in RFC 1701.
- It is a generic encapsulation mechanism developed before the development of mobile IP.
- GRE allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.
- Fig. 3.3.13 shows the generic routing encapsulation. The GRE header is prepended to the packet of one protocol suite with the original header and data.

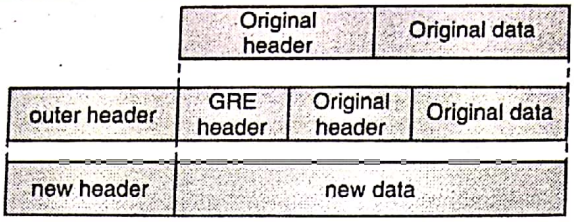


Fig. 3.3.13 : Generic routing encapsulation

Fig. 3.3.13 shows the header of the packet inside the tunnel between home agent (HA) and COA using GRE encapsulation.

The various fields of the GRE header that follow the outer header are described as follows :

1. **Protocol type :** Protocol type is set to 47 for GRE encapsulation.
2. **C bit :** If C bit is set, the checksum field contains the valid IP checksum of the GRE header and the payload.
3. **R bit :** If set, it indicates that the offset and routing fields are present and contains valid information.
4. **K bit :** If it is set, indicates the key field is present and may be used for authentication.
5. **S bit :** If set, indicates that the sequence number field is present.
6. **s bit :** If set, indicates that the strict source routing is used.
7. **rec. (recursion control) :** It represents a counter that shows the number of allowed recursive encapsulations.

ver.	IHL	DS(TOS)	length				
IP identification			flags	fragment offset			
TTL		GRE	IP checksum				
IP address of HA							
Care-of address COA							
C	R	K	S	s	rec.	rsv.	ver.	protocol
checksum (optional)								offset (optional)
key (optional)								
sequence number (optional)								
routing (optional)								
ver.	IHL	DS(TOS)	length				
IP identification			flags	fragment offset			
TTL		lay. 4 prot.	IP checksum				
IP address of CN							
IP address of MN							
TCP/UDP/ ...payload							

Fig. 3.3.14 : Generic routing encapsulation

8. **rev. (reserved) :** This field is reserved for future used and must be set to 0.
9. **ver. (version) :** It is set to **0** for the GRE version.
10. **Protocol :** Indicates the protocol used by the packet following the GRE header.
11. **Checksum :** Contains a valid IP checksum of the GRE header and the payload (present only when C bit is set).
12. **Offset :** It represents the offset in bytes for the first source routing entry (present only when R bit is set).
13. **Key :** Contains a key that can be used for authentication (present only when K bit is set).
14. **Routing :** It is a variable length field and contains the fields for source routing.

Advantage

- GRE supports other network layer protocols in addition to IP.
- It allows more than one level of encapsulation.

3.3.5(d) Optimization

Q. What is triangular routing problem? How do you optimize mobile IP for avoiding triangular routing ? **MU – May 18**

Q. Why and how can optimization in Mobile IP be achieved. **(May 18, 5 Marks)**

Triangular routing

- As discussed in section 3.3.2, the IP packet from a CN destined to an MN needs to be routed to its HA first and then tunneled to the foreign agent of the MN and IP packet from the MN can be directly routed to the CN.
- If the CN and MN are very near, then also the IP packet has to travel a long way to reach the MN. This inefficient behavior of a non optimized mobile IP is called ***Triangular Routing***.
- The triangle is made of the three segments, CN to HA, HA to COA/MN, and MN back to CN. (Refer Fig. 3.3.15)

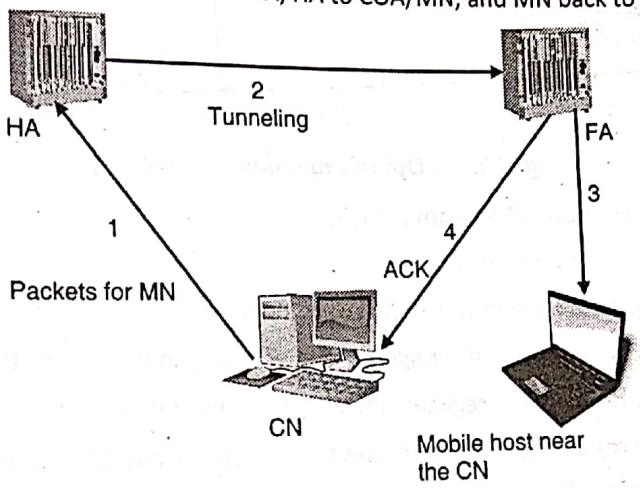


Fig. 3.3.15 : Triangular Routing

Route optimization to avoid triangular routing

To solve triangular routing problem, a route optimization protocol has been introduced. Basically this protocol defines some message so as to inform CN of an up to date location of MN. Once the current location of the MN is known, the CN itself performs tunneling and sends packet directly to MN.

The optimized mobile IP protocol needs four additional messages; these are :

1. **Binding request**

   If a node wants to know where the MN is currently located, it can send a binding request to the HA.

2. **Binding update**

   The HA sends a binding update to the CN and informs the CN the current location of an MN. The binding update can request an acknowledgement.

3. **Binding acknowledgement**

   On request, after receiving a binding update message, a node returns a binding acknowledgement.

4. **Binding warnings**

   - A binding warning message is sent by a node if it decapsulates a packet for an MN but it is not the FA for that MN currently.
   - If CN receives the binding warning, it requests the HA for a new binding update.
   - If the HA receives the warning it directly sends a binding update to the CN.

The Fig. 3.3.16 explains the four messages together with the case of an MN changing its FA and shows the exchange of messages in optimization protocol.

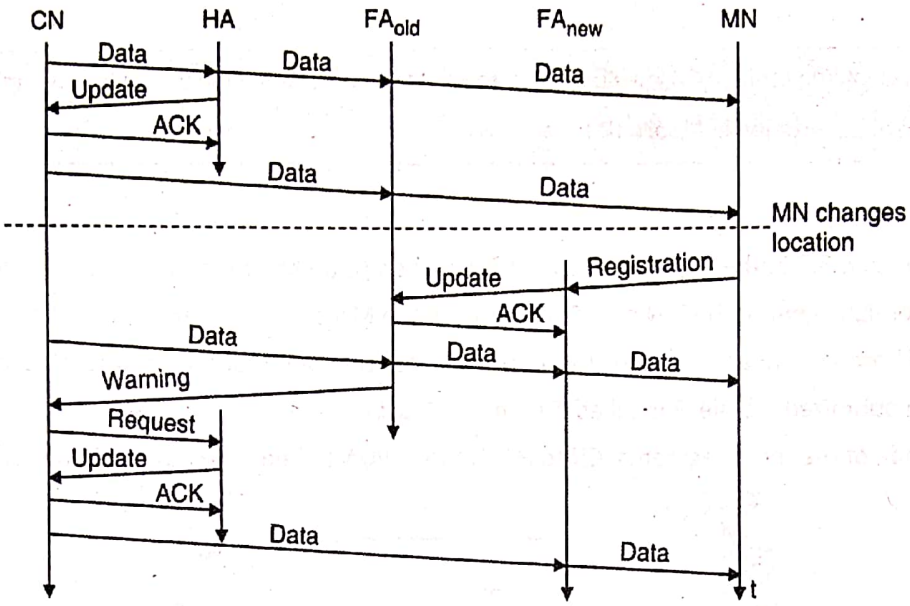


Fig. 3.3.16 : Optimized mobile IP working

- The CN requests the current location of MN from the HA.
- HA returns the COA of the MN via update message.
- CN acknowledge this updated message and stores mobility binding.
- Now CN can send data directly to the current foreign agent FA_{old}. FA_{old} now forwards these data to MN.
- The MN might now change its location and register with a new foreign agent FA_{new}.
- FA_{new} informs FA_{old} about new registration of MN via an update message and FA_{old} acknowledged this update message.
- CN doesn't know about the current location of MN, it still tunnels its packets for MN to the old foreign agent FA_{old}.
- The FA_{old} notices packets destined to MN but also knows MN currently not in current FA.
- FA_{old} might now forward these packets to the new COA of MN which is new foreign agent.
- Thus the packets that are in transit are not lost. This behavior is another optimization to basic mobile IP and provides smooth handover.
- FA_{old} sends binding warning message to CN. CN then requests a binding update.
- The HA sends an update to inform the CN about the new location, which is acknowledged. Now, CN can send data directly to FA_{new}, and avoid triangular binding.
- However, the optimization will not work if the MN does not want to reveal its current location to the CN because of security.

