5.3 Optimizations

UQ. 5.3.1 Why and how can optimization in mobile IP be achieved? **MU - May 18(Q. 3(B)), 10 Marks**

☑ **Ans. :**

Triangular routing

- Even though the computers belonging to two different countries are few meters apart then also the packets sent from one computer to the other has to travel a long path of HA and then to COA. This inefficient behaviour of non-optimized mobile IP is known as triangular routing.
- This triangle is made up of three segments, CN to HA, HA to COA/MN and MN back to CN.
- Hence this basic mobile IP protocol increases the overhead to the network between CN and HA and also between HA and COA.

- This triangular routing also increases the latency. Hence optimization is necessary.
- Optimization of the route can be obtained by conveying the current location of MN to CN. The CN can learn the location by caching it in a binding cache. The binding cache is a part of local routing table for the CN. The entity that informs the CN about the location is HA.
- The optimized mobile IP protocol needs four additional protocols.

1. Binding request
2. Binding update
3. Binding acknowledgement
4. Binding warning

1. Binding request

- Any node that wants to know the current location of an MN can send the binding request to the HA. The HA can check if the MN has allowed dissemination of its current location.
- If the HA is allowed to reveal the location it sends back a binding update.

2. Binding update

- The current location of the MN is revealed by the message sent by the HA to CN.
- The message contains the fixed IP address of the MN and the COA. The binding update can request an acknowledgement.

3. Binding acknowledgement

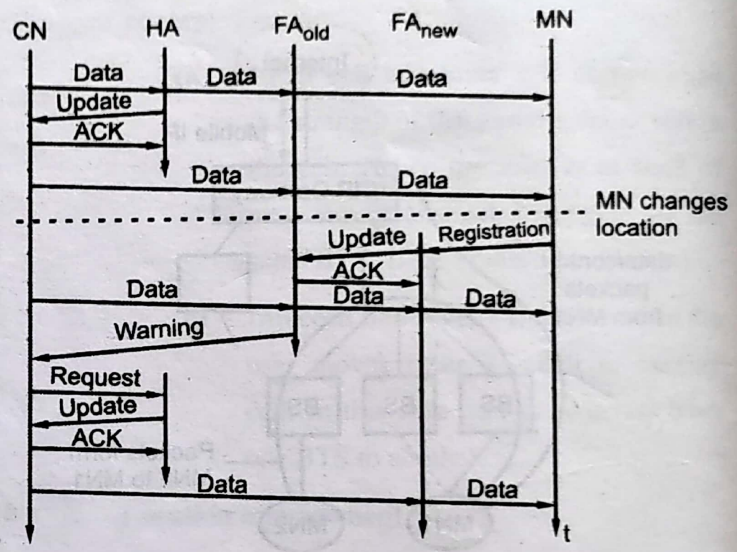
- A node returns this acknowledgement after receiving a binding update message if requested.

4. Binding warning

- When the node decapsulates a packet for an MN, but it is not the current FA for this MN, this node sends the binding warning.
- The warning comprises of MN's home address and the address of the node which has tried to send the packet to the node. The warning is an indication that the target node could benefit from obtaining the fresh binding for the MN.
- The recipient of the warning can be HA. Hence HA can send a binding update to the node that has a wrong COA for the MN.

Optimized mobile IP

- Refer Fig. 5.3.1. It shows the change of the FA with the optimized mobile IP.



(5E2)**Fig. 5.3.1 : FA with the optimized mobile IP**

- CN request about the current location from HA. If allowed by MN, the HA returns the COA of MN via an update message.
- CN acknowledges this update message and stores the mobility binding.
- Now CN is able to send data directly to FA_{old} and then to MN. It means COA is located at FA. Hence CN encapsulates the data packets for tunnelling purpose and not the HA.
- Now if MN changes its location and registers with new FA FA_{new}. This registration is also forwarded to HA to update its location database.
- Now FA_{new} conveys to FA_{old} regarding the new registration of MN through update message. This registration message contains the address of FA_{old}

- FA_{old} acknowledges this update message.
- As the CN does not know anything about the new registered FA, it keeps on tunnelling the packets to old FA.
- Thus old FA forwards these packets to new COA of MN which is FA_{new}.
- This forwarding of packets provides smooth handovers and in a way provides optimization.
- If optimization does not exist, all the packets in transit must have been lost during the location change of MN.
- To inform CN about its stale binding cache, FA_{old} sends the binding warning to CN.
- Then CN requests with binding update. HA sends an update to inform the CN about the current location. It is also acknowledged by CN.
- Now CN is able to send packets directly to FA_{new}. This avoids the issue of triangular routing.
- The disadvantage of this optimization is, it causes many security issues.

