UNIT II MOBILE NETWORK LAYER 9 Hours

Introduction - Mobile IP: IP packet delivery, Agent discovery, tunneling and encapsulation, IPV6-Network layer in the internet- Mobile IP session initiation protocol - mobile ad-hoc network: Routing: Destination Sequence distance vector, IoT: CoAP

INTRODUCTION

This chapter introduces protocols and mechanisms developed for the network layer to support mobility.

The most prominent example is Mobile IP which adds mobility support to the internet network layer protocol IP.

The internet is the network for global data communication with hundreds of millions of users. So why not simply use a mobile computer in the internet?

The reason is quite simple: you will not receive a single packet as soon as you leave your home network, i.e., the network your computer is configured for, and reconnect your computer (wireless or wired) at another place (if no additional mechanisms are available).

- The reason for this is quite simple if you consider routing mechanisms on the internet. A host sends an IP packet with the header containing a destination address with other fields. The destination address not only determines the receiver of the packet, but also the physical subnet of the receiver.
- Routers in the internet now look at the destination addresses of incoming packets and forward them according to internal look-up tables.
- As long as the receiver can be reached within its physical subnet, it gets the packets; as soon as it moves outside the subnet, a packet will not reach it.
- So now a host needs a so-called **topologically correct address.**

One might think that a quick solution to this problem would be to assign to the computer a new, topologically correct IP address.

The problem is that nobody knows about this new address. It is almost impossible to find a (mobile) host on the internet which has just changed its address.

So what about dynamically adapting the IP address with regard to the current location?

The problem is that the domain name system (DNS) needs some time before it updates the internal tables necessary to map a logical name to an IP address. This approach does not work if the mobile node moves quite often.

Another approach is the creation of specific routes to the mobile node.

Routers always choose the best-fitting prefix for the routing decision. While it is theoretically possible to change routing tables all over the world to create specific routes to a mobile node, this does not scale at all with the number of nodes in the internet.

Routers are built for extremely fast forwarding, but not for fast updates of routing tables. While the first is done with special hardware support, the latter is typically a piece of software which cannot handle the burden of frequent updates.

Several requirements accompanied the development of the standard:

Compatibility: Mobile IP has to remain compatible with all lower layers used for the standard, non-mobile, IP. Mobile IP has to ensure that users can still access all the other servers and systems in the internet. But that implies using the same address format and routing mechanisms.

Transparency: Mobility should remain ‘invisible’ for many higher layer protocols and applications. Besides maybe noticing a lower bandwidth and some interruption in service, higher layers should continue to work even if the mobile computer has changed its point of attachment to the network.

Scalability and efficiency: Enhancing IP for mobility must not generate too many new messages flooding the whole network. Special care has to be taken considering the lower bandwidth of wireless links.
It is crucial for a mobile IP to be scalable over a large number of participants in the whole internet, worldwide.

Security: Mobility poses many security problems. The minimum requirement is that of all the messages related to the management of Mobile IP are authenticated.
The IP layer must be sure that if it forwards a packet to a mobile host that this host receives the packet. The IP layer can only guarantee that the IP address of the receiver is correct. There are no ways of preventing fake IP addresses or 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

Mobile node (MN):

1. A mobile node is an end-system or router that can change its point of attachment to the internet using mobile IP.

2. 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.

3. Mobile nodes are not necessarily small devices such as laptops with antennas or mobile phones; a router onboard an aircraft can be a powerful mobile node.

