

11) compare MANET's VS VANET's ?

Ans

MANET

VANET

1. production cost of
MANET is cheap
as compared to
VANET

1) Much Expensive

2) Low Mobility

2) High Mobility

3) change in network
topology orientation is
slow

3) change in network
topology orientation
is fast

4) Sparse Node density

4) Node density
is frequent variables

5) MANET HAVE 100
kps bandwidth
available

5) VANET have
1000kps bandwidth
available

6) It ranges upto 100m

6) 500m range
available in VANET

7) MANET node lifetime
depend on power resources

7) Depend on
lifetime vehicle

8) MANET have medium
reliability

8) MANET have high
reliability

9) Attribute based addressing
scheme

9) location based
addressing scheme

10) availability of Multihop
Routing

10) Weakly available
Multihop Routing

Qns What is WAP?

The Wireless Application protocol is an open, global specification that empowers mobile users with wireless devices to easily access and interact with information and services instantly.

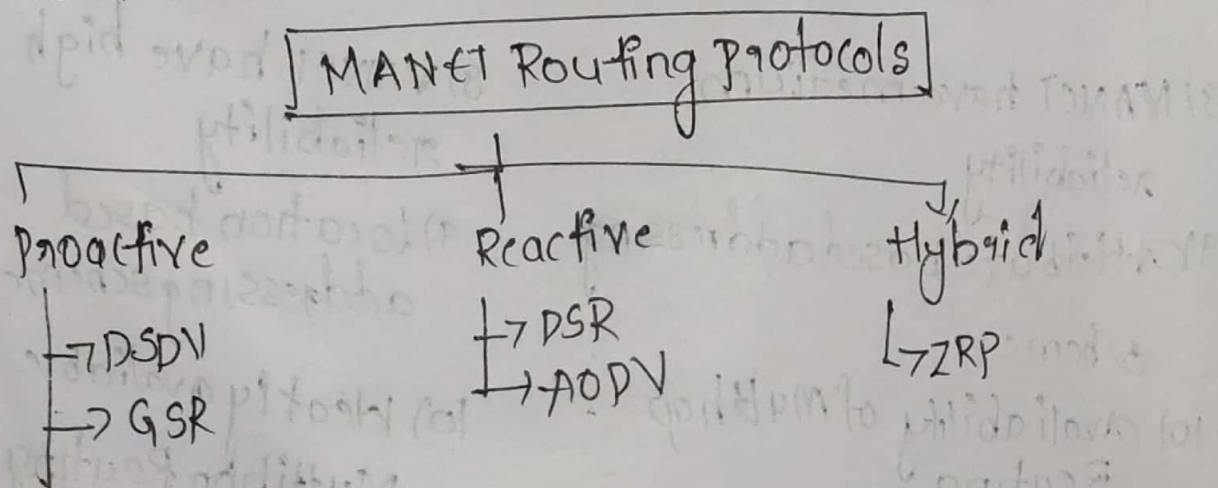
2) ~~W~~ Discuss about different protocols in Manets?

Ans In Mobile Adhoc Network (MANET)

nodes donot know the topology of their network. instead they have to discover it by their own as the topology in Ad hoc network.

is dynamic topology.

The basic rule is that a new node whenever enters into an ad-hoc network must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.



1) pro-active routing protocols (14Q)

These are also known as table-driven protocols. Each node in the network maintains a separate routing table which contains the information of the routes to all possible destination nodes. Since the topology in an ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes.

It has a limitation that it doesn't work for large networks, as the entries in the routing table become large since they need to maintain the route info to all possible nodes.

1) DSDV (Destination Sequenced Distance Vector Routing Protocol)

It is a pro-active table-driven protocol.

It actually extends the distance vector routing protocol of the networked networks as the routing is based upon the Bellman-Ford algorithm.

Distance vector routing protocol is not suited for mobile ad-hoc network due to count-to-infinity problem. Hence as a solution, Destination Sequenced Distance Vector Routing Protocol came into the picture.

Destination sequence number is added with every routing table entry in the routing table maintained by each node.

