CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.2. DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP):

DHCP is used to merge the world of mobile phones with the internet and to support mobility. Automatically assigns a unique IP address to each device that connects to a network. Used to simplify the installation and maintenance of networked computers.

If a new computer is connected to a network, DHCP can provide it with all the necessary information for full system integration into the network, e.g., addresses of a DNS server and the default router, the subnet mask, the domain name, and an IP address

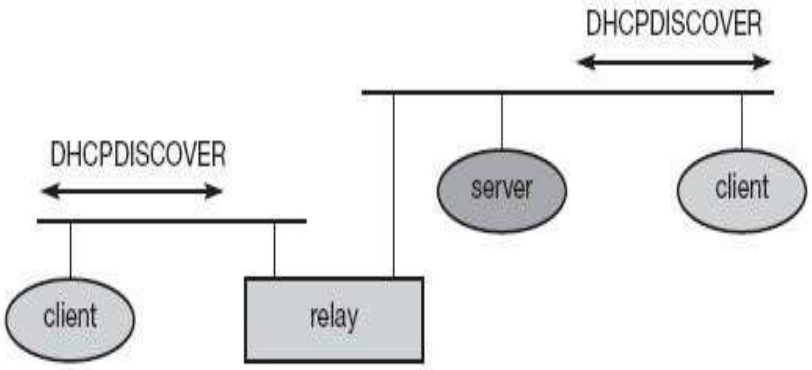


Fig. Basic DHCP Configuration

DHCP clients send a request to a server (DHCPDISCOVER) to which the server responds.

A client sends requests using DHCP is based on a client/server model.

MAC broadcasts to reach all devices in the LAN.

A DHCP relay might be needed to forward requests across inter-working units to a DHCP server.

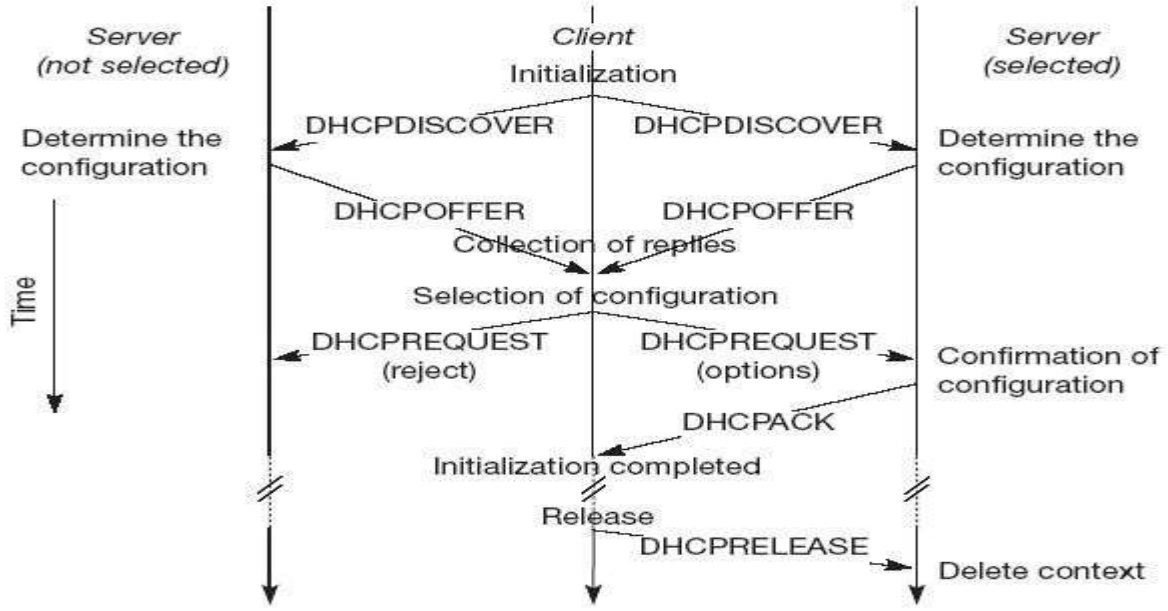


Fig. Client initialization via DHCP

The above figure shows one client and two servers.

1. The client broadcasts a DHCPDISCOVER into the subnet.

2. Two servers receive this broadcast and find the configuration they can offer to the client.

3. Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters.

4. Then the client can choose one of the configurations offered.

5. Then the client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCP REQUEST.

6. If a server receives a DHCP REQUEST with a rejection, it can free the reserved configuration for other possible clients.

7. The server with the configuration accepted by the client now confirms the configuration with DHCP ACK. This completes the initialization phase.

8. If a client leaves a subnet, it should release the configuration received by the server using DHCP RELEASE.

9. The configuration a client gets from a server is only leased for a certain amount of time, it has to be reconfirmed from time to time.

CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.6. HYBRID ROUTING PROTOCOLS(ZRP)

Combines the best features of both proactive & reactive routing protocols.

Eg: ZONE ROUTING PROTOCOL (ZRP)

ZONE ROUTING PROTOCOL (ZRP)

It is Hybrid Protocol. Based on the concept of zones. A routing zone is defined for each node separately and zones of neighbouring nodes overlap. The routing zone has a radius expressed in hops.

i.e., Zone radius: Number of hops

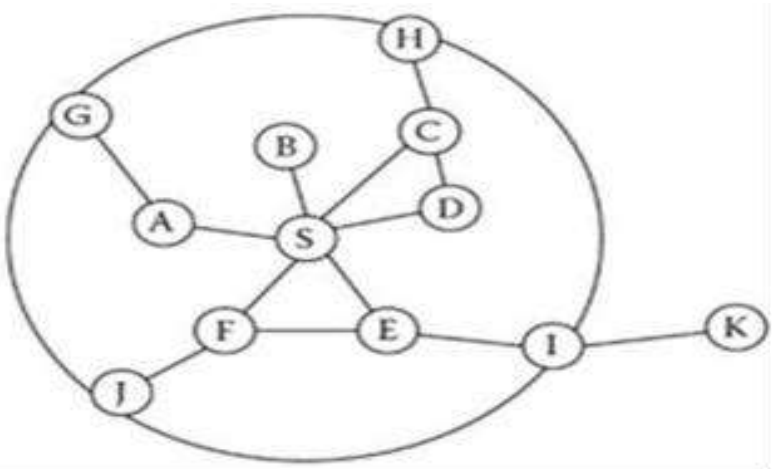
Key concept in ZRP to:

- Use a proactive routing scheme within a limited zone
- Use a reactive routing scheme for nodes beyond this zone.

Routing is divided into two parts:

Intrazone routing: 1st the packet is sent within the routing zone of the source node to reach the peripheral nodes.

Interzone routing: The packet is sent from the peripheral nodes towards the destination node.



In the diagram the routing zone of S includes the nodes A-I, but not K.

- The nodes are divided into peripheral nodes and interior nodes.
- Peripheral nodes: Nodes whose minimum distance is less than the radius.
- Interior nodes - Nodes A-F
- Peripheral nodes - Nodes G-J
- Node K is outside the routing zone
- Within the zone table driven is used
- Outside the zone On demand Route Discovery is used

Procedure:

1. The source sends a Route Request packet (RREQ) to the border nodes of its zone, containing its own address, destination address and the unique sequence no.
2. Each border nodes checks its local zone for the destination.
3. If the destination is not a member of local zone, then the border node adds its own address to the route request packet and forwards the packet to its own border nodes.
4. When the destination node is reached in this process, a route reply (RREP) is sent on the reverse path back to the source.
5. The source saves the path which is mentioned in Route Reply to send data packets to the destination

CS8601 -MOBILE COMPUTING

UNIT 3

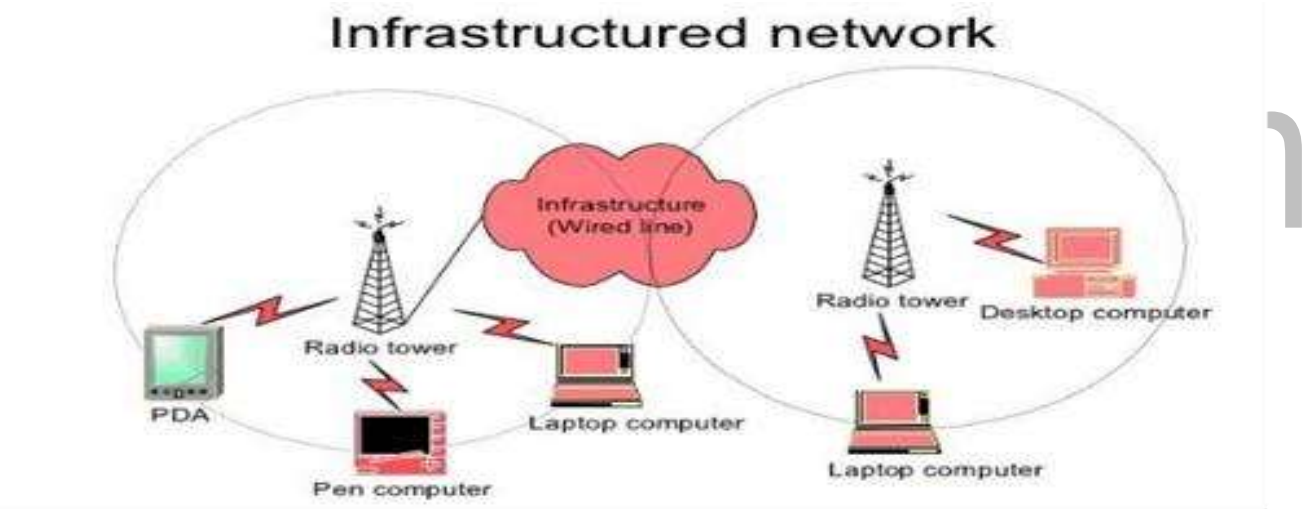
MOBILE NETWORK LAYER

3.3. MOBILE AD-HOC NETWORK (MANET)

Types of wireless network:

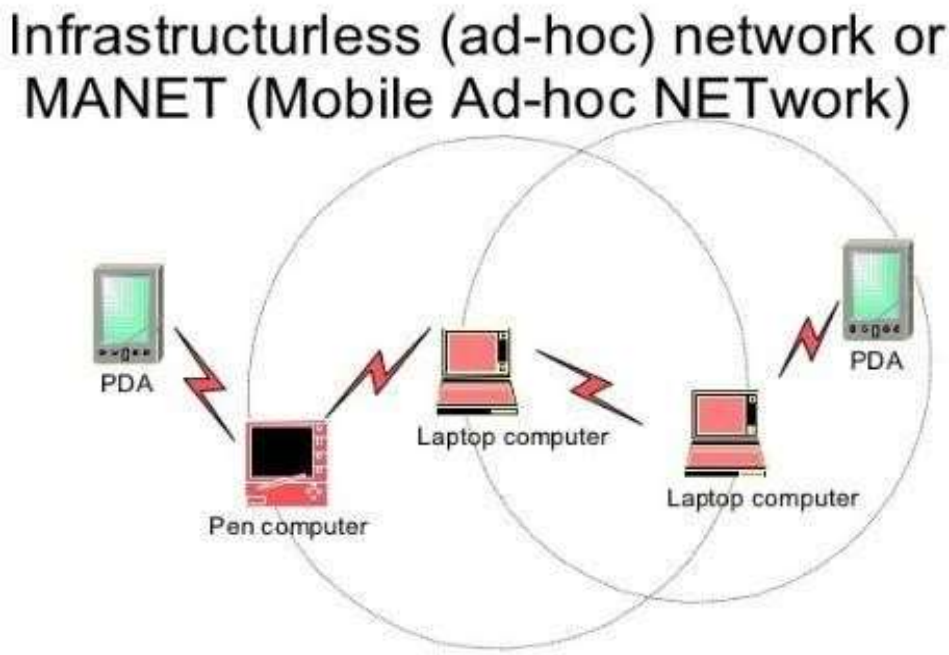
Infrastructured:

- The MN can move while communicating
- The BSs are fixed
- As the node goes out of the range of a BS, it gets into the range of another BS.