Correspondent node (CN):

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

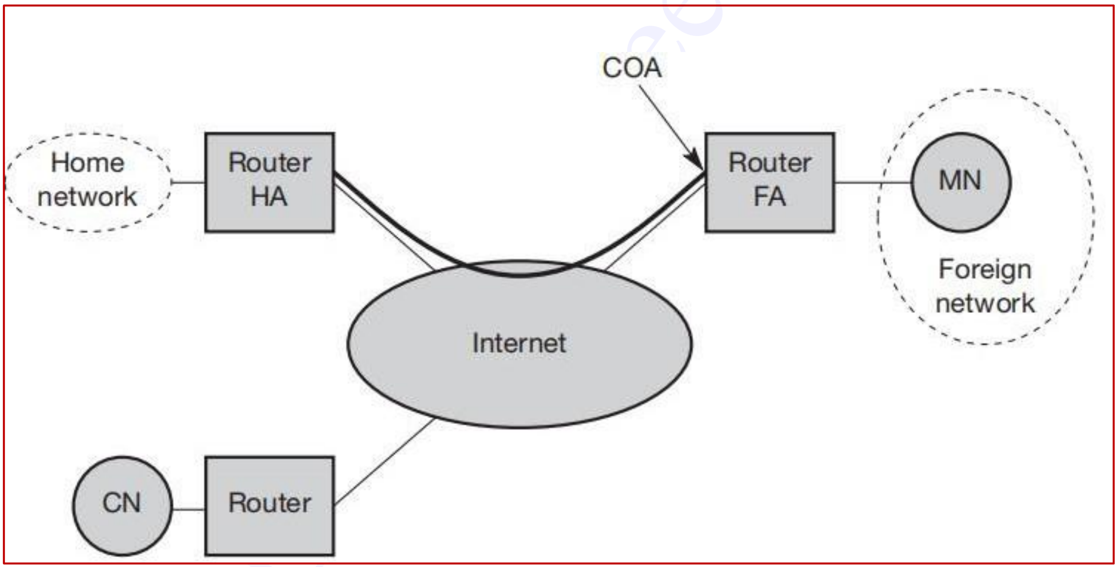


Fig 1: Mobile IP Example network

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 (defined below), acting as tunnel endpoint and forwarding packets to the MN. The FA can be the default router for the MN.

Care-of address (COA):

1. The COA defines the current location of the MN from an IP point of view.

2. All IP packets sent to the MN are delivered to the COA, not directly to the IP address of the MN.

3. Packet delivery toward the MN is done using a tunnel, as explained later. To be more precise, the COA marks the tunnel endpoint, i.e., the address where packets exit the tunnel.

There are two different possibilities for the location of the COA:

Foreign agent COA:

1. The COA could be located at the FA, i.e., the COA is an IP address of the FA.

2. 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:

1. The COA is co-located if the MN temporarily acquired an additional IP address which acts as COA.

2. This address is now topologically correct, and the tunnel endpoint is at the MN.

3. Co-located addresses can be acquired using services such as DHCP.

4. One problem associated with this approach is the need for additional addresses if MNs request a COA. This is not always a good idea considering the scarcity of IPv4 addresses.

Home agent (HA):

1. 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.

2. 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 MN comes in via the router; the HA sends it through the tunnel which again crosses the router.

3. 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 always in a foreign network with this solution.