⇒ A node will ~~increase~~ include the new update in the table only if the entry consists of a new updated route to destination with higher sequence number.

2) Global State Routing (GSR)

⇒ It is a proactive table-driven protocol.

⇒ It actually extends the link state routing of the wired networks.

⇒ It is based on Dijkstra's routing algorithm.

⇒ Link state routing protocol was not suited

for mobile ad-hoc networks because in it,

each node floods the link state routing

info directly into the whole network

i.e. Global Flooding which may lead to

the congestion of control packets in the

network.

Hence as a solution Global State Routing

Protocol (GSR) came into the picture.

Global state routing doesn't flood link state

routing packets globally into the network

=> In GSR, each of the mobile node maintains one list and three tables namely adjacency list, topology table, nexthop table and distance table.

a) Reactive routing protocols

These are also known as on demand routing protocols.

=> In this protocol the route is discovered only when it is needed.

=> The process of route discovery occurs by flooding the route request packets throughout the mobile network.

=> It consists of two major phases namely route discovery and route maintenance.

Dynamic Source Routing protocol (DSR).

It is a reactive / on-demand routing protocol.

=> In this type of routing, the route is discovered only when it is required / needed.

=> The process of route discovery occurs by flooding the routing request packets throughout the mobile network.

It consists of two phases

1) Route discovery

=> This phase determines the most optimal path for the transmission of packets b/w source and destination mobile nodes

=> Route Maintenance :

This phase performs the maintenance work of the route as the topology in mobile ad hoc

network is dynamic in nature and hence

there are many cases of link break resulting

in the network failure b/w mobile nodes

2) Ad hoc on demand vector Routing protocol (AODV)

=> It is a reactive on-demand routing protocol

=> It is the extension of dynamic source routing protocol (DSR). and it helps to remove disadvantages of DSR.

=> In DSR when after route discovery when source

mobile node sends the data packet to dest

it also contains the complete path

in its path header. Hence as

3) explain about DHCP and how client initialization is done via DHCP.

Ans Dynamic Host Configuration Protocol is an application layer protocol which is used to provide

1) Subnet Mask (option - eg. 255.255.255.0)

2) Router address (192.168.1.1)

3) DNS address

4) Vendor class identifier

DHCP is based on client server model and based on discovery, offer, request and Ack.

DHCP port number for server is 67 and for the client is 68.

=> It is a client server protocol which uses UDP services.

=> IP address is assigned from the pool of IP addresses.

=> In DHCP client and server exchange 4 DHCP messages in order to make a connection also called DORA process.

=> but there are 8 DHCP messages in the process.