5.4 IPv6 (Internet Protocol version 6)

LQ. 5.4.1 List the features of IPv6.

Ans. :

IPv6 defines many mechanisms which are needed for mobility. They come for free with this version of IP.

Features of IPv6

1. There was an issue regarding the security in earlier versions of IP but in IPv6 the authentications is the mandatory requirement of all the nodes.
2. No special add-ons are needed for securing mobile IP registration.
3. Every Ipv6 node masters the address autoconfiguration. The mechanism needed for acquiring COA is built in feature in this version.
4. It includes the feature of neighbour discovery. Hence special FA are not needed for advertising the services.
5. Due to the features of autoconfiguration and neighbour discovery, each node is able to create a topologically correct address for the current point of attachment.
6. Each IPv6 node can send binding updates to another node.
7. Soft handover is possible.
8. A CN only has to process the binding updates. The MN has to decapsulate the packet, detect the requirement of new COA and determine when to send the binding updates to HA and CN. FA is no longer needed.
9. HA itself encapsulates the packets

Disadvantages

It does not solve any firewall or privacy issues. Hence additional mechanisms on higher layers are needed for this.

5.5 Macro Mobility

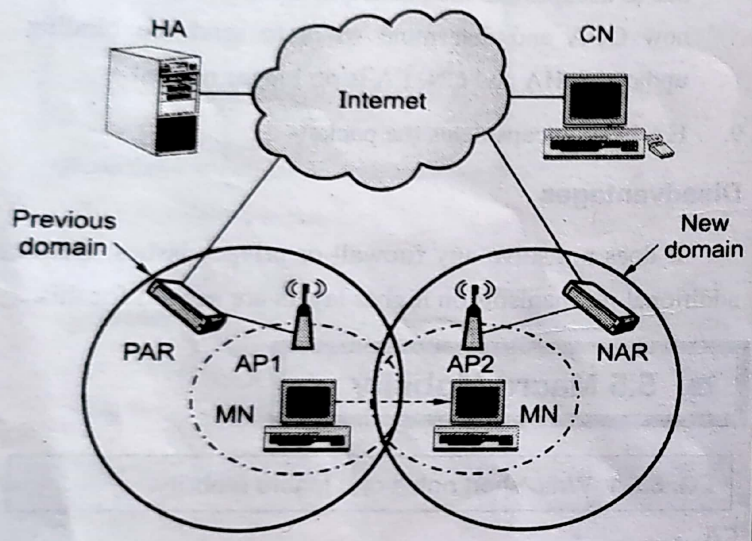
LQ. 5.5.1 Write short notes on : Macro mobility.

Ans. :

- It is inter domain mobility. It is also known as macro mobility or global scale mobility.
- It occurs when the mobile user changes his point of network attachment between two separate domains. It aims to provide uninterrupted service when the user is changing the domain.
- Actually the user moves between two independently managed networks.
- It requires full low layer handover, authentication process, network layer configuration, registration by mobility management mechanisms. It also needs significant data path changes.
- In this scalability is the main important factor to be considered. As a result macro-mobility protocols tend to closely cooperate with IP routing mechanisms to integrate fixed and mobile networks.

5.5.1 MIPv6 (Mobile IP Version 6)

- MIPv6 handles the routing packets to mobile nodes that have moved away from their home network. MIPv6 broadly focus on macro mobility.
- MIPv6 is an update of the IETF (Internet Engineering Task Force) Mobile IP standard (RFC 2002) designed to authenticate mobile devices (known as mobile nodes) using IPv6 addresses.
- Refer Fig. 5.5.1. It shows basic architecture of MIPv6.



(5E3)**Fig. 5.5.1 : MIPv6 architecture**

- There are 3 main entities as shown in the Fig. 5.5.1. they are HA (home agent), AR (access router) and AP (access point).
- There are to nodes namely CN (correspondent node) and MN (mobile node).
- MN is connected to the internet via AP or AR.