IP PACKET DELIVERY

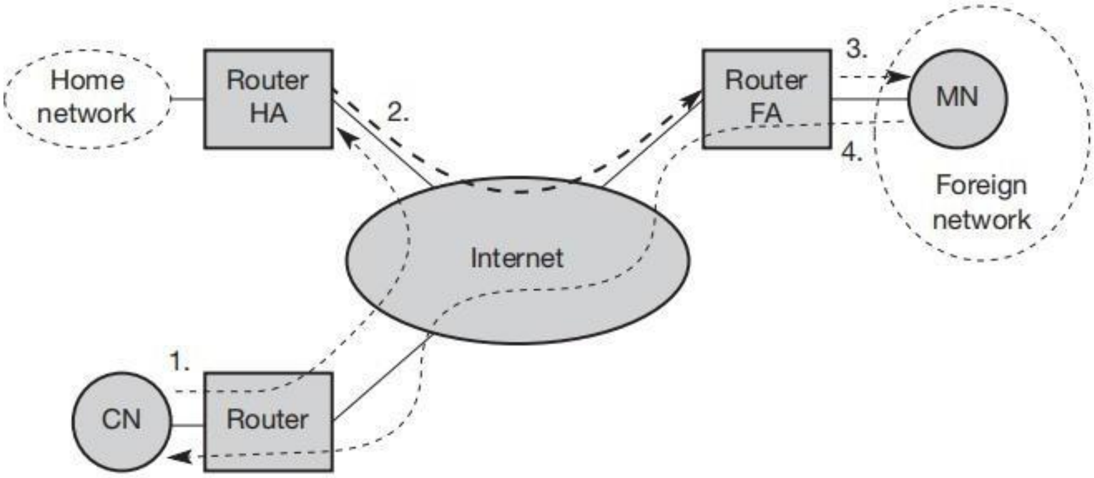


Fig 2: Packet deliver to and from the mobile node

1. A correspondent node CN wants to send an IP packet to the MN.

2. One of the requirements of mobile IP was to support hiding the mobility of the MN.

3. CN does not need to know anything about the MN's current location and sends the packet as usual to the IP address of MN **(step 1).**

This means that 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

4. The HA now intercepts the packet, knowing that MN is currently not in its home network.

5. The packet is not forwarded into the subnet as usual, but encapsulated and tunnelled to the COA.

6. 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 **(step 2).**

7. 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 **(step 3).**

8. 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.

9. The MN sends the packet as usual with its own fixed IP address as source and CN's address as destination **(step 4).**

10. 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.

If CN were also a mobile node residing in a foreign network, the same mechanisms as described in steps 1 through 3 would apply now in the other direction.

AGENT DISCOVERY

One initial problem of an MN after moving is how to find a foreign agent.

How does the MN discover that it has moved?

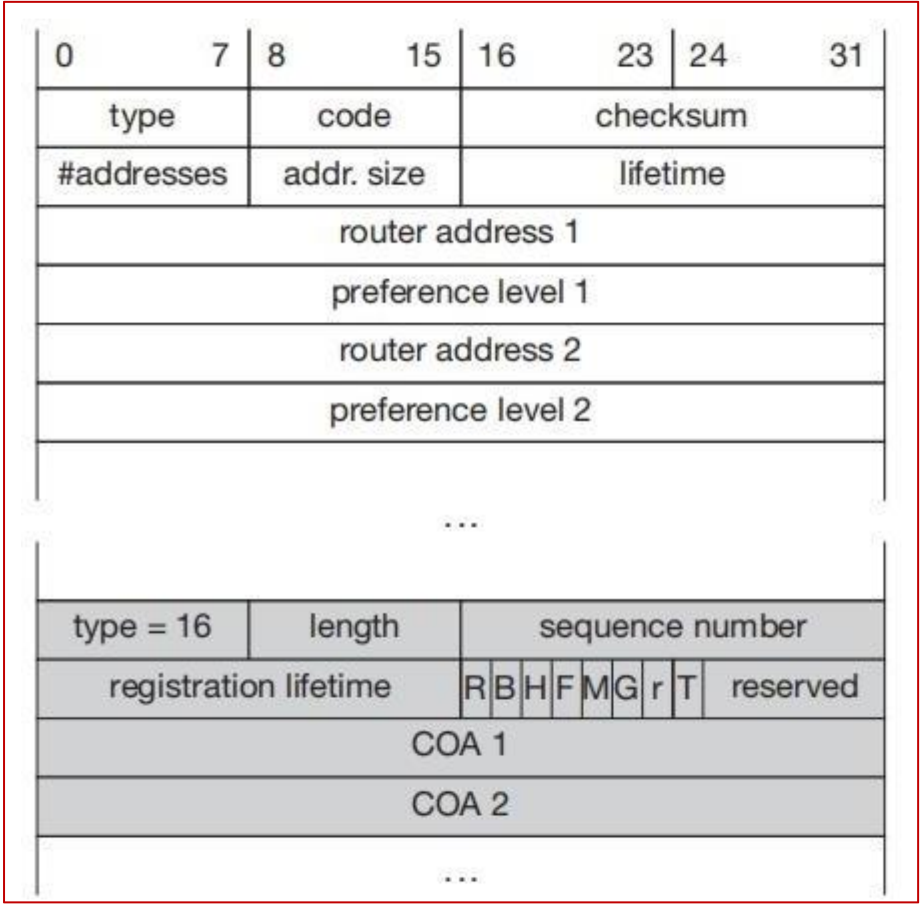
For this purpose mobile IP describes two methods:
agent advertisement
and
agent solicitation,

which are in fact router discovery methods plus extensions.