These messages are given as below:-

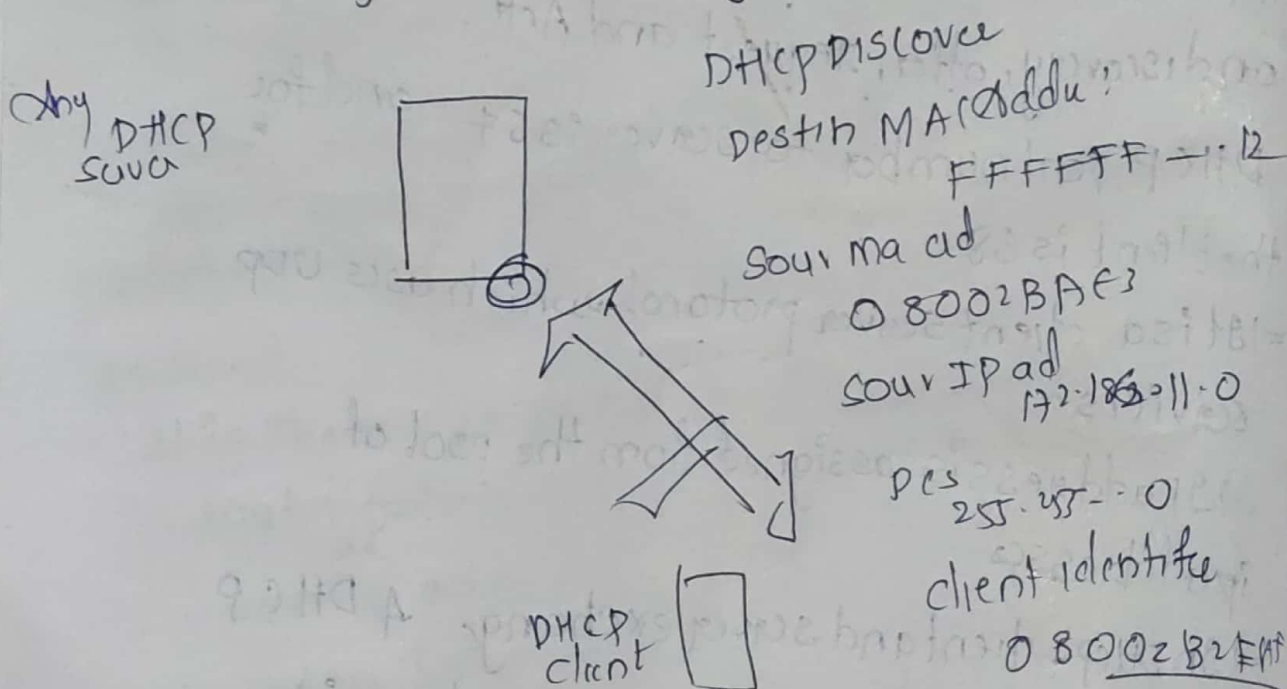
1) DHCP discover message

This is a first message generated in the communication process b/w server and client.

=> This message is generated by client in order to discover if there is any DHCP server are present in a network or not.

This message is broadcasted to all the devices present in a network to find the DHCP server.

=> This message is 576 bytes long



MACs shown in fig source mac add is
08002B2EAF2A des. mac F-12

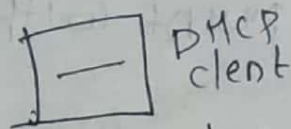
Source IP address is 0.0.0.0
and destination IP is 255.255.255.255

As the discover message is broadcast to find
out the DHCP server therefore broadcast IP
address and MAC add is used

2) DHCP offer message

The server will respond to the host in this message
specifying the unleased IP address and other
TCP configuration info. This message is broadcast
by server. Size of the message is ~~316~~ 342 bytes.

If there are more than one DHCP server then
client accept only first DHCP offer message. Also a server
is specified in packet in order to identify the server.



DHCP offer
Des MAC add: F-12

Des Source MAC add = 08002B2EAF2A

Source IP: 172.16.32.12

Des IP: 255.255.255.255

Offered IP address: 172.16.32.51

Server identifier: 172.16.32.12



Lease length: 72 hours
Client identifier: 08002B2EAF2A

Now for the offer message source MAC address
192.16.32.12 and destination IP address
255.255.255.255

source MAC is 00AA00123456, destination mac address
(FF - FF)

Here offer message is broadcast to all the by source
destination IP is broadcast IP

source IP address is source IP address

Also the server has provided the offered IP
address 192.16.32.11 and lease time of 42 hours

and server identifier: 192.168.0.2 B2AT2A
client

3) DHCP request message

When a client receives the offer message, it
responds by ~~send~~ broadcasting a DHCP
request message. The client will produce gratuitous
ARP to check if there is any host present with

same IP address.

If no reply by other host then there is no host
with same TCP configuration and it ~~is~~
message is broadcasted to server showing
the acceptance of IP address. Client ID is
also added in this message

DHCP acknowledgment message

On response to request message received the server will make an entry with specified client ID and bind the IP address offered with lease time. Now client will have IP address provided by server.

DHCP negative acknowledgment message

Whenever a server receives a request for IP address that is invalid according to scopes that is configured, it sends DHCP NAK message to client. Eg. When the server has no IP address or pool is empty.

3) DHCP decline

If DHCP client determines the offered configuration parameters are different it sends DHCP decline message to server.