Handover scenario

- There are two access points namely AP1 and AP2, in the network.
- There are two different access routers to which these Aps are connected. They are denoted PAR (Previous Access Router) and NAR (New Access Router), respectively
- When the MN moves from the radio range of the AP1 to that of the AP2, the handover happens.
- When the MN moves from its home IP network, it detects foreign networks based on Agent Advertisement messages that can be solicited. Then MN updates binding with its HA.
- The MN is identified by its unchanging home address.
- When a data packet is sent to the MN by another CN, the HA interprets it based on the home address of the MN. This HA stores the registration mapping between the MN's home address and its current CoA. The packet is then tunnelled from the HA to the MH (directly or through an FA).
- Major issue faced by MIPv6 is handover latency.

Handover latency in MIPv6

Handover latency can be categorised inn three parts as

1. L2 handover latency
2. Rendezvous time delay
3. Registration delay

1. L2 handover latency

It is defined asthe time interval from the moment that layer 2 link down trigger from the PAR happens to the moment that the layer 2 link up trigger to the NAR happens.

2. Rendezvous time delay

It has two types of latency.

(i) **Movement detection latency :** It is the time interval taken by the MN to detect the presence of a NAR at the new access network

(ii) **New COA configuration latency :** It is the time interval taken to configure a new CoA for the MN including router Discovery and implementing DAD process

3. Registration delay

It is the time taken to send BU to the HA/CN and the subsequent resumption of communications indicated by a new data packet arriving at the MN from the NAR without passing through the tunnel between NAR and PAR.

Advantages

1. MIPv6 neighbour discovery and address auto configuration allow nodes to operate in any location without any special support.
2. No FA is needed.

Disadvantages

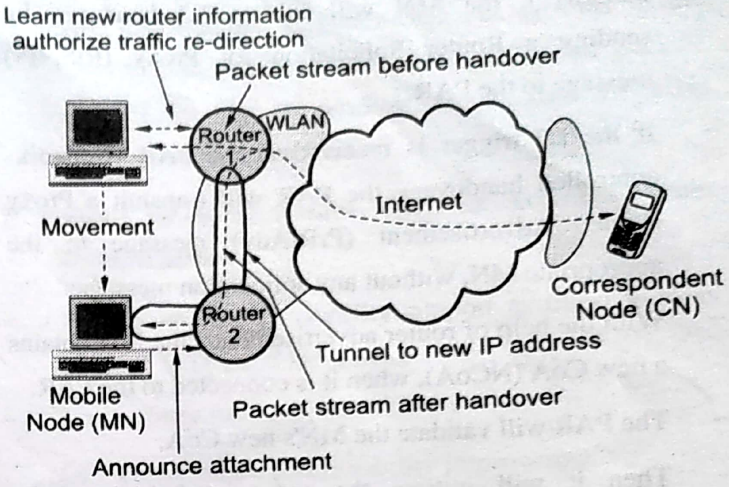
1. It utilizes the network resources even if they are not needed. Because it needs that the traffic addressed to MN should always be routed to its home network. Only in that case it will ne tunnelled by HA to its final destination. This uses network resources unnecessarily.
2. Due to long transmission path and tunnelling overhead, quality of service is affected.
3. It faces major issue of handover latency.

5.5.2 FMIPv6 (Fast Handover MIPv6)

- To reduce the issue of high handover latency in MIPv6, fast handover mechanisms in MIPv6 are proposed. It is known and FMIPv6.
- It describes two possible ways to initiate the handover

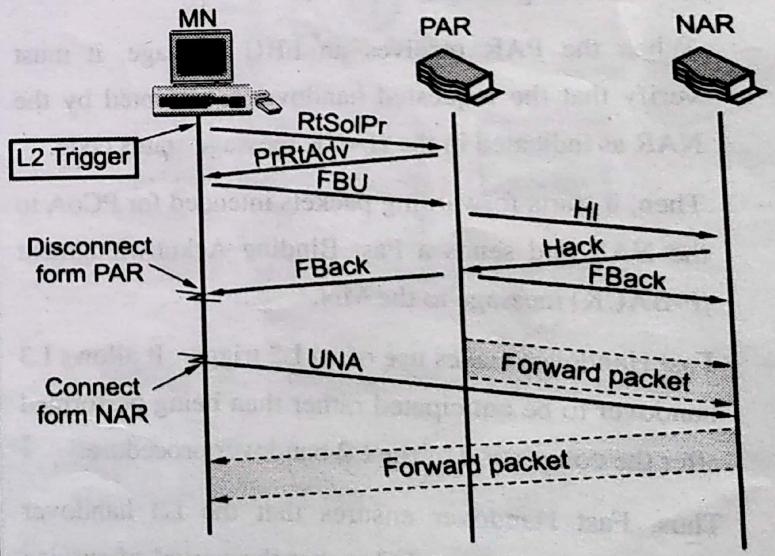
1. Predictive fast handover
2. Reactive fast handover