3.3.6 Reverse Tunnelling

- There may be a situation where it is not feasible or desired to have the mobile node (MN) send packets directly to the internetwork via FA.
- In that case, an optional feature called **reverse tunneling** is used if it is supported by mobile node, home agent and foreign agent.
- As shown in Fig. 3.3.17 , a reverse tunnel is setup between MN and HA (If COA is co-located), or between FA and HA (if FA acts as COA)
- All transmission from MN are now tunneled back to the home network where HA transmits them over the Internet.

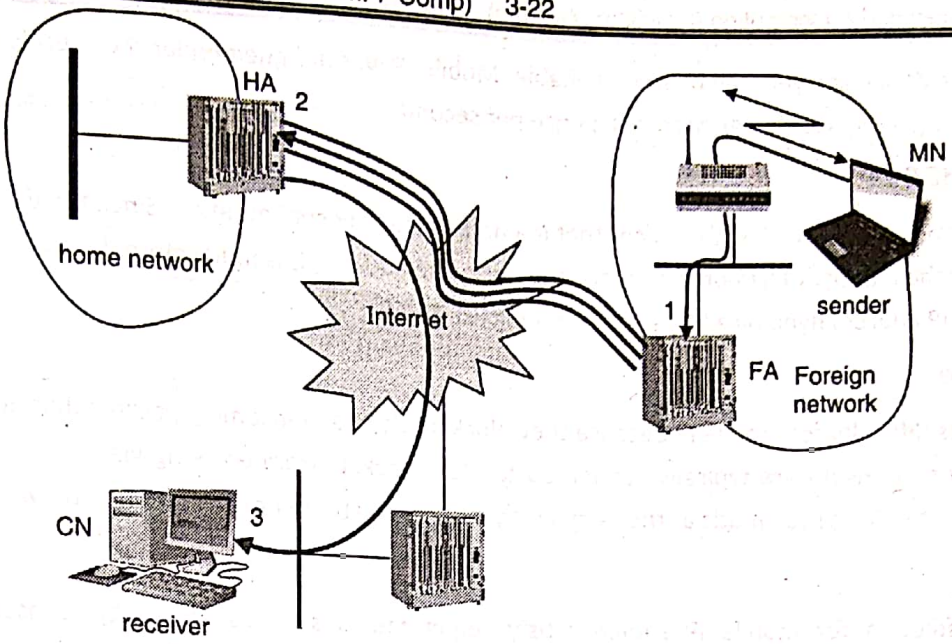


Fig. 3.3.17 : Reverse tunneling

Reverse tunneling is used in following scenario.

1. **Ingress Filtering/Firewalls**
   - If the network where mobile node located has implemented certain security measures that prohibits the node from sending packets using its normal IP address.
   - With a reverse tunnel the packet is first encapsulated by FA and sent to the HA.
2. **Multi-cast**

   Reverse tunneling is required for multicasting where the nodes in multicast group are in the home network, as an MN in a foreign network cannot transmit multicast packets directly in this case, as the foreign network might not provide the technical infrastructure for multicast communication.
3. **TTL (time to live)**
   - When an MN is in home network, and if MN node moves to a foreign network, its TTL might be too low for the packets to reach the same node as before.
   - A reverse tunnel is needed that represents one hop transmission.

Problems with reverse tunneling

- Reverse tunneling may cause a triangular routing problem in the reverse direction. All packets from MN to CN now go through the HA. The CN might not be able to decapsulate the packet as the CN could be a non Mobile IP device, so the RFC 3024 does not offer solution to this reverse triangular routing.
- Reverse tunneling may raise some security issues. For example, a tunnel which starts in the private network of a company and reaching out into the internet could be hijacked and abused for sending packets through firewall.
- Reverse tunneling may also introduce the possibility of denial-of-service attack.

3.3.7 Limitations of Mobile IP

1. **Frequent Mobility**

   Mobile IP was designed to handle mobility of devices, but only relatively infrequent mobility. This is due to the work involved with each change. This overhead isn't a big deal when you move a computer once a week, a day or even an hour. It can be an issue for "real-time" mobility such as roaming in a wireless network, where hand-off functions

operating at the data link layer may be more suitable. Mobile IP was designed under the specific assumption that the attachment point would not change more than once per second.

2. Issue with DHCP

Mobile IP is intended to be used with devices that maintain a static IP configuration. Since the device needs to be able to always know the identity of its home network and normal IP address, it is much more difficult to use it with a device that obtains an IP address dynamically, using something like DHCP.

3. Security Issue

Firewalls, causes difficulty for mobile IP because they block all classes of incoming packets that do not meet specified criteria. Enterprise firewalls are typically configured to block packets from entering via the internet. In many cases authentication with FA is problematic as the FA typically belongs to another organization or network.

4. QoS Issue

- The QoS solution for mobile IP should satisfy requirements such as scalability, conservation of wireless bandwidth, low processing overhead, authorization and accounting etc.
- When handover occurs in mobile IP environment, some applications such as web browser and file transfer using TCP connection will face disconnection or a degradation of the performance.
- Another problem is with the tunnel based communication. In tunnel based communications different data flows addressed to the same IP address are treated in the same manner. Thus tunneling makes it hard to give a flow of packets a special treatment needed for QoS.

3.3.8 Mobile IP and IPv6

- **Ipv4 :** The network layer protocol in the TCP/IP protocol suite is currently IPv4. IPv4 provides the host-to-host communication between systems in the Internet. IPv4 has some deficiencies that make it unsuitable for the fast growing Internet, including the following:
  - Despite all short term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long term problem in Internet.
  - The Internet must accommodate real time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided by IPv4 design.
  - The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.
- **Ipv6 :** To overcome these problems, IPv6 also known as IPng (Internet Protocol next generation) was proposed. In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet.
  - The format and the length of the IP addresses were changed along with the packet format
  - Related protocols such as ICMP were also modified.
  - Other protocols in the network layer, such as ARP, RARP, IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes.

The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

- Larger address space-An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address, this is huge increase in address space.
- Better Header format-IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.
- New Options-IPv6 has new options to allow for additional functionalities.
- Allowance for extension-IPv6 is designed to allow the extension of protocol if required by new technologies or applications.
- Support for resource allocation-In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.
- Support for more security-The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto configuration and neighbor discovery enables every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.
- The MN is now able to :
  - Decapsulates the packets
  - To detect when it needs a new COA and
  - To determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

3.4 Routing

- Routing in wireless ad-hoc networks is different and complicated than wired networks or wireless networks with infrastructure. This difference can be explained by example shown in Fig. 3.4.1.
- Fig. 3.4.1 shows the network topology at two different time t_1 and t_2.
- Seven nodes are connected depending upon the current transmission characteristics between them.
- At time t_1 node N4 can receive N1 over a good link, but N1 receives N4 via a weak link. Links may not have the same characteristics in both directions.
- The situation may change at time t_2 N1 cannot receive N4 any longer, N4 can receive N1 via a weak link. Network topology is frequently changed in ad-hoc networks.

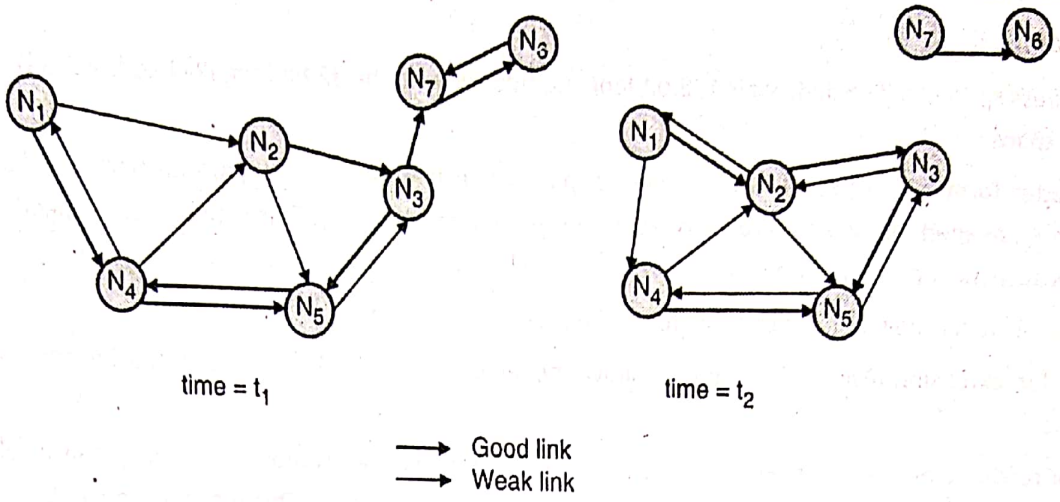


Fig. 3.4.1 : Ad-hoc network example

The main difference between ad-hoc and wired networks due to this routing in ad-hoc networks are different are as follows :

1. Asymmetric links

- Links are not symmetric in both directions as we have seen. Node N2 can receive N1 but N1 cannot receive signals from N2.
- Thus routing information collected for one direction is not useful for other direction.
- However many routing algorithms for wired networks rely on a symmetric scenario.