4. DHCP release

A DHCP client sends DHCP release packet to server to release IP address and cancel any remaining lease time.

5) DHCP inform

If a client address has obtained IP address manually then client uses a DHCP inform to obtain other local configuration parameters.

In reply to the DHCP inform message, DHCP server sends
Ack message with local config suitable for
client without allocating new IP address.

4) Write short notes on Mobile IP Agent Discovery?

Ans \Rightarrow Mobile Internet protocol

\Rightarrow It is designed by Internet Engineering Task
Force (IETF)

\Rightarrow It is a standard communication protocol
that is designed to allow a mobile device user
to move from one place network to another
network without changing IP address.

\Rightarrow Requirements of Mobile IP:

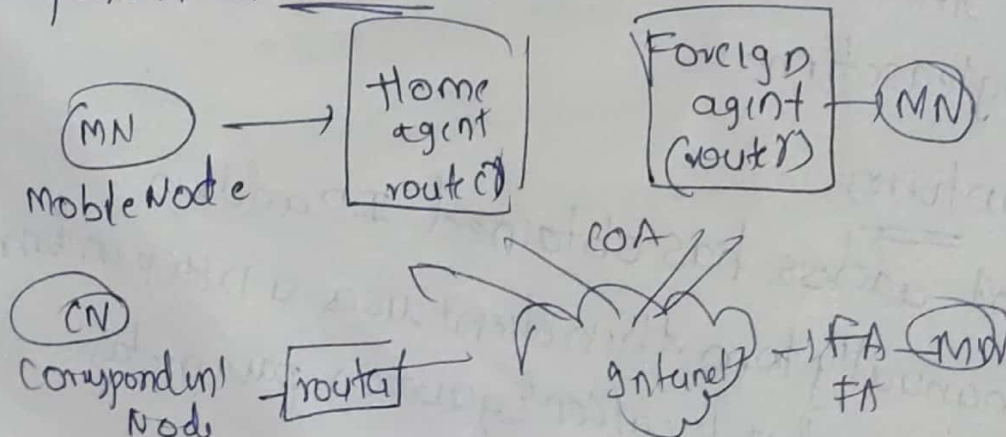
compatibility

Security

Transparency

Efficient & scalability

Components of Mobile IP:



i) Mobile node (MN): End user device which using mobile IP

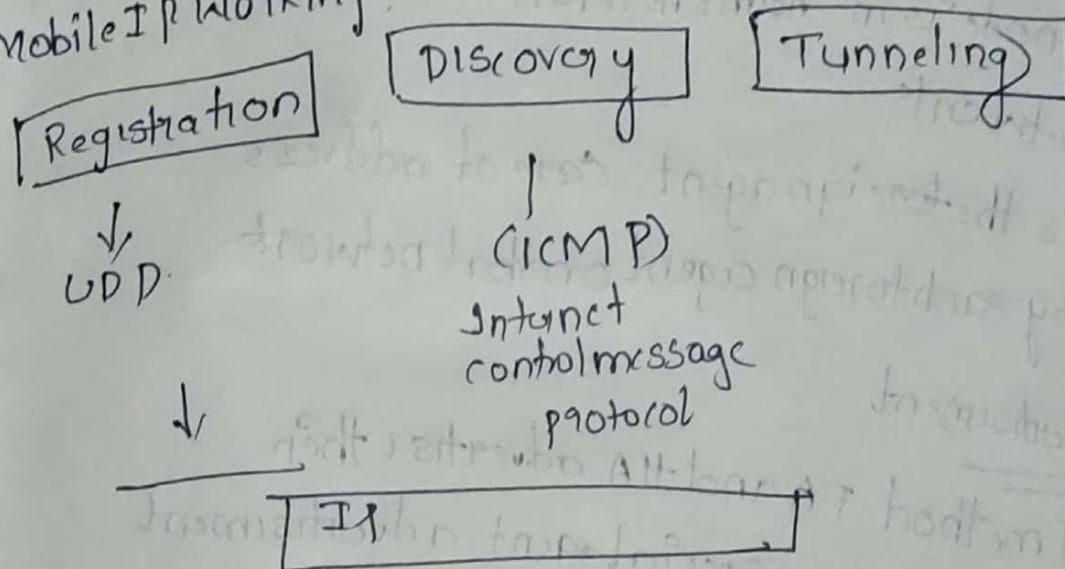
ii) CN: other node device for communication

iii) HN: MN is designated to this network typically home router

iv) Foreign network: when MN moved to another network now in FN

v) CoA: care of Address: define current location of MN in terms of IP.