Infrastructureless or Mobile ad-hoc (MANET):

- The MN can move while communicating
- There are no fixed BSs.
- All the nodes in the network need to act as routers.
- Used to simplify the installation and maintenance of networked computers.
- MANET are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links.
- No existing fixed infrastructure or centralized administration
- Mobile nodes are free to move randomly i.e., network topology changes frequently.
- Each node work as a router.



FEATURES OF MANET:

- MANET can be formed without any pre-existing infrastructure.
- It follows dynamic topology where nodes may join and leave the network at any time and the multi-hop routing may keep changing as nodes join and depart from the network.
- It does have very limited physical security, and thus increasing security is a major concern.
- Every node in the MANET can assist in routing of packets in the network.
- Limited Bandwidth & Limited Power

CHARACTERISTICS OF MANET

1. Lack of fixed infrastructure

– bring new n/w designing challenges.

– Pair of nodes can either communicate directly when they are in within the range or can communicate via multi-hop communication.

2. Dynamic topologies :

– n/w topology can change unpredictably because of the mobility of devices in MANET

– Rate of topology change depends on the speed of mobile movement

***3.* Bandwidth constrained, variable capacity link:**

– Wireless link have lower capacity compare to wired link

– Factors affecting Bandwidth: Noise, Interference…….

4. Energy constrained operation:

– Nodes depends on battery power

– Small battery – limited amount of energy

– Need more energy during Routing

– "Energy Conservation" – important objective of MANET routing protocol

5. Increased vulnerability:

– New type of security threats

– Increased the possibility of eavesdropping, spoofing, DOS attacks.

– Difficult to identify the attacker because:

– Devices keeps on moving

– Do not have global Identifier

CHALLENGES / CONSTRAINTS / DESIGN ISSUES OF MANET

1) Limited bandwidth:

Limited bandwidth because of the effect of multiple access, fading, noise, and interference conditions, etc.,

2) Dynamic topology:

Dynamic topology membership may disturb the trust relationship among node.

3) Routing Overhead:

Unnecessary routing overhead since nodes often change their location within network.

4) Hidden terminal problem:

The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender, but are within the transmission range of the receiver.

5) Packet losses due to transmission errors:

Much higher packet loss due to factors such as increased collisions due to the presence of hidden terminals, presence of interference, uni- directional links, frequent path breaks due to mobility of nodes.

6) Mobility-induced route changes:

The network topology in an ad hoc wireless network is highly dynamic due to the movement of nodes; hence an on-going session suffers frequent path breaks. This situation often leads to frequent route changes.

7) Battery constraints:

Devices used in these networks have restrictions on the power source in order to maintain portability, size and weight of the device.

8) Security threats:

Brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping.

APPLICATIONS OF MANET

Application	Possible Applications
Tactical networks	• Military communication and operations • Automated battlefields
Emergency services	• Search and rescue operations • Disaster recovery • Replacement of fixed infrastructure in case of environmental disasters • Policing and fire fighting • Supporting doctors and nurses in hospitals
Commercial and civilian environments	• E-commerce: electronic payments anytime and anywhere • Business: dynamic database access, mobile offices • Vehicular services: road or accident guidance, transmission of road and weather conditions, taxi cab network, inter-vehicle networks • Sports stadiums, trade fairs, shopping malls • Networks of visitors at airports
Home and enterprise networking	• Home/office wireless networking • Conferences, meeting rooms • Personal area networks (PAN), Personal networks (PN) • Networks at construction sites
Education	• Universities and campus settings • Virtual classrooms • Ad hoc communications during meetings or lectures
Entertainment	• Multi-user games • Wireless P2P networking • Outdoor Internet access • Robotic pets • Theme parks
Sensor networks	• Home applications: smart sensors and actuators embedded in consumer electronics • Body area networks (BAN) • Data tracking of environmental conditions, animal movements, chemical/biological detection
Context aware services	• Follow-on services: call-forwarding, mobile workspace • Information services: location specific services, time dependent services • Infotainment: touristic information
Coverage extension	• Extending cellular network access • Linking up with the Internet, intranets, etc.

CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.1. Mobile IP

The IP addresses are designed to work with stationary hosts because part of the address defines the network to which the host is attached. A host cannot change its IP address without terminating on-going sessions and restarting them after it acquires a new address. Other linklayer mobility solutions exist but are not sufficient enough for the global Internet.

Mobility is the ability of a node to change its point-of-attachment while maintaining all existing communications and using the same IP address.

Nomadicity allows a node to move but it must terminate all existing communications and then can initiate new connections with a new address.

Mobile IP is a network layer solution for homogenous and heterogeneous mobility on the global Internet which is scalable, robust, secure and which allows nodes to maintain all ongoing communications while moving.

Design Goals:

Mobile IP was developed as a means for transparently dealing with problems of mobile users. Mobile IP was designed to make the size and the frequency of required routing updates as small as possible. It was designed to make it simple to implement mobile node software. It was designed to avoid solutions that require mobile nodes to use multiple addresses.

Requirements:

There are several requirements for Mobile IP to make it as a standard. Some of them are:

1. ***Compatibility*****:** The whole architecture of internet is very huge and a new standard cannot introduce changes to the applications or network protocols already in use. Mobile IP is to be integrated into the existing operating systems. Also, for routers also it may be possible to enhance its capabilities to support mobility instead of changing the routers which is highly impossible. Mobile IP must not require special media or MAC/LLC protocols, so it must use the same interfaces and mechanisms to access the lower layers as IP does. Finally, end-systems enhanced with a mobile IP implementation should still be able to communicate with fixed systems without mobile IP.

2 ***Transparency*:** Mobility remains invisible for many higher layer protocols and applications. Higher layers continue to work even if the mobile computer has changed its point of attachment to the network and even notice a lower bandwidth and some interruption in the service. As many of today's applications have not been designed to use in mobile environments, the effects of mobility will be higher delay and lower bandwidth.

3 ***Scalability and efficiency***: The efficiency of the network should not be affected even if a new mechanism is introduced into the internet. Enhancing IP for mobility must not generate many new messages flooding the whole network. Special care is necessary to be taken considering the lower bandwidth of wireless links. Many mobile systems have a wireless link to an attachment point. Therefore, only some additional packets must be necessary between a mobile system and anode in the network. It is indispensable for a mobile IP to be scalable over a large number of participants in the whole internet, throughout the world.

4 ***Security***: Mobility possesses many security problems. A minimum requirement is the authentication of all messages related to the management of mobile IP. It must be sure for the IP layer if it forwards a packet to a mobile host that this host really is the receiver of the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There is no way to prevent faked IP addresses and other attacks.

The goal of a mobile IP can be summarized as: 'supporting end-system mobility while maintaining scalability, efficiency, and compatibility in all respects with existing applications and Internet protocols'.

Entities and terminology

The following defines several entities and terms needed to understand mobile IP

Mobile Node (MN):

A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP. The MN keeps its IP address and can continuously communicate with any other system in the internet as long as link-layer connectivity is given. Examples are laptop, mobile phone, router on an aircraft etc.

Correspondent node (CN):

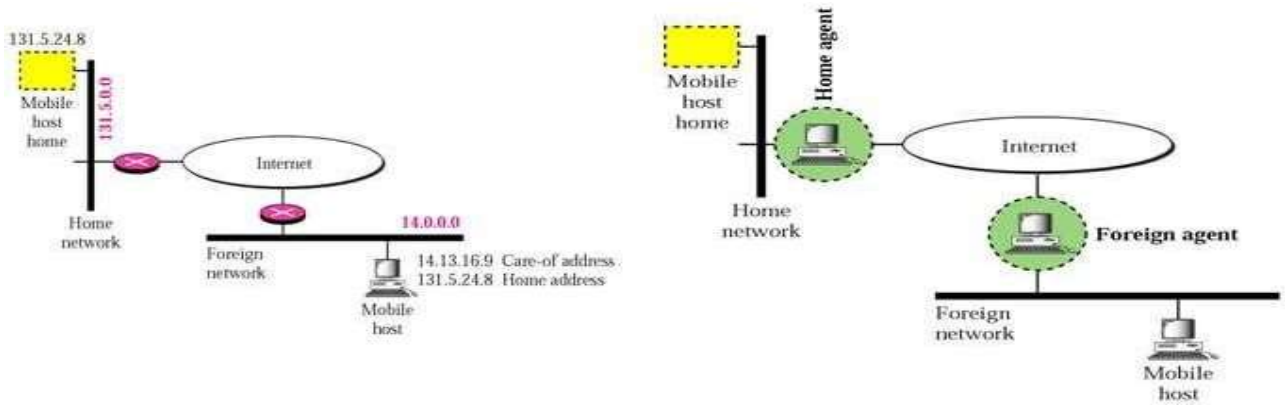
At least one partner is needed for communication. In the following the CN represents thispartner for the MN. The CN can be a fixed or mobile node.

Home network:

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

Foreign network:

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



Foreign agent (FA):

The FA can provide several services to the MN during its visit to the foreign network. The FA can have the COA, acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN. FAs can also provide security services because they belong to the foreign network as opposed to the MN which is only visiting. FA is implemented on a router for the subnet the MN attaches to.

Care-of address (COA):

The COA defines the current location of the MN from an IP point of view. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN. Packet delivery toward the MN is done using a tunnel, i.e., the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel, there are possibilities for the location of the COA.

Foreign agent COA:

The COA could be located at the FA, i.e., the COA is an IP address of the FA. The FA is the tunnel end-point and forwards packets to the MN. Many MN using the FA can share this COA as common COA.

Co-located COA:

The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, and the tunnel endpoint is at the MN. Co-located addresses can be acquired using services such as DHCP.

Home agent (HA):

The HA provides several services for the MN and is located in the home network. The tunnel for packets toward the MN starts at the HA. The HA maintains a location registry, i.e., it is informed of the MN's location by the current COA. Three alternatives for the implementation of an HA exist.