2. Redundant links

- Wired network have redundant link to survive link failure, but this redundancy is limited.
- In ad-hoc networks there might be many redundant links up to high complexity.
- Routing algorithms in wired network can handle up to some redundancy, but a large redundancy can cause a large computational overhead for routing table updates.

3. Interference

- In ad-hoc networks links comes and go depending on the transmission characteristics, one transmission may interfere with other, and nodes might overhear the transmissions of other nodes.
- Interference chances in wireless ad-hoc networks are very high.

4. Dynamic topology

- This is the greatest problem in routing for ad-hoc networks.
- Mobile nodes moves or medium characteristics might change frequently. This results frequent changes in topology as shown in Fig. 3.4.1 (at time=t_2). Due to change in topology, in ad-hoc networks the routing tables have to be updated frequently.

There are basically two classes of flat routing algorithms :

1. Table-Driven routing protocols (Proactive)

- These protocols are also called as proactive protocols since they maintain the routing information even before it is needed.
- Each and every node in the network maintains routing information to every other node in the network. Routes information is generally kept in the routing tables and is periodically updated as the network topology changes.
- Many of these routing protocols come from the link-state routing.

Examples of proactive routing protocols

- Destination Sequence Distance Vector (DSDV)
- Optimized Link State Routing (OLSR)
- Fisheye State Routing (FSR)
- Wireless Routing Protocol (WRP)

Advantage

- These protocols can give good real time traffic QoS.
- Route availability reduces delay (no route acquisition delay)

Disadvantage

- The proactive protocols are not suitable for larger networks, as they need to maintain node entries for each and every node in the routing table of every node. This causes more overhead in the routing table leading to consumption of more bandwidth.
- Possibly inefficient (due to unnecessary signaling message overhead)
- Redundant routes may exist
- Some computed routes may not be needed

2. On Demand routing protocols (Reactive)

- These protocols are also called reactive protocols since they don't maintain routing information or routing activity at the network nodes if there is no communication.
- If a node wants to send a packet to another node then this protocol searches for the route in an on-demand manner and establishes the connection in order to transmit and receive the packets.
- The route discovery usually occurs by flooding the route request packets throughout the network.

Examples of Reactive routing protocols

- Dynamic Source Routing (DSR)
- Ad-hoc On demand Distance Vector (AODV)

Advantage

- Eliminates periodic route advertisements
- May reduce power and bandwidth requirements.

Disadvantage

- Adds route-acquisition delay
- May cause more signaling if route expiration times are too short

3.4.1 Destination Sequence Distance Vector Routing (DSDV)

DSDV is a ***proactive table driven*** mobile ad-hoc network routing protocol. It is an enhancement of distance vector routing (Bellman Ford algorithm).

Problems with Distance Vector

- In Distance vector routing each node exchanges its routing table periodically with its neighbors.
- Each node uses its local information for creating its routing table.
- However, the local information may be old and invalid. This is because changes at one node in the network propagate

- However, the local information may be old and invalid. This is because changes at one node in the network propagate slowly through the network (step-by-step with every exchange). Thus the local information may not be updated promptly.
- This gives rise to loops. A message may loop around a cycle for a long time (count-to-infinity problem).
- Solutions used for this problem in wired networks such as poisoned reverse and split horizon do not work in case of ad-hoc networks due to the rapidly changing topology.

DSDV now adds two things to the distance vector algorithm.

1. Sequence numbers

- Each node advertise routing table with a sequence number.
- This sequence number used to distinguish stale route with the fresh route and help the nodes to process advertisements in correct order thus avoids loops that are likely in distance vector.

2. Damping

- It prevents temporary change in the network topology from destabilize the routing. These changes are of short duration only.
- When a node receives an advertisement containing a change in the current network topology, it waits for a certain time before forwarding the updates in routing table to other nodes.
- Waiting time depends on the time interval between the first and the best announcement of a path to a certain destination.

DSDV algorithm

- Each node maintains a routing table which stores
  - Next hop and cost metric towards each destination.
  - Also a sequence number that is created by the destination itself.
- In DSDV each node periodically forwards its own routing table to its neighbors. And each node increments and appends its sequence number when sending its local routing table.
- Each route is tagged with a sequence number, the routes with greater sequence numbers are preferred.
- Each node advertises a monotonically increasing even sequence number for itself.
- When a node finds that a route is broken, it increments the sequence number of the route and advertises it with infinite metric. Thus infinite metric indicates the route is broken.
- Destination advertises new sequence number.

Example

- Let S(X) be the destination sequence number for Z already present in X's routing table.
- Now say X receives information about route to Z with the destination sequence number S(Y) form node Y. Thus S(Y) is the destination sequence number sent from Y.
- X now compares S(X) and S(Y).
  - If S(X) > S(Y), then X ignores the routing information received from Y.
  - If S(X) = S(Y), and cost of going through Y is smaller than the route known to X, then X sets Y as the next hop to Z.
  - If S(X) < S(Y), then X sets Y as the next hop to Z, and S(X) is updated to equal S(Y).

Advantages of DSDV

- DSDV is an efficient protocol for route discovery. Whenever a route to a new destination is required, it already exists at the source.
- Hence, latency for route discovery is very low.
- DSDV also guarantees loop-free paths.

Disadvantages of DSDV

- However, DSDV needs to send a lot of control messages. These messages are important for maintaining the network topology at each node.
- This may generate high volume of traffic for high-density and highly mobile networks.
- Special care should be taken to reduce the number of control messages.

3.4.2 Dynamic Source Routing (DSR)

- DSR is a **reactive routing** protocol which is able to manage a MANET.
- DSR was specifically designed for use in **multi-hop wireless ad hoc networks** of mobile nodes.
- It uses an **on-demand** approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. This approach saves the bandwidth
- It uses **Source routing** for route discovery that is the source node determines the whole path from the source to the destination node and deposits the addresses of the intermediate nodes of the route in the packets.

DSR contains 2 phases

1. Route Discovery (find a path)
2. Route Maintenance (maintain a path)

1. Route Discovery

- A node only tries to discover a route to a destination if it has to send something to this destination and there is no known route.

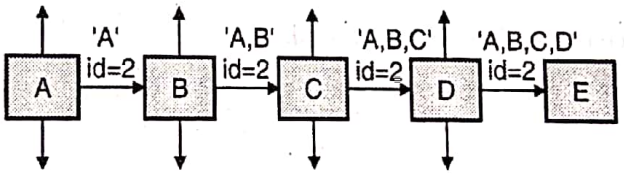


Fig. 3.4.2 : Route Discovery example

- If node A has in his Route Cache a route to the destination E, this route is immediately used. If not, the Route Discovery protocol is started :
  1. Node A (initiator) sends a Route Request packet by flooding the network
  2. If node B has recently seen another Route Request from the same target or if the address of node B is already listed in the Route Record, Then node B discards the request!
  3. If node B is the target of the Route Discovery, it returns a Route Reply to the initiator. The Route Reply contains a list of the "best" path from the initiator to the target. When the initiator receives this Route Reply, it caches this route in its Route Cache for use in sending subsequent packets to this destination.
  4. Otherwise node B isn't the target and it forwards the Route Request to his neighbors (except to the initiator).

2. Route Maintenance

- In DSR every node is responsible for confirming that the next hop in the Source Route receives the packet. Also each packet is only forwarded once by a node (hop-by-hop routing).
- If a packet can't be received by a node, it is retransmitted up to some maximum number of times until a confirmation is received from the next hop. Only if retransmission results then in a failure, a Route Error message is sent to the initiator that can remove that Source Route from its Route Cache. So the initiator can check his Route Cache for another route to the target.
- If there is no route in the cache, a Route Request packet is broadcasted.

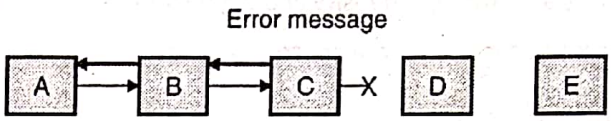


Fig. 3.4.3 : Route maintenance example

Example :

1. If node C does not receive an acknowledgement from node D after some number of requests, it returns a Route Error to the initiator A.
2. As soon as node receives the Route Error message, it deletes the broken-link-route from its cache. If A has another route to E, it sends the packet immediately using this new route.
3. Otherwise the initiator A is starting the Route Discovery process again.