Mobile IP Working:



Agent discovery: It is used whenever mobile node isn't in home network.

- Hence we need to search for foreign agent & methods.

Agent Advertisement

FA advertise their presence through their's periodic advertisement message
⇒ Agents give the info to all

Agent Discovery

A mobile node use a method known as agent discovery to determine the following information
has
When the node moved from one network to another

⇒ Whether node is in home network or foreign network

⇒ What is the foreign agent care of address offered by each foreign agent on that network

Agent Advertisement

For the first method FA and HA advertise their presence periodically using special agent advertisement messages. These messages can be seen as a beacon broadcast into subnet

⇒ For these advertisement Internet control messages are used with some mobility extensions.

presence through
agent message

known as
the following
one network to

work or
case of address
on that network

advertis (their
agent advertisement
seen as a

cont. new prod. of floor
ability extensions

Agent solicitation. If no agent advertisements
are present or the interval time is too high
and an MN has not received COA, the
mobile node must send agent solicitations

5) explain about Tunneling and Encapsulation
and write about different types of Encapsulation

Tunneling

Tunneling is a protocol that allows for secure
movement of data from one network to another.

Tunneling involves allowing private network
communications to be sent across a public
network such as the Internet through a process
called encapsulation.

⇒ Tunneling is also known as port forwarding
⇒ In tunneling the data are broken into
smaller pieces called packets as they move along
tunnel for transport

⇒ As the packets move through the tunnel
they are encrypted.
The private network data and the protocol into
that goes with are encapsulated in public
network transmission units
to sending

Encapsulation

- ⇒ Encapsulation is the mechanism of taking packet consisting of packet header and data and putting it into data part of a new packet put out
- ⇒ The reverse operation taking a packet put out of data part of another packet known as decapsulation
- ⇒ Encapsulation and decapsulation are the operations typically performed when a packet is transferred a higher protocol layer to lower layer or vice versa.

Types of Encapsulation

Three types of encapsulation protocols are specified for Mobile IP.

1) IP-in-IP encapsulation: required to be supported. Full IP header added to original IP packet. The new header contain HA address as source and Care of Address as destination.

Minimal encapsulation: optional.

Requires less overhead but requires change to original header.

Destination address changed to Care of address and source IP address is maintained as is.

Generic Routing Encapsulation
Allow packets of different protocol suit to be
encapsulated by another protocol suit

8) Explain WAP with its Architecture (13)

Ans Wireless Application Protocol or WAP is what is WAP?
a programming model.

=> WAP is a de facto standard or protocol designed
for microbrowser and it enables the mobile
devices to interact, exchange and transmit
info over the Internet.

=> WAP is based upon the concept of the
Worldwide web (WWW) and backend functioning

also remains similar to WWW.

but it uses markup languages wireless
markup language. to access WAP services. whereas

WWW uses HTML as a markup language.

WML is defined as XML 1.0 application.

Working of Wireless Application Protocol or WAP model

The following steps defines the working of wireless
Application Protocol or WAP model