- FMIPv6 also obtains new COA before proceeding for handover and starts using this address later on.
- The difference between these two handover schemes is the time to establish the tunnel between PAR and NAR.
  1. **Predictive handover :** the tunnel is established before the layer 2 handover.
  2. **Reactive handover :** the tunnel is established directly after layer 2 handover.
- Refer Fig. 5.5.2. It shows the basic system architecture for FMIPv6.



(5E4)**Fig. 5.5.2 : Basic system architecture for FMIPv6**

- Predictive handover has shorter handover delay as compared to reactive handover. Hence we will discuss predictive handover scheme.
- In fast handover schemes, DAD (duplicate address detection) is neglected when the new COA configuration is performed. If the DAD is not performed at the beginning and is performed after the node has set up a link to the new AP, much time will be wasted if duplicate address exists and such latency cannot be tolerated for latency sensitive applications



(5E5)**Fig. 5.5.3 : Procedure for FMIPv6 (predictive mode)**

- MN or PAR may start the fast handover procedure once the L2 trigger is received.

- If the L2 trigger is received at the MN Mobile-initiated handover), the MN will initiate L3 handover by sending a Router Solicitation for Proxy (RtSolPr) message to the PAR.
- If the L2 trigger is received at the PAR (Network-controlled handover), the PAR will transmit a Proxy Router Advertisement (PrRtAdv) message to the appropriate MN, without any solicitation messages.
- With the help of router advertisements, the MN obtains a new CoA (NCoA), when it is connected to the PAR.
- The PAR will validate the MN's new CoA.
- Then it will initiate the process of bidirectional tunnelling between the PAR and the NAR. It is done by sending a Handover Initiate (HI) message to the NAR.
- The NAR verifies that its new CoA and it can be used on the NAR's link.
- Once the Hi message is received the NAR sets up a host route for the MH's previous CoA (PCoA and responds with a Handover Acknowledge (HACK)) message.
- When the MN receives a PrRtAdv message, it sends a Fast Binding Update (FBU) message, generally prior to disconnecting its link.
- When the PAR receives an FBU message, it must verify that the requested handover is accepted by the NAR as indicated in the HACK message status code.
- Then, it starts forwarding packets intended for PCoA to the NAR and sends a Fast Binding Acknowledgment (F-BACK) message to the MN.
- Fast Handover makes use of an L2 trigger. It allows L3 handover to be anticipated rather than being performed after the completion of the L2 handover procedure.
- Thus, Fast Handover ensures that the L3 handover delay is minimized, and also that the period of service disruption, which normally occurs when an MN moves between two ARs, is eliminated.

5.6 Micro Mobility

LQ.5.6.1 Write short notes on : Micro mobility.

☑ **Ans. :**

- Intra domain mobility is known as micro mobility. It is also known as local mobility.
- It takes place when the mobile user moves within the domain boundaries.
- Mobile IP faces issues with the duration of the handover and the scalability of the registration procedure.
- IP micro mobility protocols supports seamless handover control in limited geographical areas.
- In IP micro mobility, the frequent updates generated by local changes of the points of attachment are kept away from the home network. The information about only the major changes is conveyed to HA. Major changes may include changes of region.
- There are three approaches for micro mobility support.