Agent advertisement

- Here foreign agents and home agents advertise their presence periodically using special agent advertisement messages.
- These advertisement messages can be seen as a beacon broadcast into the subnet. Routers in the fixed network implementing this mechanisms also advertise their routing service periodically to the attached links.

The agent advertisement packet according to RFC 1256 with the extension for mobility is shown in Figure 3.



<table>
<tr><td>0 7</td><td>8 15</td><td colspan="8">16 23</td><td>24 31</td></tr>
<tr><td>type</td><td>code</td><td colspan="9">checksum</td></tr>
<tr><td>#addresses</td><td>addr. size</td><td colspan="9">lifetime</td></tr>
<tr><td colspan="11">router address 1</td></tr>
<tr><td colspan="11">preference level 1</td></tr>
<tr><td colspan="11">router address 2</td></tr>
<tr><td colspan="11">preference level 2</td></tr>
<tr><td colspan="11">...</td></tr>
<tr><td>type = 16</td><td>length</td><td colspan="9">sequence number</td></tr>
<tr><td colspan="2">registration lifetime</td><td>R</td><td>B</td><td>H</td><td>F</td><td>M</td><td>G</td><td>r</td><td>T</td><td>reserved</td></tr>
<tr><td colspan="11">COA 1</td></tr>
<tr><td colspan="11">COA 2</td></tr>
<tr><td colspan="11">...</td></tr>
</table>

Fig 3: Agent Advertisement Packet

The upper part represents the ICMP packet while the lower part is the extension needed for mobility.

1. The TTL field of the IP packet is set to 1 for all advertisements to avoid forwarding them.

2. The IP destination address according to standard router advertisements can be either set to 224.0.0.1, which is the multicast address for all systems on a link (Deering, 1989), or to the broadcast address 255.255.255.255.

3. The fields in the ICMP part are defined as follows. The type is set to 9, the code can be 0, if the agent also routes traffic from non-mobile nodes, or 16, if it does not route anything other than mobile traffic.

4. Foreign agents are at least required to forward packets from the mobile node.

5. The number of addresses advertised with this packet is in #addresses while the addresses themselves follow as shown.

6. Lifetime denotes the length of time this advertisement is valid.

7. Preference levels for each address help a node to choose the router that is the most eager one to get a new node.

8. The difference compared with standard ICMP advertisements is what happens after the router addresses.

9. This extension for mobility has the following fields defined: type is set to 16, length depends on the number of COAs provided with the message and equals 6 + 4*(number of addresses).

10. An agent shows the total number of advertisements sent since initialization in the sequence number.

11. By the registration lifetime, the agent can specify the maximum lifetime in seconds a node can request during registration.

12. The following bits specify the characteristics of an agent in detail.

    - The R bit (registration) shows, if a registration with this agent is required even when using a colocated COA at the MN.

    - If the agent is currently too busy to accept new registrations it can set the B bit.

    - The following two bits denote if the agent offers services as a home agent (H) or foreign agent (F) on the link where the advertisement has been sent.

    - Bits M and G specify the method of encapsulation used for the tunnel.

- While IP-in-IP encapsulation is the mandatory standard, M can specify minimal encapsulation and G generic routing encapsulation.

- In the first version of mobile IP (RFC 2002) the V bit specified the use of header compression according to RFC 1144 (Jacobson,1990). Now the field r at the same bit position is set to zero and must be ignored.