Optimization to route discovery

To avoid too many broadcasts, that causes flooding of the network; every node has an counter and it is decremented each time the packet is broadcasted. Nodes can drop a request if the counter reaches zero.

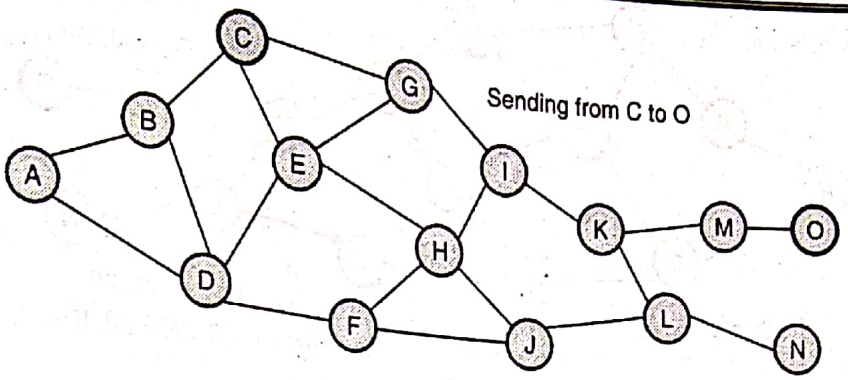
DSR Advantages

- Routes maintained only between nodes who need to communicate
- Reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead.
- A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.

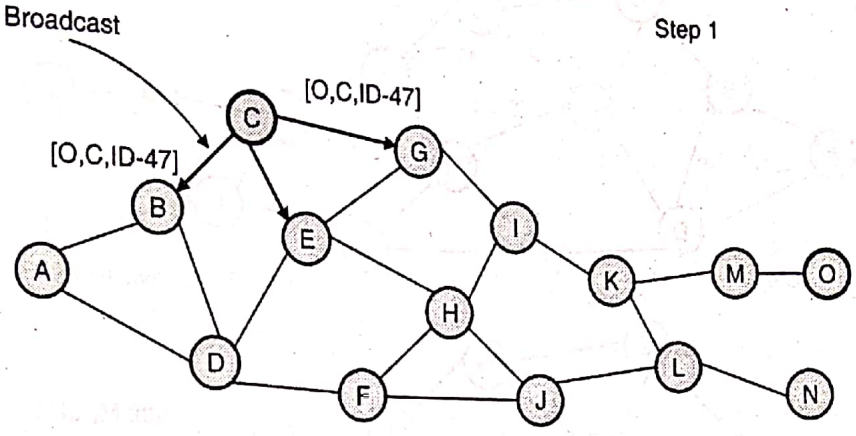
DSR Disadvantages

- Packet header size grows with route length due to source routing
- Flood of route requests may potentially reach all nodes in the network.
- Potential collisions between route requests propagated by neighboring nodes
  - Insertion of random delays before forwarding RREQ
  - Increased contention if too many route replies come back due to nodes replying using their local cache
  - Route Reply *Storm* problem
- Stale caches will lead to increased overhead

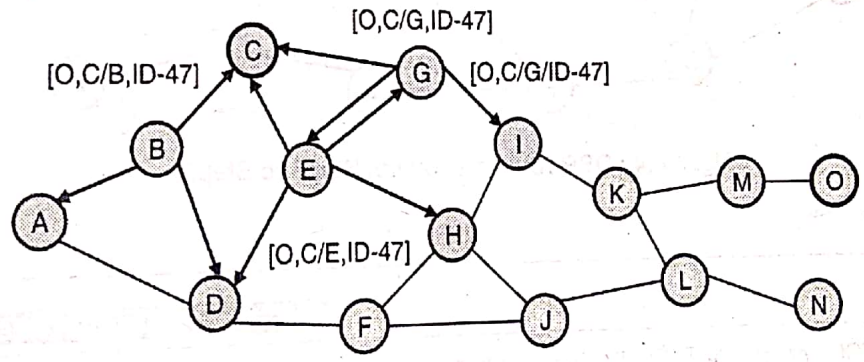
Example of DSR



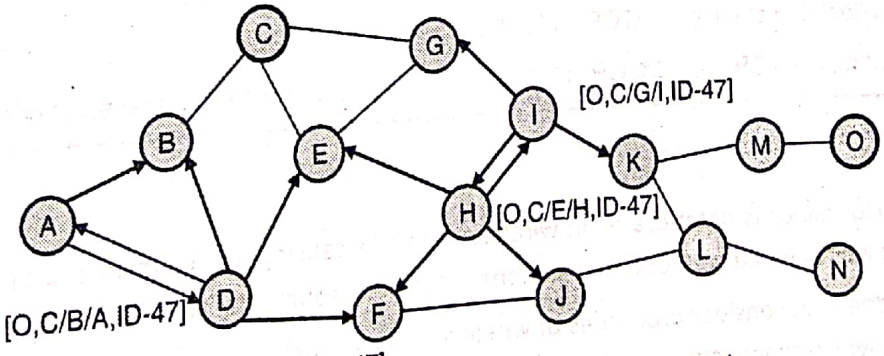
Step 1



Step 2



Step 3



Step 4

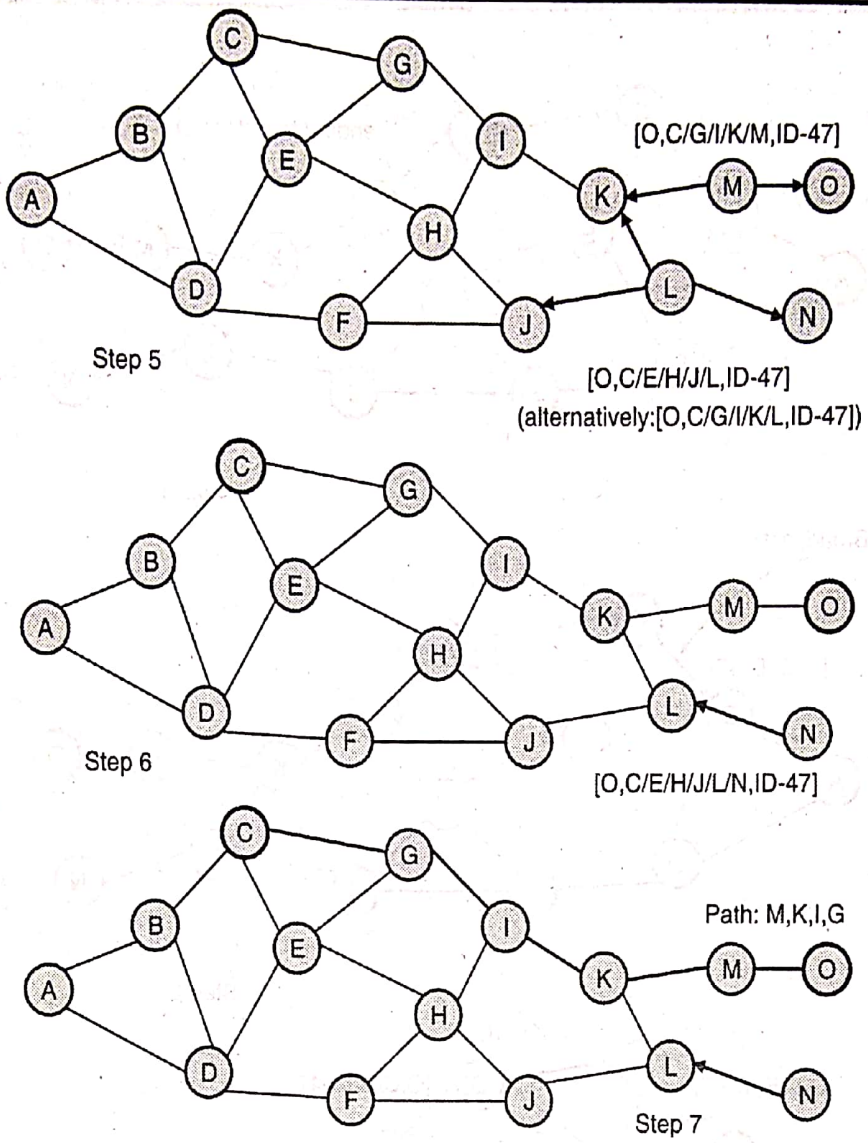


Fig. 3.4.4 : DSR route discovery, Step1 to Step7

3.5 Mobile TCP

MU – May 12, Dec. 12, Dec. 13, May 14, May 15

Q.	Explain snooping TCP and mobile TCP with their merits and demerits.	**(May 12, Dec. 13, 10 Marks)**
Q.	Discuss Mobile Transport Layer.	**(Dec. 12, 5 Marks)**
Q.	Explain merits and demerits of snooping TCP and indirect TCP?	**(May 14, 5 Marks)**
Q.	Explain the functioning of I-TCP and SNOOP -TCP, giving advantages and disadvantages of both.	**(May 15, 10 Marks)**

3.5.1 Traditional TCP

- Traditional TCP's performance is deteriorated in wireless networks causing many errors and disconnections as it was designed to perform well in wired networks and stationary node environments, and not in wireless networks.
- The traditional TCP does not consider properties of wireless network such as limited bandwidth, long latency, high bit error rate, and frequent disconnections and hence, does not guarantee reliable and efficient data transmission in wireless environment.
- TCP assumes that most of the packet losses in wired network are due to congestion. But in wireless environment, there could be many reasons for packet losses those need to be considered.