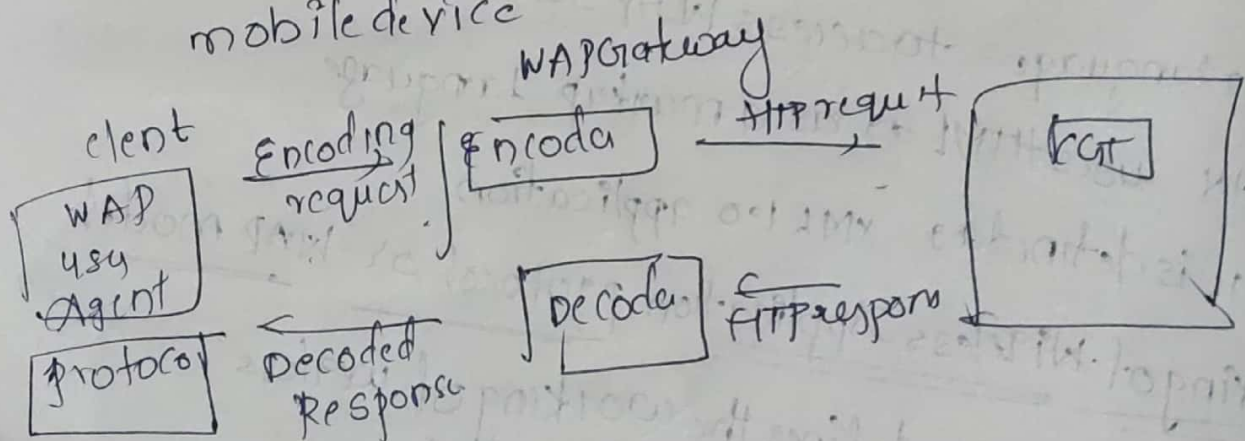
=> The WAP model consists of 3 levels
Client, gateway and origin server

=> When a user hits the browser in his/her mobile device and selects a website that she wants to view, the mobile device sends the URL encoded request via network to gateway using WAP protocol

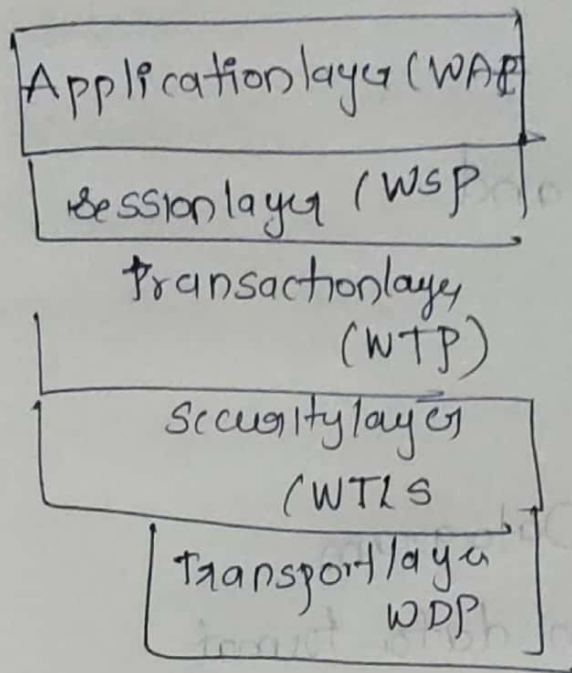
=> The request that is sent to mobile to gateway is known as encoding request

=> The sent encoding request is transferred through WAP gateway and then forwarded to the origin server in the form of HTTP request over Internet

=> When the request reaches the origin server, it processes the request and sends the response back to the mobile device



WAP protocol stack



1) Application layer

- = This layer contains Wireless Application Environment
- = It contains mobile device specifications and content development programming like WML

2) Session layer

- This layer contains Wireless session protocol
- It provides fast connection suspension and reconnection

3) Transaction layer

- This layer contains Wireless Transaction protocol (WTP)
- It runs on top of UDP and part of TCP and offers transaction support

Security layer

This layer contains Wireless Transaction Layer Security (WTLS)

It offers data integrity, privacy and authentication.

5) Transport layer

- This layer contains Wireless Datagram protocol. It presents consistent data format to higher layers of WAP protocol stack.

16) List various applications of mobile ad hoc networks?

Ans Military:

An ad hoc network will give access to the army to maintain network among all the soldiers, vehicles and headquarters.

-7 Personal area Network

=> Crisis condition

=> Medical Application

=> Environmental

=> Vehicular Ad hoc networks

=> Civilian environments