1. The HA can be implemented on a router that is responsible for the home network. This is obviously the best position, because without optimizations to mobile IP, all packets for the MN have to go through the router anyway.
2. If changing the router's software is not possible, the HA could also be implemented on an

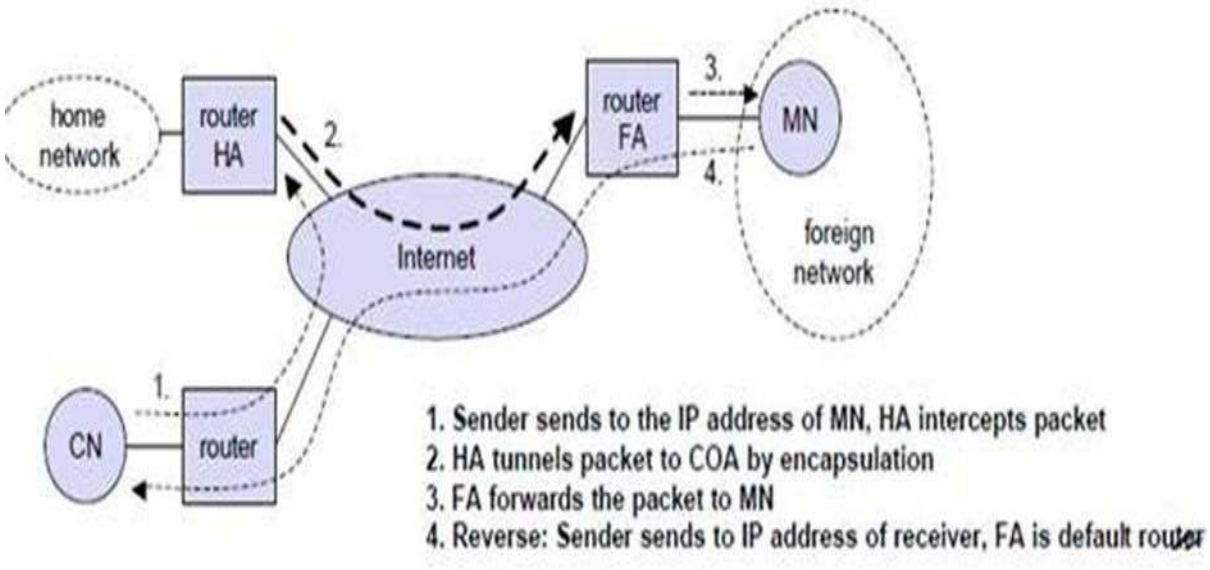
arbitrary node in the subnet. One disadvantage of this solution is the double crossing of the router by the packet if the MN is in a foreign network. A packet for the MNcomes in via the router; the HA sends it through the tunnel which again crosses the router. Finally, a home network is not necessary at all. The HA could be again on the 'router' but this time only acting as a manager for MNs belonging to a virtual home network. All MNs are alwaysin a foreign network with this solution. A CN is connected via a router to the internet, as are the home network and the foreign network. The HA is implemented on the router connecting the home network with the internet, an FA is implemented on the router to the foreign network. The MN is currently in the foreign network. The tunnel for packets toward the MN starts at the HA and ends at the FA, for the FA has the COA in the above example.

IP packet delivery

Consider the above example in which a correspondent node (CN) wants to send an IP packet to the MN. One of the requirements of mobile IP was to support hiding the mobility of theMN. CN does not need to know anything about the MN's current location and sends the packetas usual to the IP address of MN as shown below.

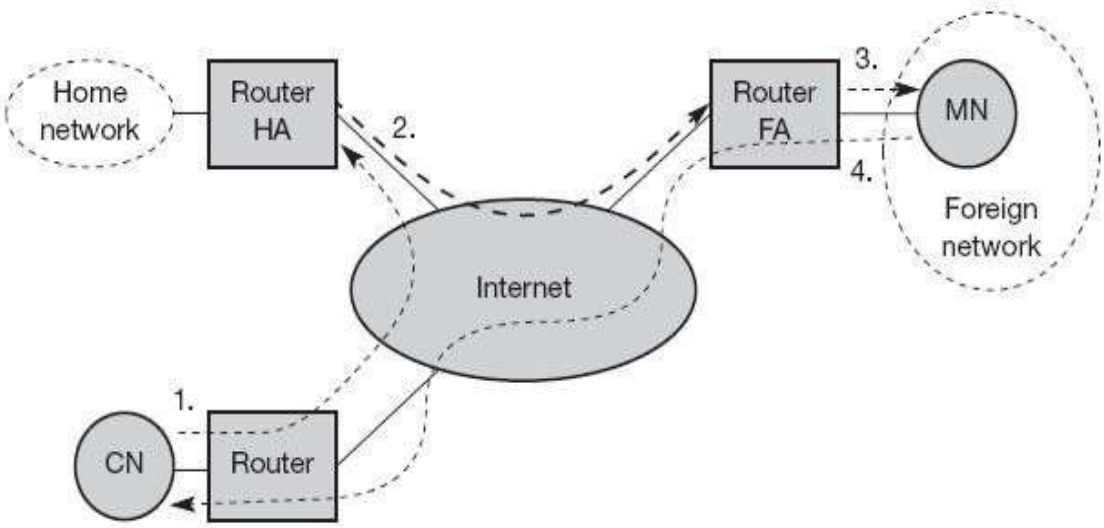
CN sends an IP packet with MN as a destination address and CN as a source address. The internet, not having information on the current location of MN, routes the packet to the router responsible for the home network of MN. This is done using the standard routing mechanisms of the internet. The HA now intercepts the packet, knowing that MN is currently not in its home network. The packet is not forwarded into the subnet as usual, but encapsulated and tunneled to the COA. A new header is put in front of the old IP header showing the COA as new destination and HA as source of the encapsulated packet .

The foreign agent now decapsulates the packet, i.e., removes the additional header, and forwards the original packet with CN as source and MN as destination to the MN . Again,for the MN mobility is not visible. It receives the packet with the same sender and receiver address as it would have done in the home network



Sending packets from the mobile node (MN) to the CN is comparatively simple. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination . The router with the FA acts as default router and forwards the packet in the same way as it would do for any other node in the foreign network. As long as CN is a fixed node the remainder is in the fixed internet as usual.

Working of Mobile IP:-



Packet delivery to and from the mobile node

Steps used in the operation of mobile IP:

STEP 1: CN sends the Packet to the IP address(home address)of the MN

STEP 2: Internet Routes the Packet to the router of the MN's home network. The HA examines the packet to find whether the MN is present in its current home network or not. If the MN is not present, then the HA encapsulates that datagram in a new packet.

STEP 3: The encapsulated packet is tunneled to the FA, which act as the new destination address. Then FA performs decapsulation to remove the additional header. Then forwards the decapsulated packet to the MN.

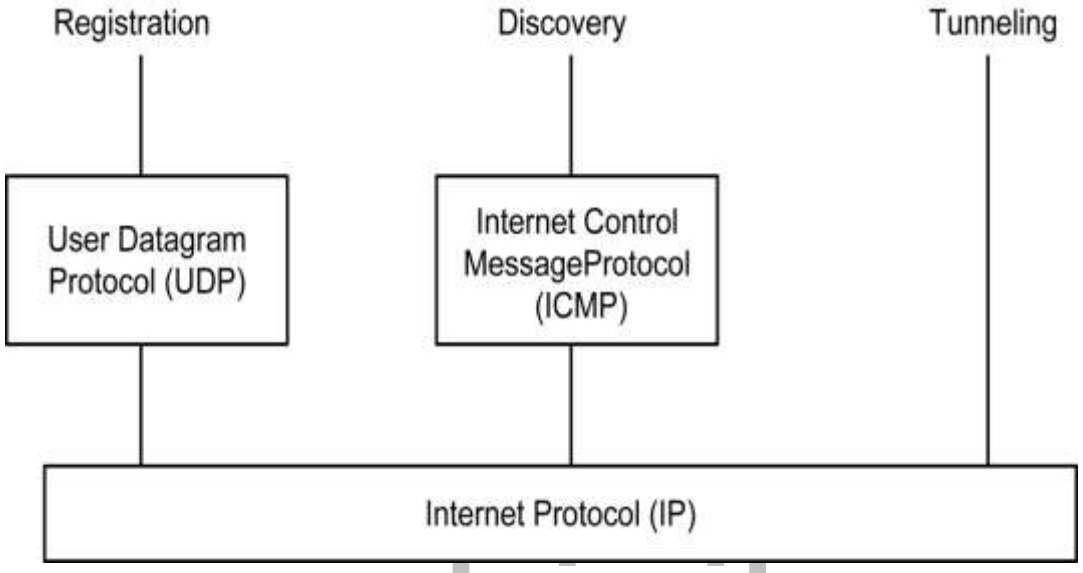
STEP 4: MN after receiving the packet from CN forwards a reply packet to the CN by specifying its own IP address along with the address of the CN.

KEY MECHANISMS IN MOBILE IP (MOBILE IP OPERATION STAGES):

a) Agent Discovery

b) Registration

c) Tunneling & Encapsulation



AGENT DISCOVERY

a) Agent Discovery

A MN uses a discovery procedure to identify prospective home and foreign agents.

- Task of MN to determine its FA & HA:

i) Both HA & FA periodically broadcast Agent Advertisement message.

ii) A MN must discover a HA before it leaves to a home network.

iii) A MN must also discover a FA after it moved to a foreign network

- Uses ICMP Router Discovery Protocol (IRDP).

ICMP Router Discovery Protocol (IRDP) - Enables host to broadcast or multicast to discover the IP address (i.e., COA) of their neighbouring routers (i.e., FA)

- **Agent Discovery methods**:

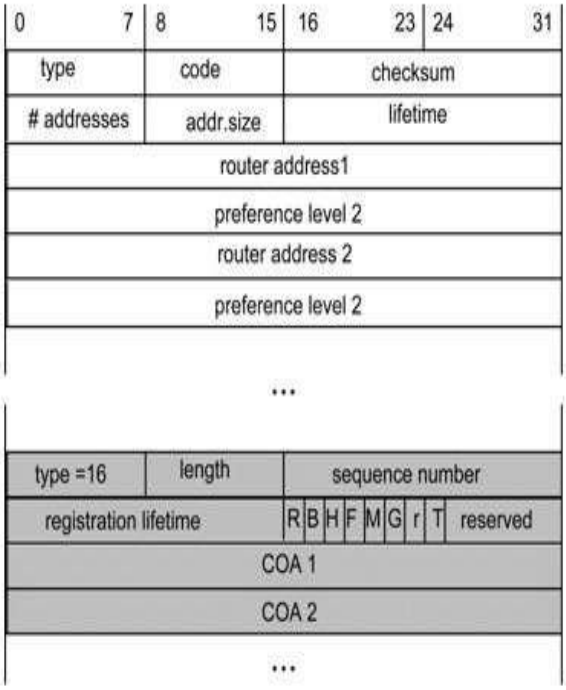
(i) Agent Advertisement
(ii) Agent Solicitation

i) Agent advertisement

Functions:

1. It allows the MN to find whether an agent is its HA or a FA.
2. If it is FA then get the COA.
3. It allows the MN to know the type of services provided by the FA.
4. It allows the MN to know about the allowed registration lifetime or roaming period for visiting foreign network

- **ICMP part**
  - **Type** – 9
  - **Code** – 0 or 16
  - **#addresses** – no. of addresses advertised with this packet
  - **Lifetime** – length of time this advr. is valid
  - **Preference** – most eager router to get new node
- **Extension part – for mobility**
  - **Type** – 16
  - **Length** – depends on no. of COAs provided with the msg.
  - **Seq. No**
  - **Reg. Lifetime** – max. lifetime in sec. a node can request during reg.
  - **R** – reg. , **B** – busy , **H** – HA , **F** – FA , **M & G** – method of encapsulation , **V** - version



Agent advertisement packet Format

Upper part represent ICMP while lower part represent extension needed for mobility.

ii) Agent solicitation:

Rather than waiting for agent advertisements a MN can sent out an agent solicitation.

This solicitation forces any agents on the link to immediately send an agent advertisement.

If MN determines that it is connected to a foreign network, then it obtains a COA.

Types of COA:

(i) Foreign Agent COA - The static IP address of a foreign agent (FA) on a visited network

(ii) Co-located COA - Temporary IP address assigned to the MN.

Represents the current position of the MN on the Foreign network & can be used by only one MN at a time.

A co-located care-of address can be obtained by Dynamic Host Configuration Protocol (DHCP).

Steps:

1. MA (HA, FA) broadcast agent advertisement message at regular intervals.

2. The MN receiving the agent advertisement message observes whether the message is from its own HA & determine whether it is on the home network or on the foreign network.

3. If the MN does not wish to wait for the periodic advertisement, it can send out agent solicitation message that will be responded to by a MA.

After these steps of advertisements or solicitations the MN can now receive a COA, either one for an FA or a co-located COA. The MN knows its location (home network or foreign network) and the capabilities of the agent.