- The following section describes the traditional TCP designed for a wired network and also discusses the need for modification to the traditional TCP in order to use it efficiently in wireless networks.

1. Congestion Control

- TCP was originally designed for fixed networks with fixed end systems.
- Routers are responsible to transfer packets from source to destination.
- If a packet is lost in the wired network, the probable reason of that is congestion. Congestion is nothing but a temporary overload at some point in the transmission path, i.e. a state of congestion at a node.
- Each router maintains buffers for packets. If the sum of the packets' input rate destined for one output link exceeds the capacity of the output link, then the buffer becomes full and it cannot forward the packets fast enough, so the packets are dropped by the router.
- A dropped packet is lost and a gap is noticed by the receiver in the packet stream.
- The receiver continues to acknowledge all in-sequence packets up to the missing one.
- The receiver notices the missing acknowledgement of the lost packet and assumes a packet is lost due to congestion.
- Retransmitting the lost packet and continuing to send packets at full sending rate would only increase congestion.
- To reduce congestion, the transmission rate is slowed down considerably by TCP.
- All other TCP connections with the same problem follow the same process. By doing this, the congestion is resolved soon.
- This behavior of TCP during congestion is called **slow-start**.
- TCP ensures that even under heavy load the available bandwidth will be shared equally.

2. Slow start

- The behavior of TCP after detection of congestion is called slow start.
- It is used to resolve congestion quickly.

Slow-start working

- Sender calculates a congestion window for the receiver. The start size of window is one segment (TCP packet).
- The sender sends one packet and waits for an acknowledgement. If this acknowledgement arrives, the sender increases the congestion window by one. And now sends two packets (congestion window = 2).
- After arrival of two corresponding acknowledgements, the sender adds 2 in the congestion window, one for each acknowledgement.
- This scheme doubles the congestion window every time the acknowledgement arrives. This is called as an **exponential increase,** and it continues till a certain value called as **congestion threshold.**
- Once congestion window crosses the congestion threshold, further increase in transmission rate is linear i.e. congestion window is increased by one each time the acknowledgement is received.
- This linear increase continues till the sender detects the packet loss.
- Once the packet loss is detected; the sender sets the congestion threshold to half of its current congestion window and congestion window is set to one. The above steps are repeated again.

3. Fast retransmit/fast recovery

- The sender detects the loss of packets in two ways.
  - (i) If a time-out occurs at the receiver, in that case the sender activates normal slow start.
  - (ii) If the sender receives continuous acknowledgements for the same packet (Duplicate acknowledgements).

- If this is the case, then the sender can deduce two things - one is that the receiver got all packets up to the acknowledgement in sequence and second is that the receiver is continuously receiving something from the sender. Therefore, the packets must have been lost due to simple transmission error and not due to network congestion.
- The sender can now retransmit the missing packet(s) before the timer expires. This behavior is called as a **fast retransmit**.
- The receipt of an acknowledgements show 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 improves the efficiency of TCP dramatically.

4. Implication on mobility

There are many problems that degrade the performance of TCP.

Transmission errors

TCP assumes congestion if packets are dropped. This is not always true for wireless networks, where often, packet loss is due to transmission errors.

Mobility (i.e. handoff)

Mobility (i.e. handoff) itself can cause packet loss, if e.g. a mobile node roams from one access point (e.g. foreign agent in Mobile IP) to another while there are still packets in transit to the wrong access point and forwarding is not possible.

High delay

Wireless networks have a considerably longer latency (delay) than wired network.

Battery powered devices

Mobile devices are battery powered and hence power is a scarce source. Protocol designed for mobile or wireless networks should be power efficient.

Limited Bandwidth

- Available bandwidth within a cell may change dramatically. This leads to difficulties in guaranteeing QoS parameters such as delay bounds and bandwidth guarantees.
- **Slow start** is the mechanism of traditional TCP for wired network to deal congestion. In that, TCP assumes packet losses due to congestion. However, in wireless network there could be some other reasons that cause packet loss such as BER, and frequent disconnections by handoff.
- If we use traditional TCP in wireless environment, it drastically reduces the congestion window size and doubles the transmission timeout value. This unnecessary congestion control reduces the utilization rate of the bandwidth, reduces the network performance severely.
- Serial time-out at TCP sender degrades overall throughput more than losses due to bit errors or small congestion window do.
- Hence we required to change TCP for mobile environment. There are large number of devices and applications that are using current TCP; it is not possible to change TCP completely just to support mobile users or wireless links.
- Therefore any enhancement to TCP has to be compatible with the standard TCP.

3.5.2 Classical TCP improvements

- In modified TCP, following characteristics are desired :

1. Improve the TCP performance for mobile entities.

2. Maintenance of end-to-end TCP semantics.
3. Minimize the problem caused by lengthy disconnections or by frequent disconnections.
4. Adjust with dynamically changing bandwidth over the already starved wireless link.
5. Make sure that the handoff management is efficient.

- The following sections present some classical solutions that can be used to modify standard TCP to improve the performance of wireless environment.

3.5.2(a) Indirect TCP (I-TCP)

MU - May 13, May 14, May 15, Dec. 15, May 17, May 18

Q. Explain I-TCP in detail. **(May 13, 10 Marks)**

Q. Explain merits and demerits of indirect TCP ? **(May 14, 5 Marks)**

Q. Explain functioning of I-TCP and Snooping TCP. Giving advantages and disadvantages of both. **(May 15, May 17, 10 Marks)**

Q. Explain the functioning of Mobile TCP. **(Dec. 15, 5 Marks)**

Q. Explain any two TCP for Mobile communication. **(May 18, 5 Marks)**

- There are two facts: one is that TCP performs poorly together with wireless links and second is that TCP within the fixed network cannot be changed.
- Fig. 3.5.1 shows an example with a mobile host connected via a wireless link and an access point to the wired internet where the correspondent node resides. The correspondent node could also use wireless access.
- I-TCP separates a TCP connection into two parts : a fixed and a wireless part.
  - **Fixed part is** between the mobile support router (access point) and the fixed host over the fixed network.
  - **Wireless part** is between the MH (Mobile host) and its access point over the wireless medium.
- Standard TCP is used between the fixed computer and the access point.
- A good point for segmenting the connection between mobile host and correspondent host is at the foreign agent of mobile IP.
- The foreign agent is responsible for controlling the user mobility. And during handover, foreign agent transfers the connection to the new foreign agent.
- The foreign agent acts as a proxy and relays all data in both directions.

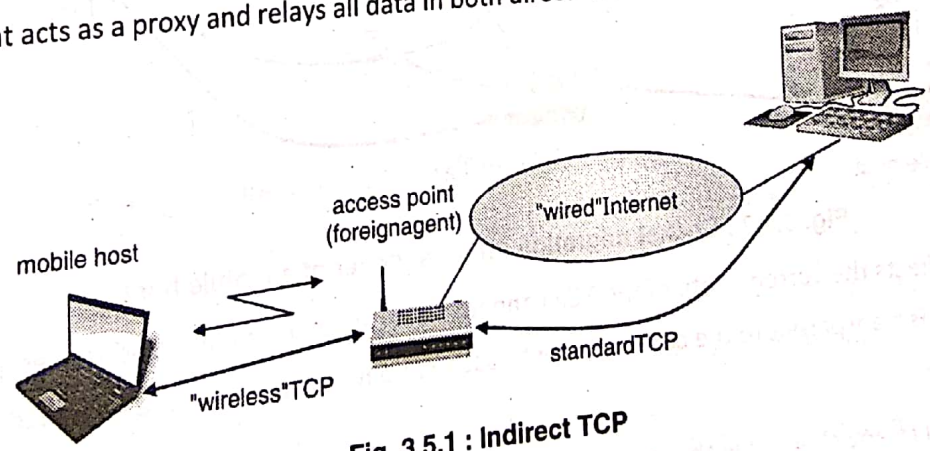


Fig. 3.5.1 : Indirect TCP

There may be following scenarios.