- The new field T indicates that reverse tunneling is supported by the FA.

- The following fields contain the COAs advertised.

- A foreign agent setting the F bit must advertise at least one COA.

A mobile node in a subnet can now receive agent advertisements from either its home agent or a foreign agent.

This is one way for the MN to discover its location.

– –

Agent solicitation

1. If no agent advertisements are present or the inter-arrival time is too high, and an MN has not received a COA by other means, e.g., DHCP, the mobile node must send agent solicitations.

2. Care must be taken to ensure that these solicitation messages do not flood the network, but basically an MN can search for an FA endlessly sending out solicitation messages.

3. Typically, a mobile node can send out three solicitations, one per second, as soon as it enters a new network.

4. It should be noted that in highly dynamic wireless networks with moving MNs and probably with applications requiring continuous packet streams even one second intervals between solicitation messages might be too long.

5. Before an MN even gets a new address many packets will be lost without additional mechanisms.

6. If a node does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (typically one minute).

7. Discovering a new agent can be done anytime, not just if the MN is not connected to one.
8. Consider the case that an MN is looking for a better connection while still sending via the old path.

9. This is the case while moving through several cells of different wireless networks. After these steps of advertisements or solicitations the MN can now receive a COA, either one for an FA or a co-located COA.

10. The MN knows its location (home network or foreign network) and the capabilities of the agent (if needed).

Tunneling and Encapsulation

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

Packets entering a tunnel are forwarded inside the tunnel and leave the tunnel unchanged.

Tunneling, i.e., sending a packet through a tunnel, is achieved by using encapsulation.

Encapsulation is the mechanism of taking a packet consisting of packet header and data and putting it into the data part of a new packet.

The reverse operation, taking a packet out of the data part of another packet, is called **decapsulation**.

- Encapsulation and decapsulation are the operations typically performed when apacket is transferred from a higher protocol layer to a lower layer or from a lower to a higher layer respectively.

- Here these functions are used within the same layer. This mechanism is shown inFigure 4 and describes exactly what the HA at the tunnel entry does.

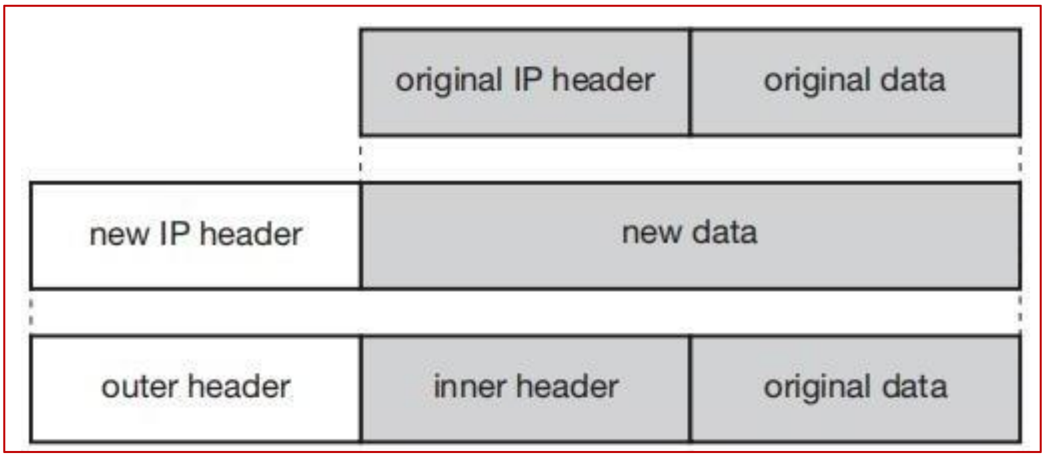


Fig 4 : IP Encapsulation

- The HA takes the original packet with the MN as destination, puts it into the data part of a new packet and sets the new IP header in such a way that the packet is routed to the COA.