The next step for the MN is the registration with the HA if the MN is in a foreign network

b) Registration

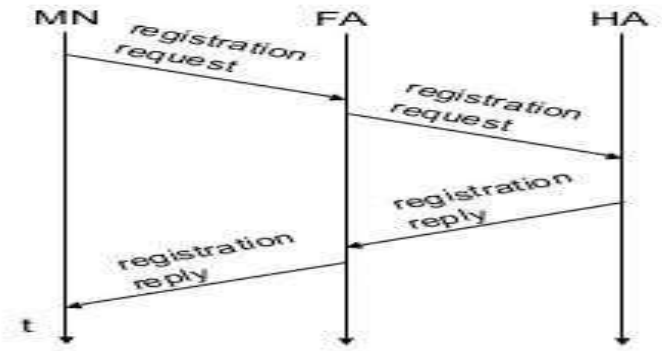
If the MN discovers that it is on the home network, then it operates normally without Mobile IP. If the MN has moved to a new network & obtain the COA from a FA, then this address should be registered with the HA.

- ✓ Registration – A MN uses an authenticated registration procedure to inform the HA of its COA.
- ✓ Registration messages uses UDP Protocol.
- ✓ Registration can be done in two different ways:

  (i) Registration of the MN through FA
  (ii) Directly with HA

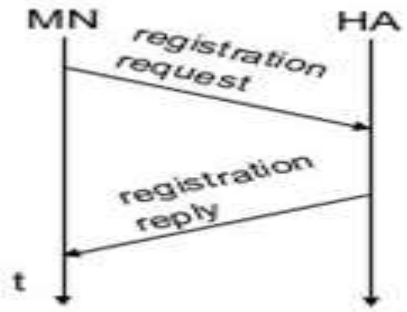
[i] Registration of the MN through FA

If the COA is at the FA;MN sends its registration request containing the COA to the FA which then forward the request to the HA. Now HA will do the mobility binding containing the mobile node's home IP address and the current COA. Then finally the HA Acknowledges via FA to MN.



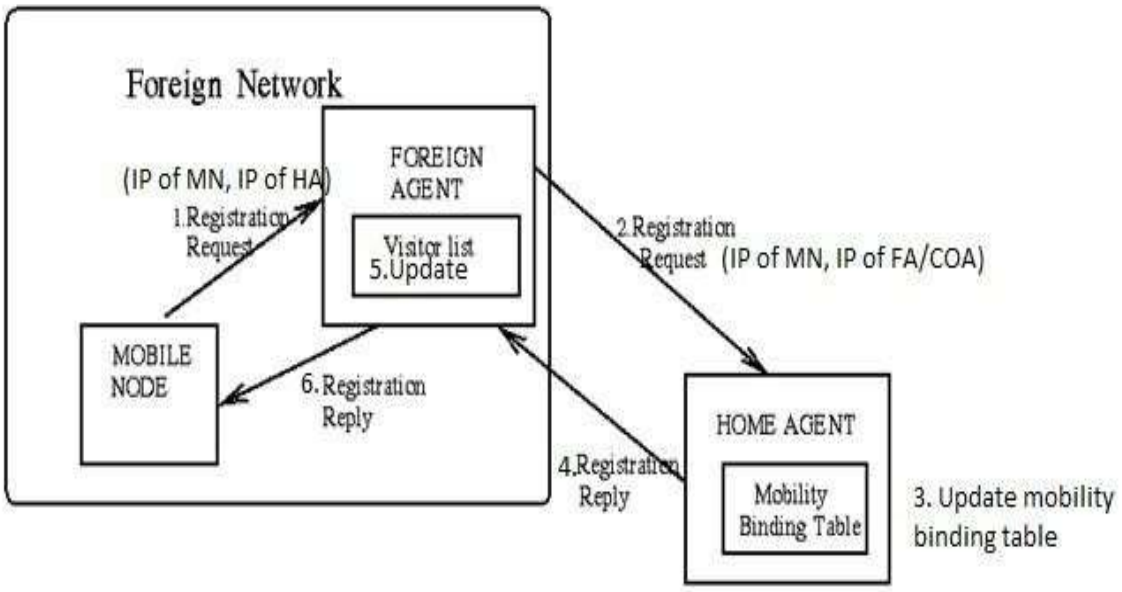
[ii] Directly with HA

If the COA is co-located; MN sends the request directly to the HA and vice versa. Also, a registration procedure for MNs returning to their home network.



REGISTRATION PROCESS:

The registration process involves the exchange of registration requests and registration reply messages. When the mobile node registers by using a foreign agent, the registration process takes the following steps, which is shown in the figure.



1. If MN travels to foreign network, it registers with the FA by sending a registration request message, which includes permanent IP address of the MN & IP address of HA.

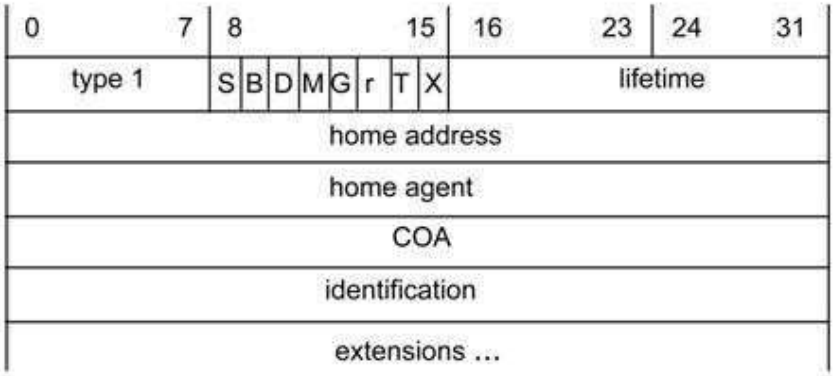
2. The FA in turn performs the registration process on behalf of the MN by sending the registration request message to HA, which includes permanent IP address of the MN & IP address of FA(i.e., COA)

3. When the HA receives the registration request, it updates the “mobility Binding Table”.

4. Then HA sends an acknowledgement (registration reply) to the FA.

5-6. The FA in turn updates its “Visitor list” & relays the reply to the MN.

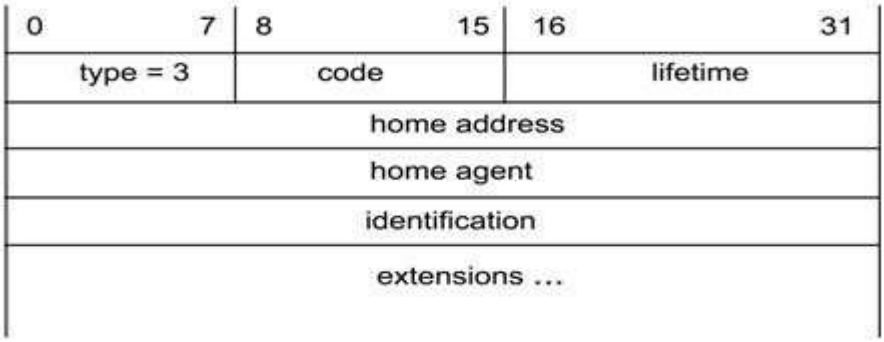
Registration Request Packet format:



- ***UDP packets are used for registration requests.***
- IP source address is the MN interface address and IP destination address is the FA or HA address.
- **Type** – 1 , **S** – an MN wants the HA to ***retain prior mobility binding***

  B – MN want to receive broadcast packets received by HA in home n/w
- **M & G** – ***minimal*** or ***generic*** routing encapsulation.
- ***Destnation port*** – 434
- ***UDP is used because of low overheads and better performance.***

Registration Reply Packet format:



- **Type** – 3
- **code** – result of the registration request
- **lifetime** – validity of the registration ,
- **Home IP address**
- **Home Agent address**
- 64-bit **identification** used to match the registration request with reply

Mobility Binding Table:

Maintained on HA of MN. Maps MN's home address with its current COA.

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Visitor List:

Maintained on FA. Maps MN's home address with its MAC address (address ofNIC) & HA's address.

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

TUNNELLING AND ENCAPSULATION:

Tunneling (data transfer) – Mechanism used to forward IP datagrams from a home address to a care-of address i.e., sending a packet through a tunnel

A tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel endpoint.

Two primary functions:

- ***Encapsulation*** – Mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet. HA encapsulates all the packets addressed to MN & forward them to FA.
- ***Decapsulation*** - The reverse operation, taking a packet out of the data part of another packet FA decapsulates all the packets addressed to MN & forward them.

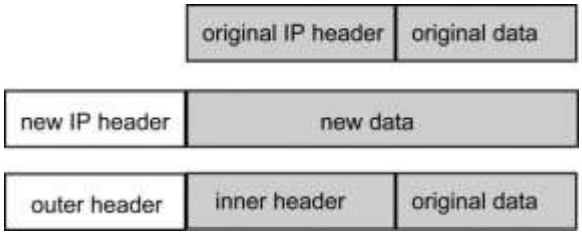
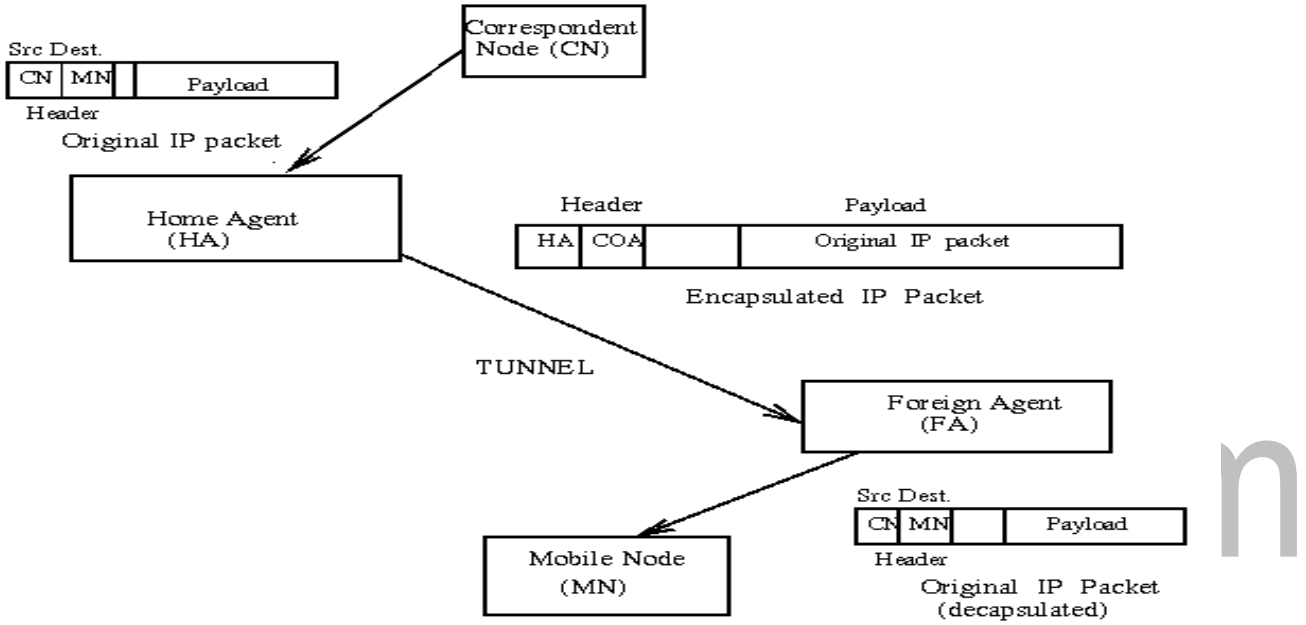


Fig. IP Encapsulation



Steps in Encapsulation:

1. When a HA receives a packet addressed to a MN, it forwards the packet to the COA using IP -within -IP encapsulation

2. Using IP -within -IP , the HA inserts a new IP header in front of the IP header of any datagram.

3. Destination address is set to the COA.

4. Source address is set to the HA's address.

5. After stripping out the 1st header, IP processes the packet again.

There are different ways of performing the encapsulation. They are:

- **IP-in-IP Encapsulation**
- **Minimal Encapsulation**
- **Generic Routing Encapsulation**

(1) IP-in-IP Encapsulation:

This is the mandatory method for Mobile IP.Full IP header added to the original IP packet.The inner IP header source and destination address identify the original sender and the receiver. The new(outer) header contains HA address as source & COA as destination.