1. **Correspondent host sends a packet to mobile host**
   - Since the correspondent node is a fixed node, it sends a TCP packet via a standard TCP.

- An access point receives that packet and sends an acknowledgement to a fixed host for the received packet.
- The access point buffers the packet and forwards this packet to a mobile host using wireless TCP.
- If there is any transmission error on wireless link then access point retransmits that packet instead of fixed host retransmitting it. (This is also called local retransmission).
- Once the acknowledgement is received for the packet form the mobile host; the access point then removes that packet from its buffer.
- Thus the access point acts as a proxy.

2. Mobile host transmits a packet to a fixed host

- Mobile host sends a TCP packet and access point receives that packet and sends an acknowledgement to mobile host.
- If a packet is lost at wireless link then the mobile host notices this event much faster and retransmits the packet.
- The access point then transmits that packet to the fixed host via standard TCP connection.
- If a packet is lost in wired network then FA handles the retransmissions.
- After receiving the acknowledgement the packet is removed from the buffer.

3. The mobile host moves to a new location and handover takes place

- When mobile host moves to a new location, it registers with new foreign agent. After registration the new foreign agent informs the old foreign agent about its current location.
- The old foreign agent forwards all the buffered packets to new foreign agent as the packet in the buffer have already been acknowledged.
- With the buffered data the sockets of the access point must also migrate to the new foreign agent. This is shown in Fig. 3.5.2.

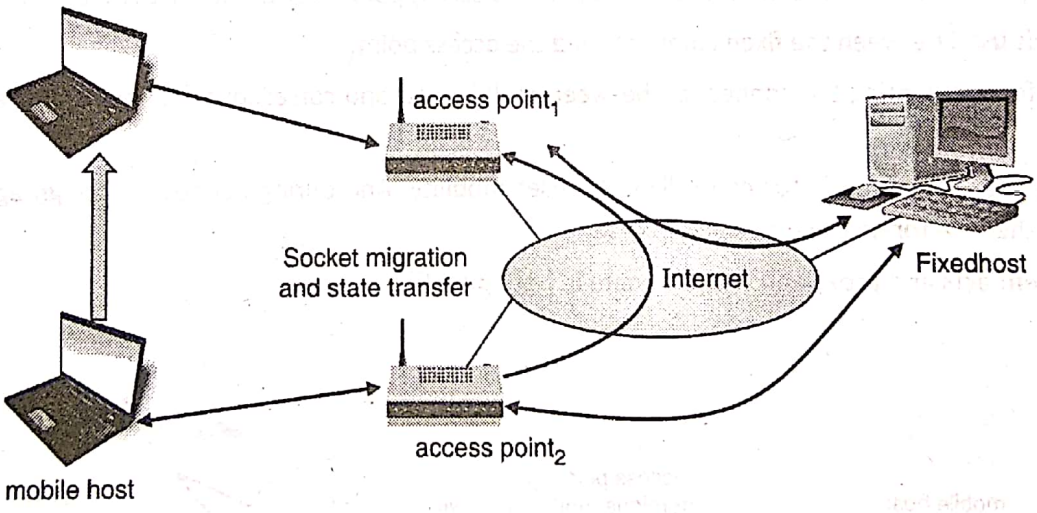


Fig. 3.5.2 : Socket migration after handover of a mobile host

- The socket reflects the current state of the TCP connection i.e. sequence number, addresses, port numbers etc.
- The handover is transparent to the correspondent host and no new connection is established for the mobile host.

Advantages of I-TCP

- I-TCP does not require any changes in the standard TCP used for wired networks.
- Due to the partitioning transmission errors on the wireless link cannot propagate into the fixed network.
- It is simple to control, mobile TCP is used only for one hop between, e.g., a foreign agent and mobile host.
- A very fast retransmission of packets is possible, the short delay on the mobile hop is known.

- Due to the segmentation of the TCP connection, the mobile host and correspondent host can use different transport layer protocols.
- Different solutions to optimize the transfer over the wireless link can be tested or carried out without putting of the Internet at risk.

Disadvantages of I-TCP

- It losses end-to-end semantics; an acknowledgement sent by access point to a sender does now no longer mean that a receiver really got a packet. If a foreign agent crashes before sending acknowledged packet to a mobile host; the sender has no way to find out whether packets have been received or not.
- Higher handover latency is more problematic. All packets sent by correspondent host are buffered by the foreign agent. If a mobile host changes its location, old foreign agent has to forward the buffered packets to the new foreign agent as they have already been acknowledged by the old access point.
- The foreign agent must be a trusted entity because TCP connection ends at this point.

3.5.2(b) Snooping TCP (S-TCP)

MU – May 12, Dec. 13, May 14, May 15, May 17, May 18

Q. Explain snooping TCP with its merits and demerits. **(May 12, Dec. 13, May 14, 5 Marks)**

Q. Explain the functioning of SNOOP -TCP, give advantages and disadvantages. **(May 15, 10 Marks)**

Q. Explain functioning of I-TCP and Snooping TCP. Giving advantages and disadvantages of both. **(May 15, May 17, 10 Marks)**

Q. Explain any two TCP for Mobile communication. **(May 18, 5 Marks)**

- Snooping TCP works completely transparently and leaves the TCP end-to-end connection intact.
- It overcomes the some drawbacks of the I-TCP.

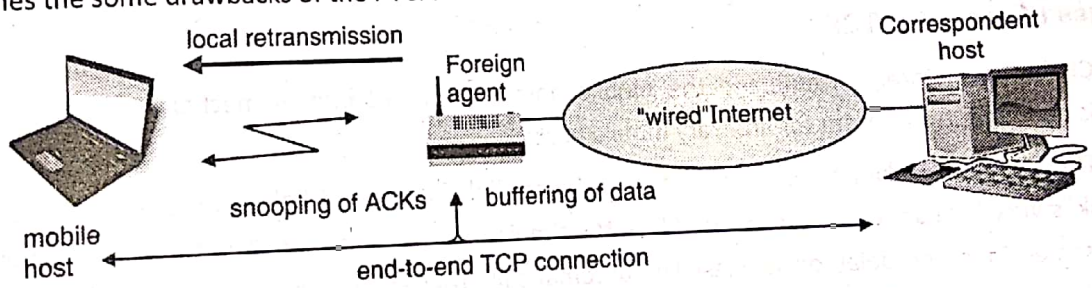


Fig. 3.5.3 : Snooping TCP

Snooping TCP works as follows :

1. Correspondent host sends a packet to mobile host

- Correspondent host sends a packet to mobile host via wired TCP connection. The access point buffers the packet sent by correspondent host.
  - Access point also snoops on the packet in both directions to reorganize acknowledgements.
  - Once the mobile host receives the packet, it sends an acknowledgement and this acknowledgement also passes through the access point.
  - If the access point doesn't receive any acknowledgement from a mobile host within certain amount of time, then it retransmits the packet from its buffer, performing a much faster retransmission compared to the fixed host.
  - The time-out for acknowledgements can be much shorter, because it reflects only the delay of one hop plus processing time.

- It is also possible that mobile host sends duplicate acknowledgements for the same packet to indicate a packet loss; the foreign agent can filter these duplicate acknowledgements so, that unnecessary retransmissions from the correspondent host can be avoided.

2. Mobile host transmits a packet to a correspondent host

- When a mobile host sends a packet to correspondent host, the foreign agent keeps track of the sequence numbers of these packets.
- When a foreign agent detects a gap in the sequence numbers, i.e. packet loss, it sends a negative acknowledgement (NACK) to the mobile host.
- Once the mobile host receives the NACK, it can retransmit the missing packet immediately.
- Reordering of the packets is done automatically at the correspondent node by TCP.

Note that to maintain end-to-end semantics of TCP, foreign agent must not acknowledge data itself to the correspondent host (instead FA forwards the ACK received from the MH). This ensures the correspondent host that the mobile host has actually received the data. Now if foreign agent crashes, the time-out mechanism of correspondent host still works and triggers a retransmission of a lost packet.