1. Cellular IP
2. Hawaii
3. Hierarchical Mobile IPv6 (HMIPv6)

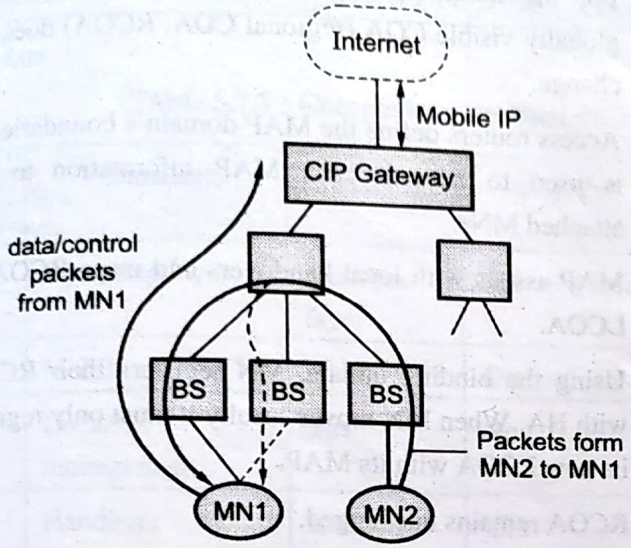
1. Cellular IP

UQ. 5.6.2 Write short note on : Cellular IP.
MU - Dec. 15(Q. 6(e)), Dec. 16(Q. 6(c)), 5 Marks

☑ **Ans. :**

- Refer Fig. 5.6.1. It shows basic architecture of cellular IP.
- It provides the local handovers without renewed registration. It is done by installing a single cellular IP gateway (CIPGW) for each domain. This CIPGW acts as a FA for the outside world.
- Within the cellular IP domain, all nodes collect routing information for accessing MNs based on the origin of the packets sent by the MNs towards the CIPGW.

- Simultaneous forwarding of packets which are destined for MN can be allowed to take multiple paths. Due to this the soft handover is obtained.



(5E6)**Fig. 5.6.1 : Basic architecture of cellular IP**

- A MN moving between adjacent cells will temporarily be able to receive packets via both old and new base stations if this is supported by the lower protocol layers.
- Cellular IP needs changes in the basic mobile IP protocol and it is not transparent to existing systems.
- The foreign network's routing tables are updated based on the messages sent by the mobile nodes. But they cant be trusted.

Advantages

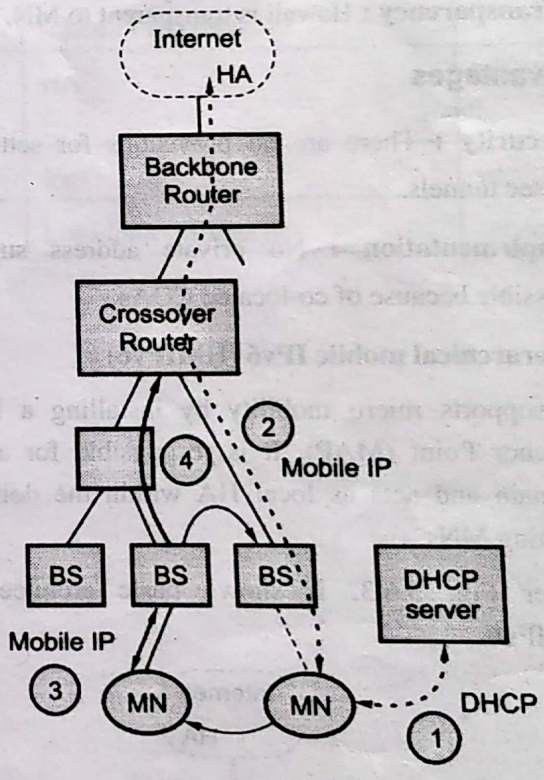
1. **Manageability :** It is mostly self configuring. Integration of CIPGW into firewall would facilitate administration of mobility related functionality.
2. It has simple and elegant architecture.

Disadvantages

1. **Efficiency :** As the packets are forwarded on multiple paths, additional network load is induced.
2. **Transparency :** Changes to MNs are needed.
3. **Security :** Routing tables are updated based on the messages sent by mobile nodes. All systems in the network can easily obtain the copy of all packets destined for MN by sending packets with the MNs source address to the CIPGW.

2. Hawaii (Handoff Aware Wireless Access Internet Infrastructure)

- It keeps the micro mobility support as transparent as possible to HA and MN.
- It is majorly focused on the
  - (i) Performance and reliability improvements
  - (ii) Quality of service mechanisms
- Refer Fig. 5.6.2. It shows basic architecture of Hawaii.