- **Ver** – IP protocol version no.
- **IHL** – internet header length
- **TOS** – type of services (copied from inner header)
- **Length** – complete encapsulated packet length.
- **IP id. , flags , frag. offset** – used for fragments
- **TTL** -time to live
- **IP-in-IP** – upper layer protocol
- **IP checksum** – error detection

ver.	IHL	DS(TOS)	length
IP identification		flags	fragment offset
TTL	*IP-in-IP*	IP checksum	
IP address of HA			
Care-of address of 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			

(2) Minimal Encapsulation :

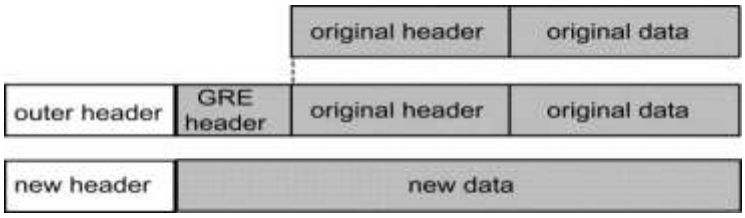
It is an optional method for mobile IP. In IP-in-IP several fields are redundant. Minimal Encapsulation will remove these redundancy.

ver.	IHL	DS(TOS)	length
IP identification		flags	fragment offset
TTL	*min. encap*	IP checksum	
IP address of HA			
Care-of address of COA			
lay. 4. protoc.	S	reserved	IP checksum
IP address of MN			
original sender IP address (if S = 1)			
TCP/UDP/...payload			

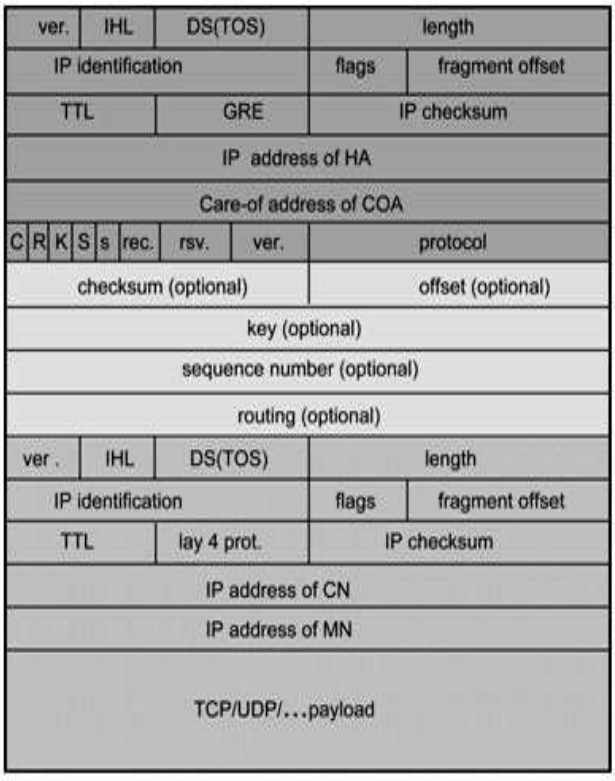
- Type – 55
- If S bit is set , ***the original sender address of the CN*** is included.

(3) Generic Routing Encapsulation (GRE):

Minimal Encapsulation & IP-in-IP only works for IP while GRE also supports other network layer protocols. It allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite. The packet of one protocol suite with the original packet header and data is taken and a new GRE header is prepended. Together this forms the new data part of the new packet. Finally, the header of the second protocol suite is put in front. The outer header is the standard IP header with HA as source address and COA as destination address.



- **Type = 47** for GRE.
- **C** – checksum.
- **R** – indicates if the offset and routing fields are present and contain valid information
- **offset** – represents the offset in bytes for the first source routing entry.
- **routing field** – if present, has a variable length and contains fields for source routing.



key – used for authentication.

K bit - if set indicates if authentication key is present.

S bit - if set indicates if the Sequence number field is present.

rec – recursion control field. This field represents a counter that shows the number of allowed recursive encapsulations.

rsv – reserved for future use. Must be zero.

ver = 0 for GRE version.

Lay 4 protocol specifies the protocol of the packet following the GRE header.

CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.7. MULTICAST ROUTING PROTOCOL(ODMRP)

Multicast is the delivery of a message to a group of destination nodes in a single transmission. Multicast Protocols are

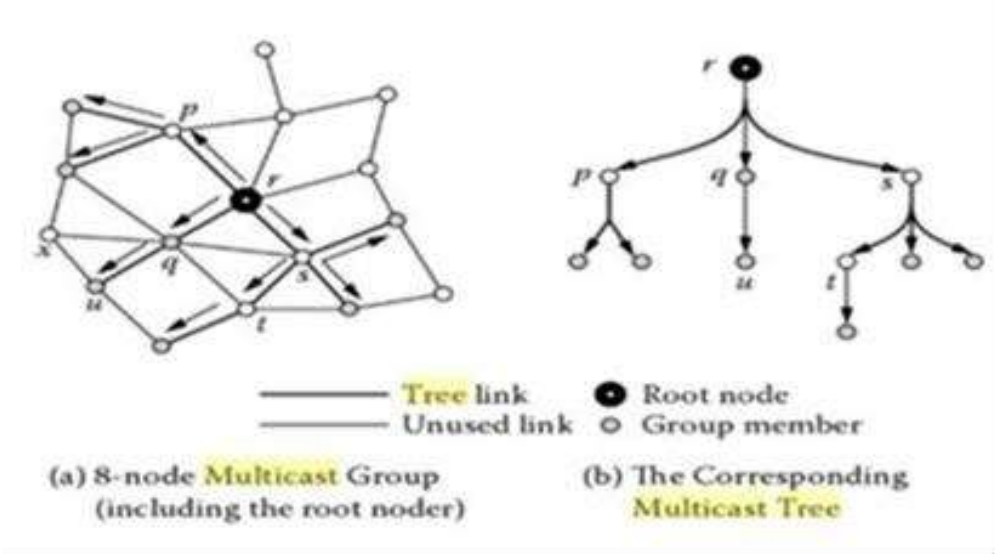
Tree based Protocol and Mesh based Protocol

a) Tree based Protocol

This establishes a single path between any two nodes in the multicast group.

Example: AMRoute, AMRIS

The tree consists of root node(r), three intermediate nodes (p,s,t) and seven group members. For node u, the packet transmission is relayed through two tree links, that is, from r to q and then q to u. To maintain the tree structure even when nodes move, group members periodically send Join Request message.



b) Mesh Based Protocol

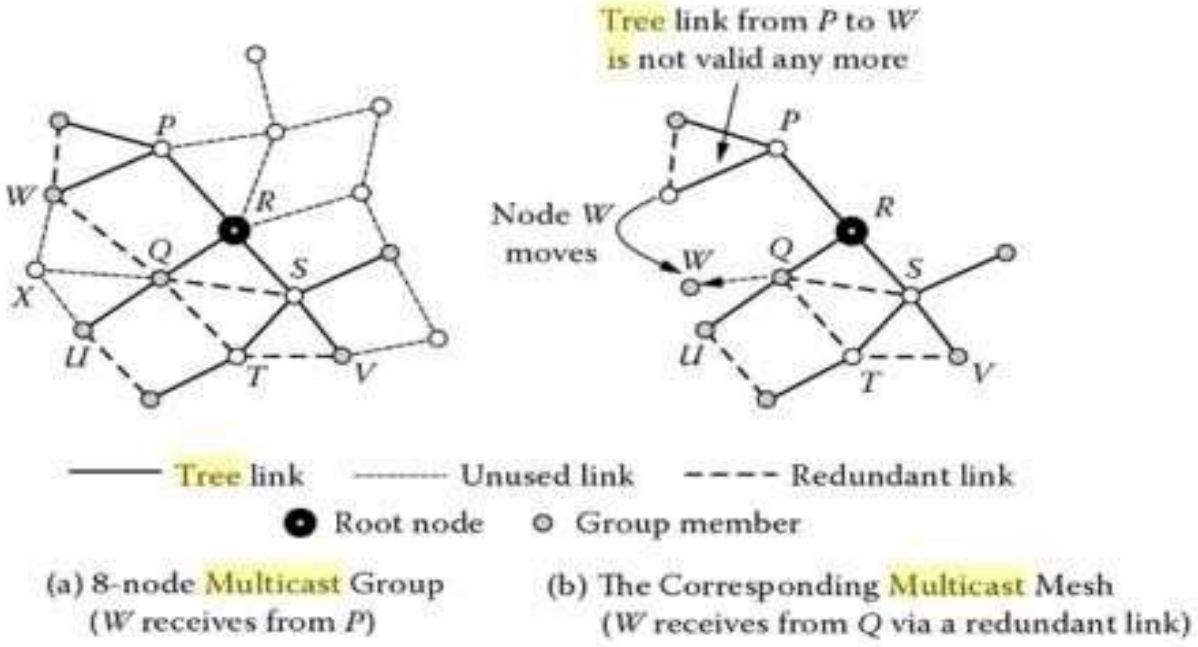
This establishes a multiple path between source - receiver pair.

Example: ODMRP, CAMP

Tree based protocols, may not perform well in the presence of highly mobile nodes because multicast tree structure is fragile and needs to be frequently readjusted.Each node in a mesh can have multiple parents.Multiple links exist and other links are immediately available when the primary link is broken due to node mobility. This avoids frequent reconfigurations. Sending a Packet from R to U involves three transmissions(R,Q,U) & fourteen receives(5 neighbours of R,6 neighbours of Q and 3 neighbours of U).

For eg, the transmission from node Q is received not only by U but also be neighbour nodes R,S,T,W and X; the redundant link from Q to W may be useful when the path from P to W is broken

Drawback of this scheme is that multiple copies of the same packet are forwarded through the mesh.



(a) 8-node Multicast Group (W receives from P)

(b) The Corresponding Multicast Mesh (W receives from Q via a redundant link)

ON-DEMAND MULTICAST ROUTING PROTOCOL (ODMRP)

Provides richer connectivity among multicast members using a mesh based approach.

- Supplies multiple route for one particular destination.
- Helps in case of topology changes & node failures.
- Use the concept of Forwarding Group - A subset of nodes forwards multicast packets.
- Operation of ODMRP:

1. A sender node wishing to send multicast packets periodically floods a JOIN REQUEST to entire network.

2. A Node receiving a non-duplicate JOIN REQUEST, stores the upstream node ID (i.e. backward learning) into routing table & rebroadcasts the packet.