Advantages of Snooping-TCP

- The end-to-end semantics are preserved.
- Correspondent host need not to be changed; most of the enhancements are done in the foreign agent.
- It doesn't need handover of the state as soon as the mobile host moves to another foreign agent. Assume there might still be data in the buffer not transferred to the new foreign agent. All that happens is a time-out at the correspondent host and the retransmission of the packets to the new foreign agent.
- It doesn't matter if the new foreign agent uses the enhancement or not. If not, snooping TCP automatically falls back to the standard solution.

Disadvantages of snooping TCP

- Using NACK between foreign agent and the mobile host assumes additional mechanisms on mobile host. This approach is no longer transparent for arbitrary mobile hosts.
- Snooping TCP does not isolate the behavior of the wireless link from wired link as in case of I-TCP. If the delay in wireless link is very high as compared to wired link, the timers of the access point and the correspondent host would almost be same. Thus, the delay on wireless link automatically triggers time-out in correspondent host and causes retransmissions. Thus the effectiveness of S-TCP completely depends on the quality of wireless link.
- If user applies end-to-end encryption, S-TCP fails. Because TCP header would be encrypted and hence snooping on the sequence numbers is meaningless.

3.5.2(c) Mobile TCP (M-TCP)

MU – May 12, Dec. 13, May 13, Dec. 17, May 18

Q.	Explain M-TCP in detail.	**(May 13, 5 Marks)**
Q.	Explain mobile TCP with its merits and demerits.	**(May 12, Dec. 13, 5 Marks)**
Q.	Write a short note on M-TCP.	**(Dec. 17, 5 Marks)**
Q.	Explain any two TCP for Mobile communication.	**(May 18, 5 Marks)**

- The occurrence of lengthy and/or frequent disconnection is the major problem in wireless networks. M-ICP deals with the lengthy and/or frequent disconnections.

- M-TCP aims :
  - To improve overall throughput
  - To lower the delay
  - To maintain end-to-end semantics of TCP
  - To provide a more efficient handover
- The connection is split up into 2 parts by M-TCP similar to I-TCP.
- The correspondent host and supervisory host communicate via the unmodified standard TCP.
- The communication between supervisory host (SH) and mobile host (MH) is done by the modified special TCP.
- For transferring data between both parts, the supervisory host is used.
- SH does not perform caching or retransmission of data as a relatively low bit error rate is assumed by M-TCP on the wireless link. Whenever a packet is lost on the wireless link, the original sender must retransmit it. TCP end-to-end semantics are thus maintained. For fair sharing over the wireless link, M-TCP needs a bandwidth manager.

Working of M-TCP

- Packets are sent to the mobile host by a correspondent host.
- If any packet is lost on the wireless link, then the original sender retransmits the packet. Thus, end-to-end semantics are maintained.
- All the packets sent to MH are monitored by the SH and are acknowledged by the MH via ACK packets.
- After a set amount of time, if the SH still does not receive any ACK, it assumes that the MH is disconnected.
- SH sets sender's window size to zero and thus chokes the sender. Once the window size is set to zero, the sender is forced to go into a persistent mode. In the persistent mode, independent of the receiver's period of disconnected state, the state of the sender will not change.
- Once the SH detects the connectivity again, the sender's window size is again set to the old value, enabling the sender to send at full speed.

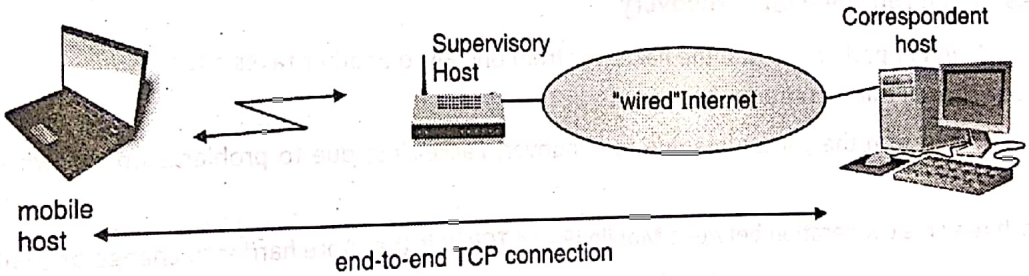


Fig. 3.5.4 : Mobile TCP (M-TCP)

Advantages of M-TCP

- End-to-end semantics are maintained. SH itself doesn't send any ACK, it only forwards ACKs that were received from the MH.
- It avoids unnecessary retransmissions, if the MH is disconnected.
- It is not necessary to forward all data to a new SH because SH does not buffer any data.

Disadvantages of M-TCP

- Losses on wireless link are propagated to the wired link. This is because SH does not act as a proxy and does not buffer the packets and is not responsible for local retransmission.
- It requires new network elements like bandwidth manager.

3.5.3 Fast Retransmit/Fast Recovery

- This scheme improves the performance during handover.
- Moving to a new FA can cause packet loss or time out at mobile host or correspondent host. In such case standard TCP assumes congestion and goes into slow start mode although there is no congestion (Here packet loss is caused due to handover).
- A host can use fast retransmit/fast recovery after it receives duplicate acknowledgements. The idea here is to automatically force the fast retransmit behavior on the mobile host and correspondent host.

Correspondent host enters in fast retransmit mode

- As soon as mobile host registers at a new foreign agent, it starts sending duplicate acknowledgements (three duplicate ACKs) to the correspondent host.
- On receiving these duplicates the correspondent host continues to send with the same rate it did before the mobile host moved to new foreign agent.
- Thus the correspondent host goes into fast transmit mode and not to the slow start.

Mobile host enters in fast retransmit mode

- Mobile host may also enter in slow start after moving to a new foreign agent.
- To avoid this, after handover a mobile host automatically activates fast retransmit mode.
- The mobile host retransmits all unacknowledged packet using the current congestion window size without going into slow start.

Advantages of fast retransmit/fast recovery

- Foreign agent or correspondent host need not to be changed.
- Minor changes are required in mobile host's software.
- Very Simple.

Disadvantages of fast retransmit/fast recovery

- Insufficient isolation of packet losses. If the handover from one FA to another takes a longer time, the correspondent node will have already started retransmissions.
- This approach focuses on the packet loss due to handover. Packet loss due to problems on the wireless link is not considered.
- This approach requires cooperation between Mobile IP and TCP. It is therefore harder to change one without affecting the other.

3.5.4 Transmission/ Time-out Freezing

- This approach can handle long disconnections of MH.
- Quite regularly, it happens that the MAC layer predict the connection problems, before the connection is actually interrupted from TCP point of view.
- Additionally, the MAC layer knows the actual reason of the disconnection and does not assume congestion as TCP does.
- MAC layer can now inform the TCP layer for the upcoming loss in connection.
- TCP can now stop packet sending and freeze the current state of congestion window and all timers of TCP.
- If the disconnections occur frequently then additional mechanism in the access point must be included to inform the correspondent host about the reason of interruption.

- As soon as the MAC layer detects connectivity again, it informs the TCP to resume operation with the same congestion window and the timers.

Advantages of transmission/time-out freezing

- It offers a way to resume TCP connection even after a longer interruption of the connection.
- This scheme is independent of any other TCP mechanisms such as acknowledgements or sequence numbers. So it can be used together with encrypted data.

Disadvantages of transmission/time-out freezing

- Mobile host as well as correspondent host needs to be changed.
- All mechanisms are based on the capability of MAC layer to detect future interruption.
- If the encryption is used that depends on time-dependent random numbers, then this scheme required resynchronization after interruption.

3.5.5 Selective Retransmission

- In the standard TCP acknowledgments are in sequence.
- If a packet is lost, the sender has to retransmit all the packets starting from the lost packet. (GO-BACK N retransmission). This wastes the bandwidth.
- The selective retransmission approach allows a retransmission of a selective packet i.e. the sender can now determine which packet is to be retransmitted.

Advantages of Selective retransmission

- Sender need to retransmit lost packet only. Thus, bandwidth requirement is much lower and it is advantageous in slow wireless links.
- Improves the performance of TCP in wireless as well as in wire networks.

Disadvantages of Selective retransmission

- Complexity of receiver side increases.
- More buffer space is required at the receiver side to store all the packets following the missing packet and wait for the gap to be filled.

3.5.6 Transaction oriented TCP (T/TCP)

- If a mobile host wants to send a packet via TCP, it requires three steps: connection setup, data transmission, and connection release.
- Both connection setup and connection release require three way handshaking.
- If a mobile host has to send one packet, TCP requires seven packets. Three for connection set up, one for data and again three for connection release (Fig. 3.5.5).
- For the large transmission this overhead is negligible but for small amount of data it is not negligible.
- The transaction oriented TCP provides a solution. It combines the connection setup and connection release with the user data packet.
- This can reduce the number of packets to two from seven.