(5E7)**Fig. 5.6.2 : Basic architecture of Hawaii**

- **Step 1 :** Once entered in Hawaii domain, a M obtains co-located COA
- **Step 2 :** Then it registers with HA.
- **Step 3 :** When MN is moving to another cell insi the foreign agent, the MN sends a registrati request to the new base station as to FA.

➪ **Step 4 :** The base station interprets the registration request and sends out a handoff update message. This reconfigures all the routers on the path from the old and new base station to crossover router.

- Once the routing is reconfigured, the base station sends the registration reply to the mobile node.
- For authenticating the MN, challenge response method is used.

Advantages

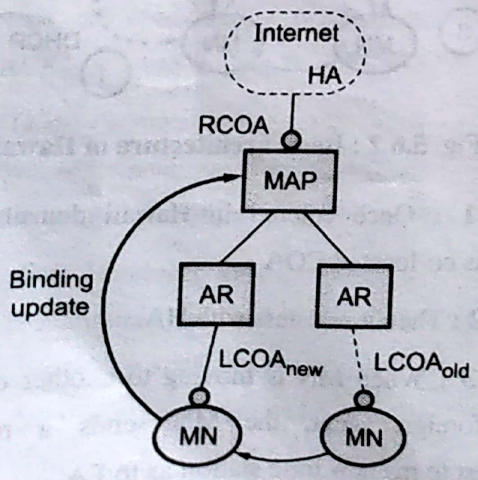
1. **Security :** Challenge response method is used. Unlike cellular IP, routing tables are always initiated by the foreign domain's infrastructure and corresponding messages could be authenticated. This reduces the risk of malicious rerouting of traffic.
2. **Transparency :** Hawaii is transparent to MN.

Disadvantages

1. **Security :** There are no provisions for setting up f IPsec tunnels.
2. **Implementation :** No private address support is possible because of co-located COAs.

3. Hierarchical mobile IPv6 (HMIPv6)

- It supports micro mobility by installing a Mobility Anchor Point (MAP). It is responsible for a certain domain and acts as local HA within the domain for visiting MNs.
- Refer Fig. 5.6.3. It shows basic architecture of HMIPv6.



(5E8) **Fig. 5.6.3 : Basic Architecture of HMIPv6**

- The MAP receives all the packets on behalf of MN. It then encapsulates the packets and forwards them to the MN's current location which is LCOA (link COA).
- For the duration MN is in the MAP domain, the globally visible COA (regional COA, RCOA) does not change.
- Access routers define the MAP domain's boundaries. It is used to advertise the MAP information to the attached MNs.
- MAP assists with local handovers and maps RCOA to LCOA.
- Using the binding update, MN registers their RCOA with HA. When MN moves locally it must only register its new LCOA with its MAP.
- RCOA remains unchanged.
- MN can also send the binding update to its former MAP. This supports smooth handover between MAP domains.
- In this MN can be provided with some sort of limited location privacy. This is because LCOAs on lower levels of the mobility hierarchy can be hidden from outside world.
- MN can also send binding update to CN. It reveals its location but optimizes the packet flow.
- MN can use their RCOAs as source address.

Advantages

1. **Security :** MN can have location privacy because LCOAs can be hidden.
2. **Efficiency :** Direct routing between CNs sharing the same link is possible.

Disadvantages

1. **Transparency :** MAP is the additional infrastructure component used in this.
2. **Security :** Routing tables are updated based on the messages sent by MN. It needs strong authentication and protection against denial of service attacks. Additional security mechanisms may be needed in MAP.

5.7 Comparison between Different Micro Mobility and Macro Mobility Protocols

LQ. 5.7.1 Compare between different micro mobility and macro mobility protocols.

Ans. :

Table 5.7.1 : Comparison between different micro mobility and macro mobility protocols

Sr. no.	Parameters	MIPv6	FMIPv6	Cellular IP	Hawaii	HMIPv6
1	Operating layer	Network layer	Network layer	Network layer	Network layer	Network layer
2	Mobility scope	Global	Global/local	local	local	local
3	Location management	Yes	No	Yes	yes	Yes
4	Handover management	Limited	Yes	Yes	Forwarding and non forwarding schemes are sued	Yes
5	Required infrastructure	HA	HA, enhanced AR	Enhanced BS	HA	HA, MAP
6	MN modification	Yes	Yes	Yes	Yes	yes
7	Handover latency	Bad	Good	good	Less than cellular IP	moderate

Chapter Ends...

❑❑❑