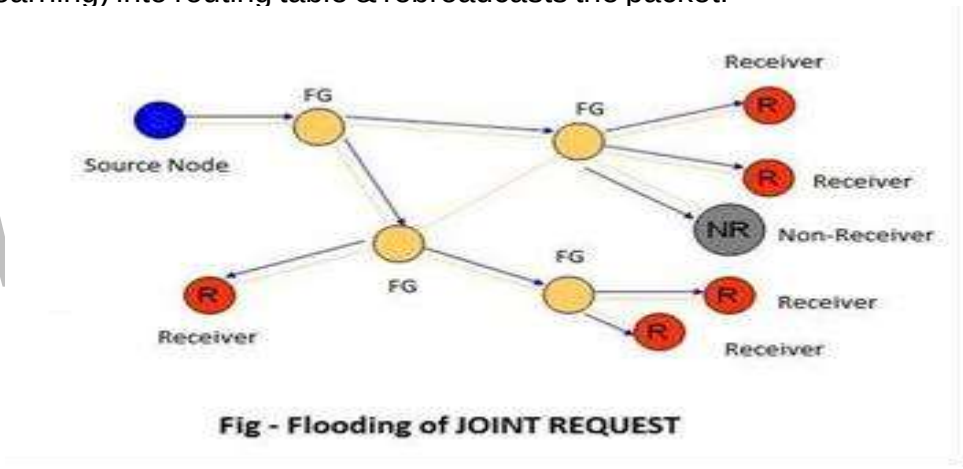


Fig - Flooding of JOINT REQUEST

3. A multicast receiver getting the JOIN REQUEST creates or updates the source entry in its member table.

4. As long as valid entries in receiver's member table, JOIN TABLE are broadcasted periodically.

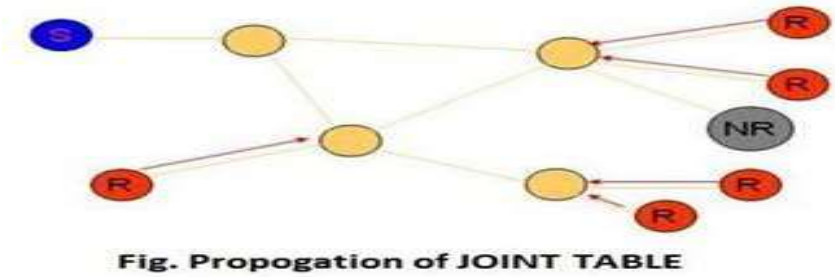


Fig. Propogation of JOINT TABLE

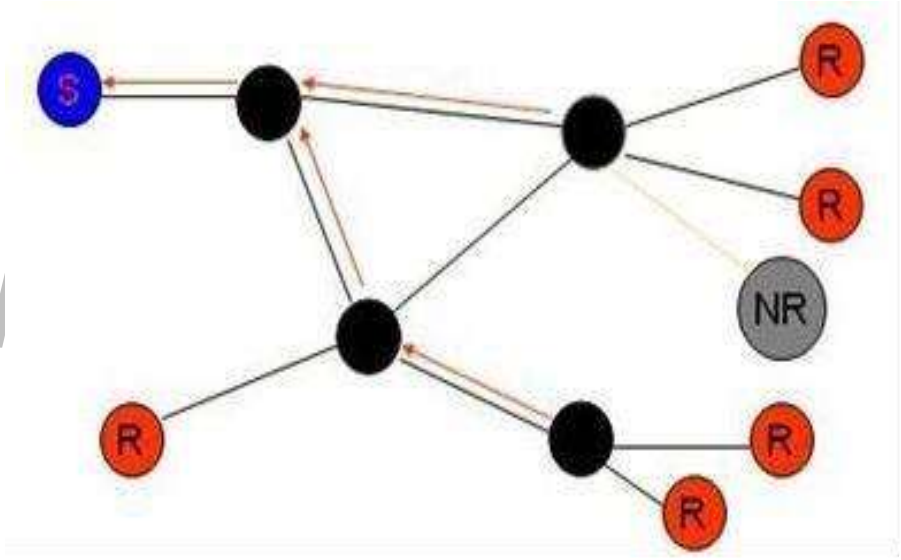
5. An intermediate node, receiving the JOINT TABLE, compares it's Node ID with the entries of that table.

6. If there's a match, it is a member of the forwarding group. Then it sets FG-FLAG & broadcasts its JOIN TABLE.

7. This process is going to create a mesh between all forwarding group members.

8. JOIN TABLE is propagated by each forwarding Group member until it reaches source via a shortest path.

9. Routes from source to receivers builds a mesh of nodes called "Forwarding Group"



CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.4. PROACTIVE PROTOCOLS (Table-driven routing protocol)

Maintain the global topology information in the form of tables at every node.

These tables are updated frequently in order to maintain consistent and accurate network state information.

EX: ***DSDV, WRP, and STAR.***

DESTINATION-SEQUENCED DISTANCE-VECTOR ROUTING (DSDV)

Based on Proactive method

Enhanced version of the distributed Bellman-Ford algorithm or Distance Vector(DV) Routing Protocol

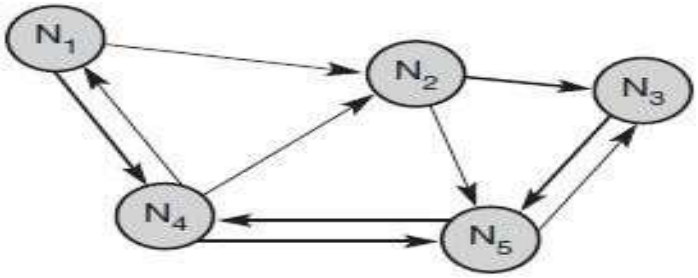
DSDV adds two things to the distance vector algorithm

Sequence Number:

- ✓ Each routing advertisement comes with a sequence number.
- ✓ Within ad-hoc networks, advertisements may propagate along any paths.
- ✓ Sequence numbers help to apply the advertisements in correct order.
- ✓ This avoid the loops in the network.

Damping:

- ✓ Transient changes in topology that are of short duration should not weaken the routing mechanisms.
- ✓ Unstable changes in the topology are not forwarded



Example Ad-hoc network

For each node N1 maintain a table that contain;

- The next hop toward this node
- The metric (number of hops)
- The sequence number
- The time at which the path has been installed first.

Important steps in the operation of DSDV:

1. Each router(node) in the network collects route information from its neighbours.
2. After gathering information, the node determines the shortest path to the destination based on the gathered information.
3. Based on the gathered information, a new routing table is generated.
4. The router broadcasts this table to its neighbours. On receipt by neighbours, the neighbour nodes recompute their respective routing tables.
5. This process continues till the routing information becomes stable.

Advantages

- Simple
- Loop free through destination seq. numbers
- No latency caused by route discovery

Disadvantages

- No sleeping nodes
- Overhead: most routing information never used

CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.5. REACTIVE PROTOCOLS (On-demand routing protocol)

They execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination.

i.e., a route is discovered only when it is necessary.

Source initiates route discovery

Two step process

- Route Discovery
- Route Maintenance

Route discovery is expensive

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

(a) DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

DSR is a source initiated on-demand(or reactive) routing protocol for ad-hoc network. Designed to restrict the bandwidth consumed by packets by eliminating the periodic table-update messages i.e., the nodes do not need to exchange the routing information periodically, which helps to reduce the bandwidth overhead. Each mobile node participating in the protocol maintains a "routing cache" which contains the list of all routes that the node has learnt

DSR works in 2 phases:

(a) Route Discovery:

• Allows any host to dynamically discover the route to any destination in the ad-hoc network.

Route Discovery Process takes place by :

1. Broadcasting a route request (RREQ) packet to all its neighbours.

The Route request (RREQ) packet contains the

i) Source address

ii) Request id

iii) Route Record, in which the sequence of hops traversed by the request packet before reaching the destination is recorded.

2. A node after receiving RREQ

2.i. If the node is an intermediate node then

- If the message has the same ID i.e. has seen it before, then the node discards this message,
- If not, the node appends its own address to the route record in the ROUTE REQUEST message then propagates the message to the next hop neighbours.

2.ii. If the node is the Target (Destination) then

- Returns a Route Reply (RREP) message to the sender
- Copies the accumulated route record from RREQ into RREP