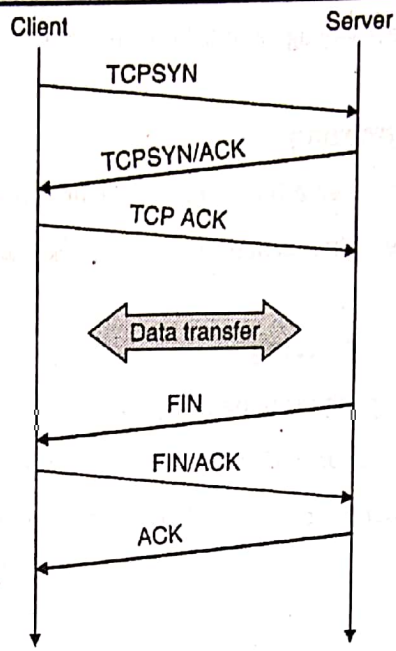


Fig. 3.5.5 : Example of TCP connection setup and release

Advantage of transaction-oriented TCP

Reduce overhead.

Disadvantage of transaction-oriented TCP

- It requires change in mobile host and all correspondent hosts.
- The mobility is no longer transparent.
- It poses many security risks.

3.5.7 Comparison of TCP Variants

Table 3.5.1 : Comparison of the TCP enhancements

Sr. No.	Approach	Mechanism	Advantages	Disadvantages
1.	**Indirect TCP**	Splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover
2.	**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
3.	**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
4.	**Fast retransmit/ fast recovery**	Avoids slow-start after roaming	Simple and efficient	Mixed layers, not transparent
5.	**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

Sr. No.	Approach	Mechanism	Advantages	Disadvantages
6.	**Selective retransmission**	Retransmit only lost data	Very efficient	Slightly more complex receiver software, more buffer needed
7.	**Transaction oriented TCP**	Combine connection setup/release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent

3.6 IPv4 and IPv6

MU - May 12

Q. What advantages does the use of IPV6 offer for mobility? **(May 12, 5 Marks)**

Ipv4

The network layer protocol in the TCP/IP protocol suite is currently IPv4. IPv4 provides the host-to-host communication between systems in the Internet. IPv4 has some deficiencies that make it unsuitable for the fast growing Internet, including the following:

- Despite all short term solutions, such as subnetting, classless addressing, and NAT, address depletion is still a long term problem in the Internet.
- The Internet must accommodate real time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided by IPv4 design.
- The Internet must accommodate encryption and authentication of data for some applications. No encryption or authentication is provided by IPv4.

Ipv6

- To overcome these problems, IPv6 also known as IPng (Internet Protocol next generation) was proposed.
- In IPv6, the Internet protocol was extensively modified to accommodate the growth and new demands of the Internet.
- The format and the length of the IP addresses were changed along with the packet format.
- Related protocols such as ICMP were also modified.
- Other protocols in the network layer, such as ARP, RARP, and IGMP were either deleted or included in ICMPv6 protocol. Routing protocols such as RIP and OSPF were slightly modified to accommodate these changes.
- The fast spreading use of Internet and new services such as mobile IP, IP telephony, and IP-capable mobile telephony, may require the total replacement of IPv4 by IPv6.

Advantages of IPv6

(i) **Larger address space :** An IPv6 address is 128 bit long. Compared with the 32 bit long IPv4 address; this is huge increase in address space.

(ii) **Better Header format :** IPv6 uses a new header format in which options are separated from the base header and inserted when needed, between the base header and the upper layer data. This simplifies and speeds up the routing process because most of the options do not need to be checked by routers.

(iii) **New Options :** IPv6 has new options to allow for additional functionalities.

(iv) **Allowance for extension :** IPv6 is designed to allow the extension of protocol if required by new technologies or applications.

(v) **Support for resource allocation :** In IPv6, the ***type-of-service*** field has been removed, but mechanism called ***Flow label*** has been added to enable the source to request special handling of packet. This mechanism can be used to support traffic such as real-time audio and video.

(vi) **Support for more security :** The encryption and authentication options in IPv6 provide confidentiality and integrity of the packet.

Features of Ipv6 to support mobility

- No special mechanisms are needed for securing mobile IP registration. In every Ipv6 node **address auto-configuration** i.e. the mechanism for acquiring a COA is inbuilt.
- **Neighbor discovery** mechanism is also mandatory for every Ipv6 node. So special foreign agents are no longer needed to advertise services.
- Combining the features of address auto-configuration and neighbor discovery enable every Ipv6 mobile node to create and obtain a topologically correct address or the current point of attachment.
- Every Ipv6 node can send binding updates to another node, so the MN can send its COA directly to the CN and HA. The FA is no longer needed. The CN processes the binding updates and makes corresponding entries in its routing cache.

  The MN is now able to :
  - Decapsulate the packets
  - Detect when it needs a new COA and
  - Determine when to send binding updates to the HA and CN
- A **soft handover** is possible with Ipv6. The MN sends its new COA to the old router serving the MN at the old COA, and the old router can encapsulate all incoming packets for the MN and forwards them to new COA.

Ipv6 Header

Fig. 3.6.1 shows both Ipv4 and Ipv6 header format.

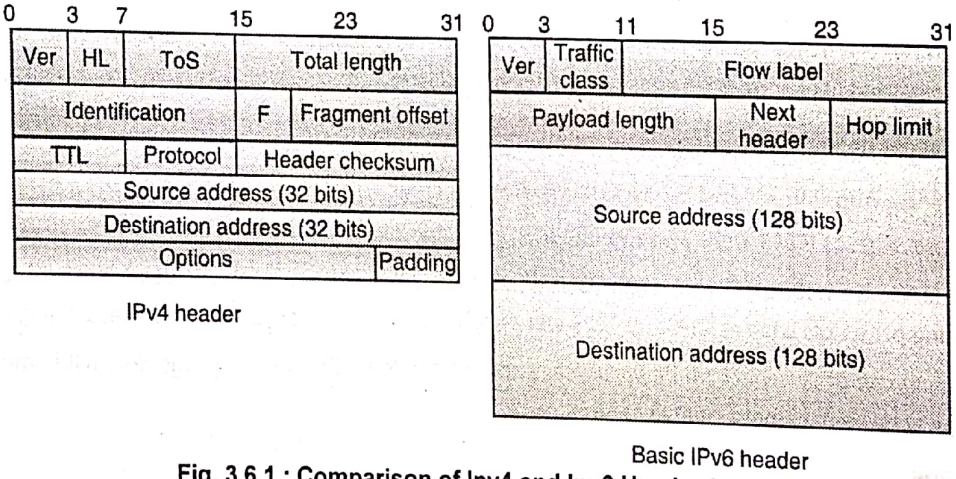


Fig. 3.6.1 : Comparison of Ipv4 and Ipv6 Header format

Fields of Ipv6 header

(i) **Version :** 4 bits. IPv6 version number.

(ii) **Traffic Class :** 8 bits. Used to specify different classes or priorities of IPv6 packets.

(iii) **Flow Label :** 20 bits. Used for specifying special router handling from source to destination(s) for a sequence of packets. It distinguishes the different types of packets such as audio, video, txt etc. and accordingly provides Quality of services to them.

(iv) **Payload Length :** 16 bits unsigned. Specifies the length of the data in the packet.

(v) **Next Header :** 8 bits. Specifies the next encapsulated protocol. The values are compatible with those specified for the IPv4 protocol field.

(vi) **Hop Limit :** 8 bits unsigned. For each router that forwards the packet, the hop limit is decremented by 1. When the hop limit field reaches zero, the packet is discarded. This replaces the TTL field in the IPv4 header that was originally intended to be used as a time based hop limit.

(vii) **Source address :** 16 bytes. The IPv6 address of the sending node.

(viii) **Destination address :** 16 bytes. The IPv6 address of the destination node.

Review Questions

Q. 1 Explain working of DRS with a suitable example.

Q. 2 Explain DSDV routing protocol.

Q. 3 Compare M-TCP and Snooping TCP.

Q. 4 Write a short note on DSR.

Q. 5 Explain any two routing algorithms used for MANET.

Q. 6 Explain the errors in wireless networks that degrade the performance of TCP.

Q. 7 Explain various types of transmission errors in wired and wireless networks.

Q. 8 Explain the errors in wireless networks that degrade the performance of TCP and how TCP snooping can improve the performance.

Q. 9 Discuss the problems of using traditional TCP in wireless networks? Explain I-TCP.

Q. 10 What are the problems with IPv4 protocol? What advantages does IPv6 provide over IPv4?

Q. 11 What are the features of IPv6? Explain IPv6 packet format.

□□□