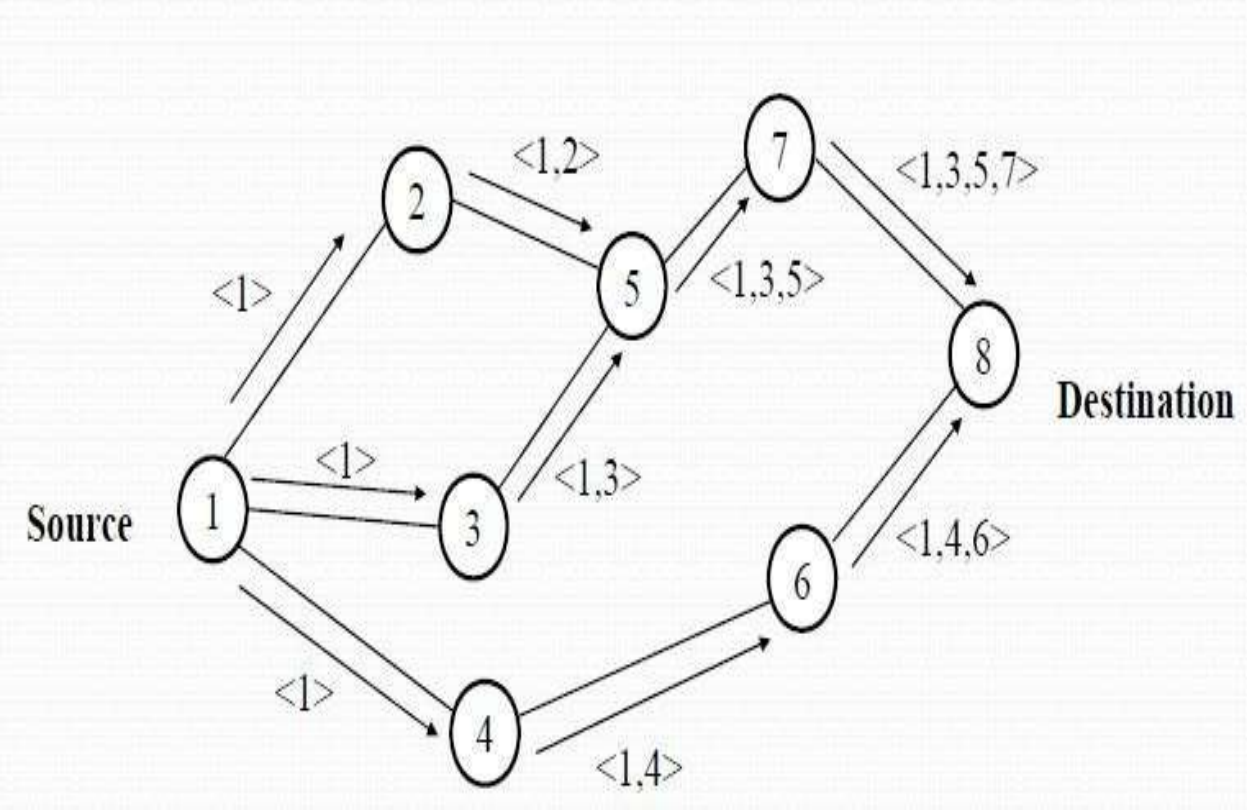


Fig. Broadcasting the RREQ packets

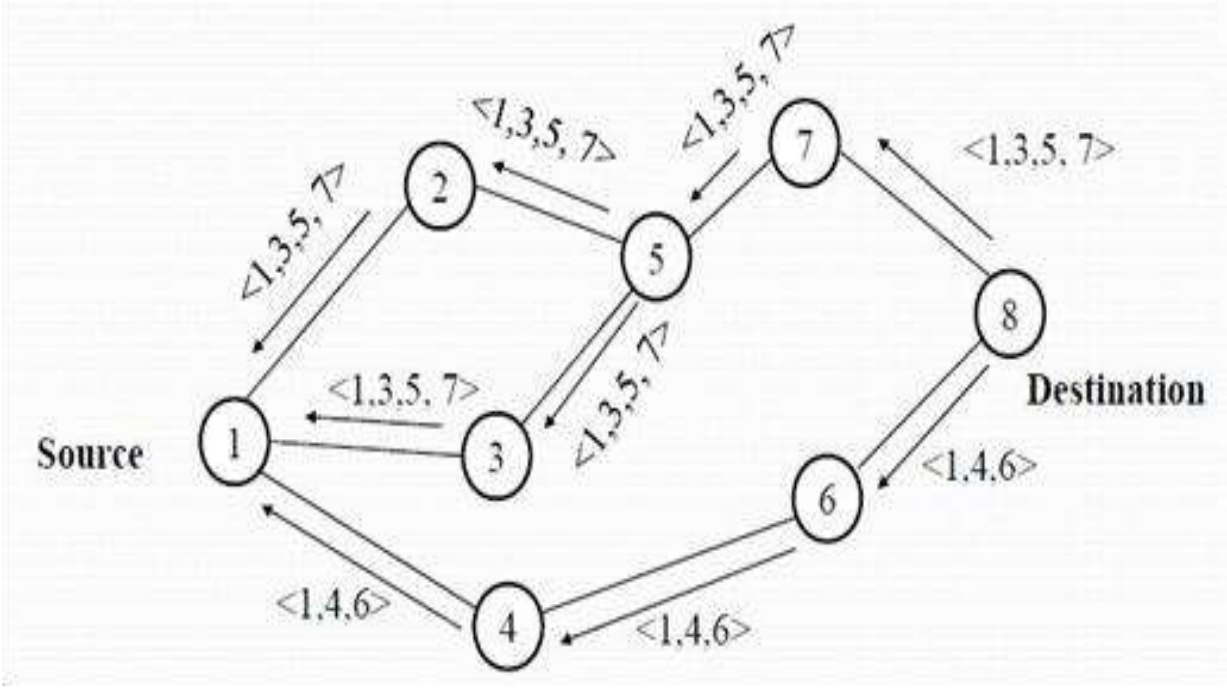


Fig. Propagation of RREP packets back to source

(b) Route Maintenance:

A known route can get broken due to the movement of some node or the battery of a node getting exhaused.

Route maintenance : The process of monitoring the correct operation of a route in use & taking corrective action when needed.

Steps:

1. When a node detects that one of its next hop neighbour node is not responding, it sends back a route error(RERR) packet containing its own address and the address of the hop that is not working

2. As Soon as source node receives the RERR message it deletes the broken link route from its cache.

3. If it has another route to the destination, it starts to retransmit the packet using the alternative route.

4. Otherwise it initiates the route discovery process again.

The basic message set consists of:

- RREQ – Route request
- RREP – Route reply
- RERR – Route error
- HELLO – For link status monitoring

Advantages:

- A perfect route is discovered always.
- Highly efficient.
- Low bandwidth Consumption.

Drawback:

- Packet header size (Non Uniform Packet Size) grows when intermediate node increases.
- Flood of route requests may potentially reach all nodes in the network

(b) AD HOC ON-DEMAND DISTANCE VECTOR ROUTING (AODV)

It is based on Reactive method

DSR vs AODV:

Major problem of DSR is its non-uniform packet size because it includes source routes in its packet header which degrades the performance. If a packet is large, it has to be split into smaller packets. The packet size in AODV is uniform unlike DSR.AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes.

AODV holds the desirable feature of DSR that routes are maintained only between nodes which need to communicate. Route is established only when it is required by a source node for transmitting data packets .Make use of hop-by-hop routing, sequence numbers and beacons.

Steps:

1. The node that needs a route to a specific destination generates a route request(RREQ).

2. The route request(RREQ) is forwarded by intermediate nodes which also learn a reverse route from the source to themselves.

3. When the request reaches a node with route to destination, it generates a route reply(RREP) containing the number of hops required to reach the destination.

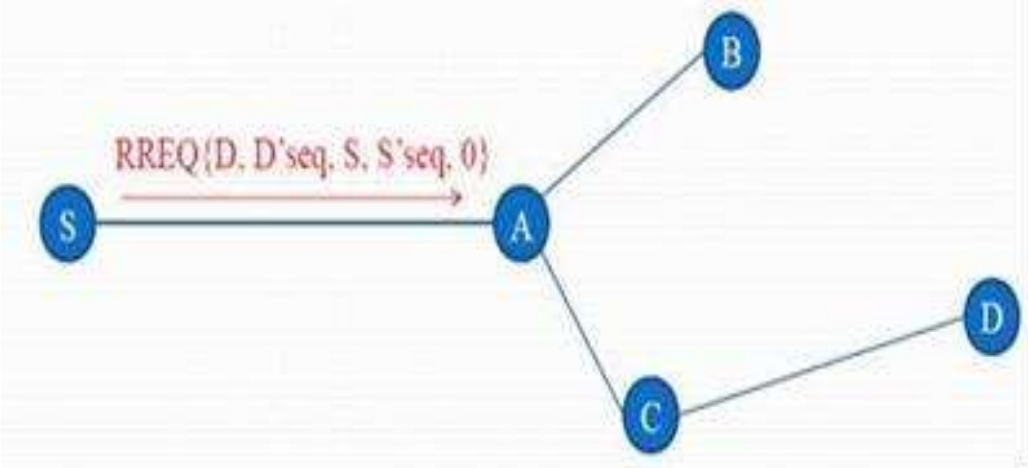
4. All nodes that participate in forwarding this reply to the source node create a forward route to destination.

5. This route created from each node from source to destination is a hop-by-hop route.

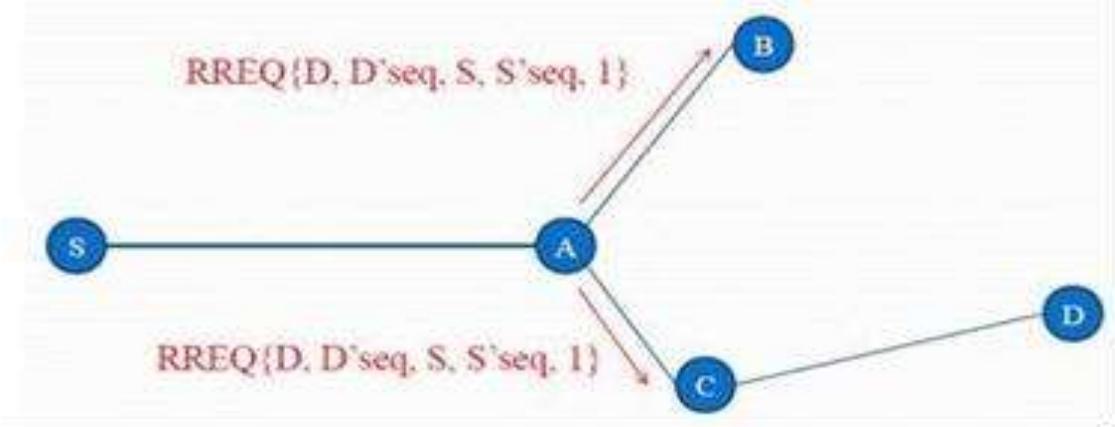
Example: Suppose Node S needs a routing path to Node D

1. Node S creates a RREQ packet & broadcasts to its neighbours.

RREQ [D's IP addr, Seq#, S's IP addr, hopcount]

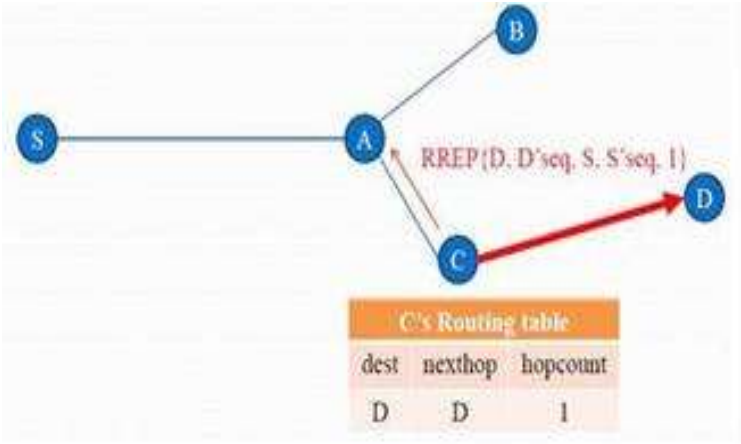


2. Node A rebroadcasts RREQ to all its neighbours.

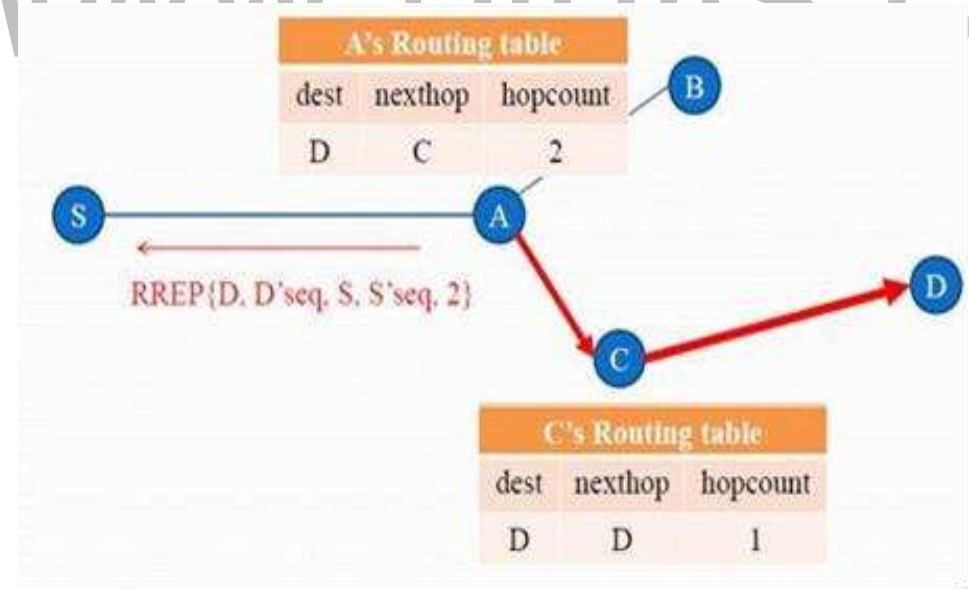


3. Since, Node C known a route to Node D

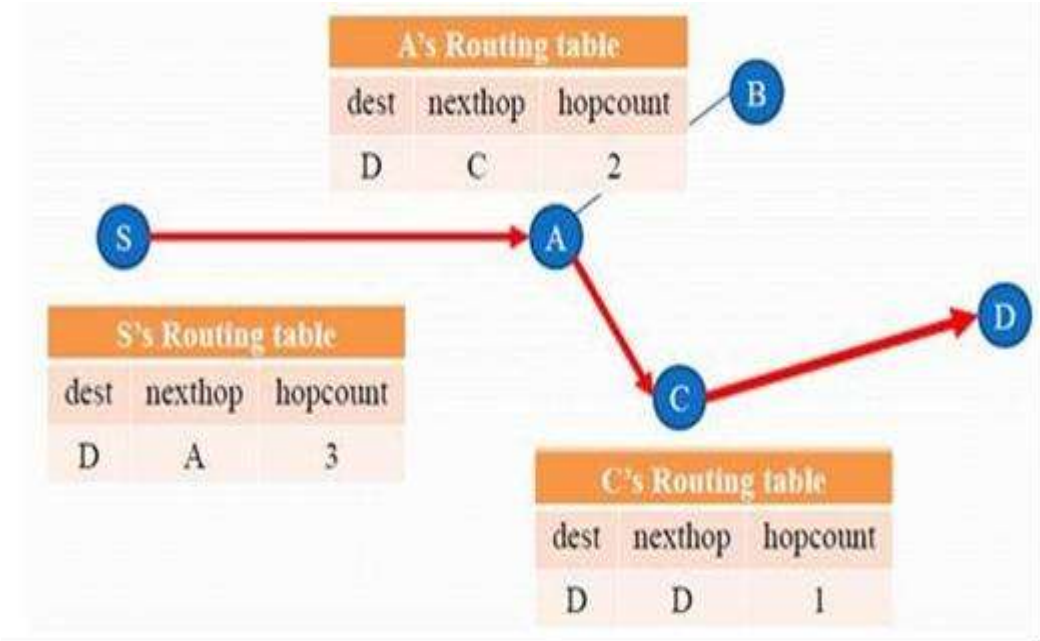
- Node C creates a RREP & unicasts RREP to A.
- Set forward path in C's routing table.



4. Node A creates a RREP & unicasts RREP to S
5. Set forward path in A's routing table



6. Set forward path in S's routing table



Difference between DSR, DSDV & AODV

Property	DSR	DSDV	AODV
Loop Free	Yes	Yes	Yes
Multicast Routes	Yes	No	No
Unidirectional Link	Yes	No	No
Periodic Broadcast	No	Yes	Yes
Routes maintained	Route Cache	Route Table	Route Table
Reactive	Yes	No	Yes

CS8601 -MOBILE COMPUTING

UNIT 3

MOBILE NETWORK LAYER

3.8. VANET: VEHICULAR AD - HOC NETWORK

The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network.

Vehicular Ad Hoc Networks (VANETs) are created by applying the principles of Mobile ad hoc networks (MANETs) - the spontaneous creation of a wireless network for data exchange - to the domain of vehicles. They are a key component of Intelligent Transportation Systems (ITS).

The term VANET became mostly synonymous with the more generic term inter-vehicle communication (IVC).

VANET is an application of mobile ad hoc network. More precisely a VANET is self-organised network that can be formed by connecting vehicle aiming to improve driving safety and traffic management with internet access by drivers and programmers.

WORKING OF VANET

VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range.

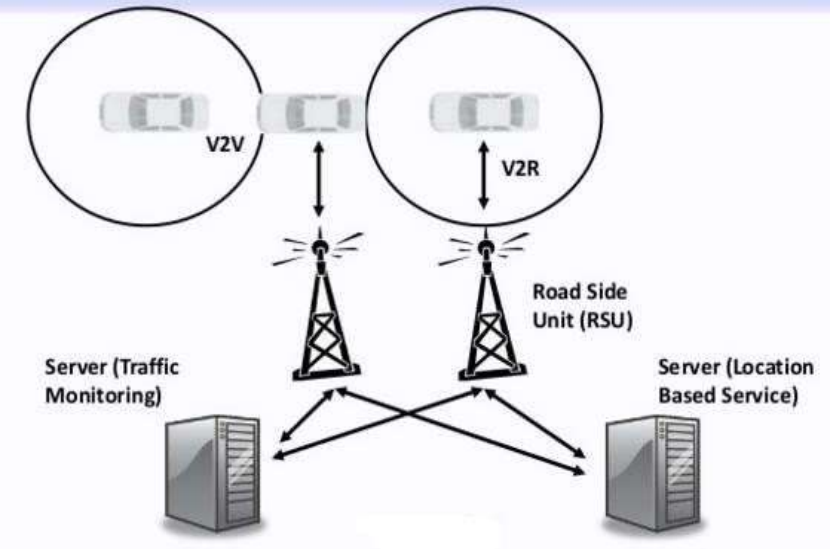
As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created.

It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes.

COMMUNICATION IN VANET

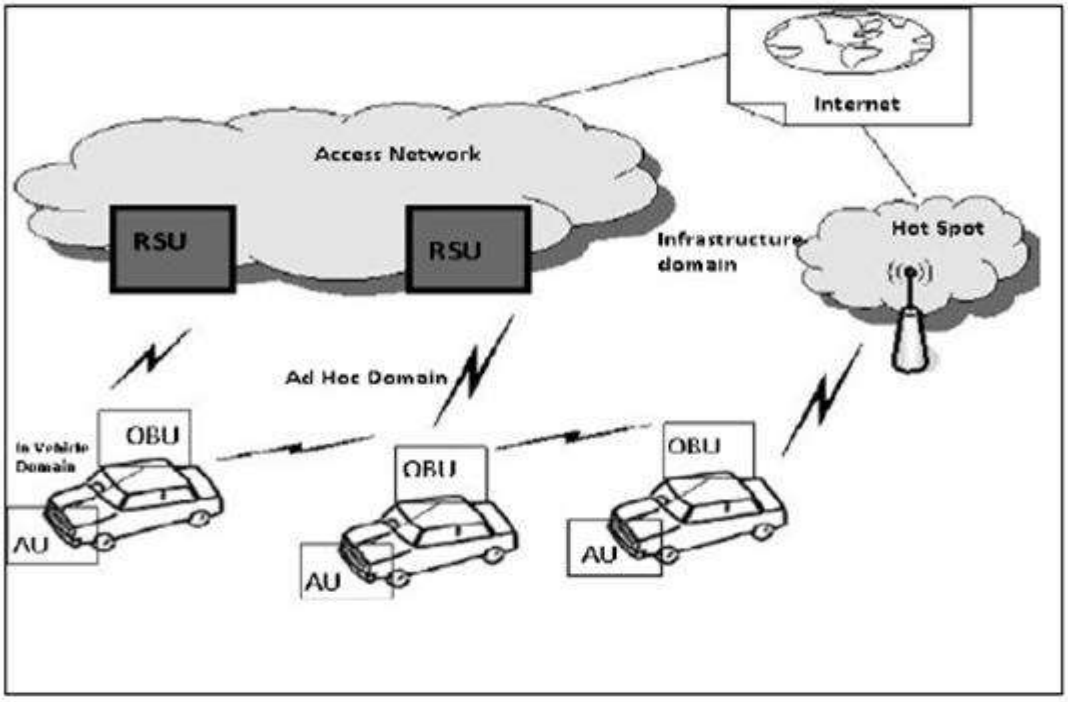
Two types of communication are provided in the VANET.

- First a pure wireless ad hoc network where vehicle to vehicle without any support of infrastructure.
- Second is communication between the road side units (RSU), a fixed infrastructure, and vehicle.



ARCHITECTURE OF VANET

Each node in VANET is equipped with two types of unit i.e. ***On Board Unit(OBU)*** and ***Application Unit (AU).*** OBU has the communicational capability whereas AU executes the program making OBU's communicational capabilities. An RSU can be attached to the infrastructure network which is connected to the Internet.



TECHNOLOGY USED IN VANET

To establish a VANET, IEEE has defined the standard 802.11p or 802.16 (WiMax). A Dedicated Short Range Communication (DSRC) is proposed which is operating on 5.9GHz band and uses 802.11 access methods. It is standardized as 802.11p which provides short range communication with low latency.

CHARACTERISTICS OF VANET

High Mobility: The nodes in VANETs usually are moving at high speed. This makes harder to predict a node's position and making protection of node privacy

Rapidly changing network topology: Due to high node mobility and random speed of vehicles, the position of node changes frequently. As a result of this, network topology in VANETs tends to change frequently.

Unbounded network size: VANET can be implemented for one city, several cities or for countries. This means that network size in VANET is geographically unbounded.

Frequent exchange of information: The ad hoc nature of VANET motivates the nodes to gather information from the other vehicles and road side units. Hence the information exchange among node becomes frequent.

Wireless Communication: VANET is designed for the wireless environment. Nodes are connected and exchange their information via wireless. Therefore some security measure must be considered in communication.

Time Critical: The information in VANET must be delivered to the nodes with in time limit so that a decision can be made by the node and perform action accordingly.

APPLICATIONS OF VANET

i) Safety Related Application:

These applications are used to increase the safety on the roads. These applications can be further categorised in following way.

Collision Avoidance: If a driver gets a warning message on time then the collision can be avoided.

Cooperative Driving: Drivers can get traffic related warning signals & these signals can co-operate the driver for an uninterrupted and safe driving.

Traffic optimization: Traffic can optimized by the use of sending signals like jam, accidents etc. to the vehicles so that they can choose their alternate path and can save time.

ii) User Based Application:

These applications provide the user infotainment. A VANET can be utilised to provide following services for the user apart from safety:

Peer to peer application: These application are useful to provide services like sharing music, movies etc. among the vehicles in the network.

Internet Connectivity: People always want to connect with the Internet all the time. Hence VANET provides the constant connectivity of the Internet to the users.

Other services: VANET can be utilised in other user based application such as payment service to collect the tall taxes, to locate the fuel station, restaurant etc.

CHALLENGING ISSUES IN VANET

Network Management: Due to high mobility, the network topology and channel condition change rapidly.

Congestion and Collision Control: The unbounded network size also creates a challenge. The traffic load is low in rural areas and night in even urban areas. In rush hours the traffic load is very high and hence network is congested and collision occurs in the network.

Environmental Impact: VANETs use the electromagnetic waves for communication. These waves are affected by the environment.

MAC Design: VANET generally use the shared medium to communicate hence the MAC design is the key issue.

Security: As VANET provides the road safety applications which are life critical therefore security of these messages must be satisfied

SECURITY ISSUES IN VANET

Lack of physical boundary: Each mobile node functions as a router & forwards packets from other nodes. AS a result, network boundaries become blurred. So it is difficult to deploy firewalls or monitor the incoming traffic.

Low power RF transmission: It if possible for a malicious node having high power RF transmission capability to continuously transmit & monopolise the medium & cause its neighbouring nodes or the entire targeted MANET to wait endlessly for transmitting their messages. Also signal jamming can lead to denial-of-service(DOS) attack.

Limited computational capabilities: Nodes in an ad hoc network usually have limited computational capabilities. It therefore becomes difficult to deploy compute-intensive security solutions such as setting up a public-key cryptosystem. Inability to encrypt messages invites a host of security attacks such as spoofing as well as several other forms of routing attacks.

Limited power supply: Since nodes normally rely on battery power, an attacker might attempt to exhaust batteries by causing unnecessary transmissions to take place at the targeted node or might cause excessive computations to be carried out by the targeted nodes.

Real time Constraint: VANET is time critical where safety related message should be delivered with 100ms transmission delay. So to achieve real time constraint, fast cryptographic algorithm should be used. Message and entity authentication must be done in time.

Data Consistency Liability: In VANET even authenticate node can perform malicious activities that can cause accidents or disturb the network. Hence a mechanism should be designed to avoid this inconsistency. Correlation among the received data from different node on particular information may avoid this type of inconsistency.

Low tolerance for error: Some protocols are designed on the basis of probability. VANET uses life critical information on which action is performed in very short time. A small error in probabilistic algorithm may cause harm.

MANET Vs VANET

MANET	VANET
Collection of mobile nodes that communicate with each other over bandwidth constrained wireless links without any infrastructure support.	Nodes(vehicles) can communicate with certain roadside infrastructures or base stations.
The node movement is more random in nature	The node mobility is constrained to the road topologies.
Power is a major constrained	The battery power available in a vehicle is quite adequate.
Cost of production is cheap	Expensive
Change in network topology is slow	Frequent & very fast
Node lifetime depends on power resource	Depends on lifetime of vehicles
Multi-hop routing is available.	Weakly available.
Attribute based addressing scheme	Location-based