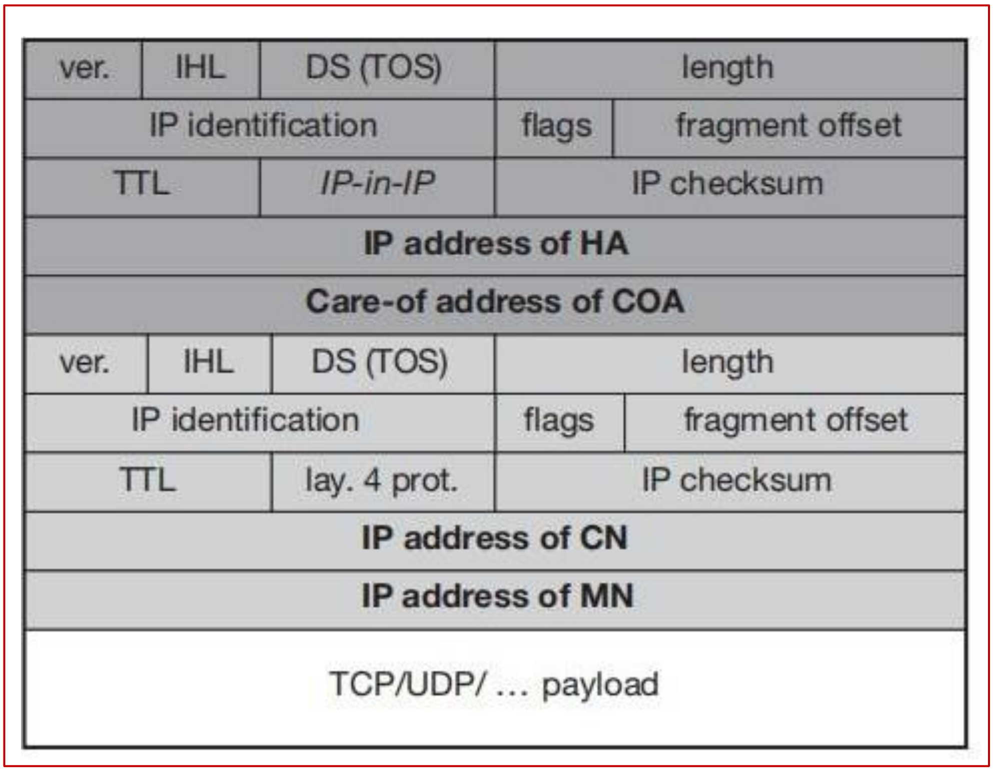
- The new header is also called the outer header for obvious reasons.

- Additionally, there is an inner header which can be identical to the original header as this is the case for IP-in-IP encapsulation, or the inner header can be computed during encapsulation.

IP-in-IP encapsulation

There are different ways of performing the encapsulation needed for the tunnel between HA and COA.

Figure 5 shows a packet inside the tunnel.



<table>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td><i>IP-in-IP</i></td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5"><b>IP address of HA</b></td></tr>
<tr><td colspan="5"><b>Care-of address of COA</b></td></tr>
<tr><td>ver.</td><td>IHL</td><td>DS (TOS)</td><td colspan="2">length</td></tr>
<tr><td colspan="3">IP identification</td><td>flags</td><td>fragment offset</td></tr>
<tr><td colspan="2">TTL</td><td>lay. 4 prot.</td><td colspan="2">IP checksum</td></tr>
<tr><td colspan="5"><b>IP address of CN</b></td></tr>
<tr><td colspan="5"><b>IP address of MN</b></td></tr>
<tr><td colspan="5">TCP/UDP/ … payload</td></tr>
</table>

Fig 5: IP-in-IP encapsulation

1. The fields of the outer header are set as follows.

2. The version field ver is 4 for IP version 4, the internet header length (IHL) denotes the length of the outer header in 32 bit words.

3. DS(TOS) is just copied from the inner header, the length field covers the complete encapsulated packet.

4. The fields up to TTL have no special meaning for mobile IP and are set according to RFC 791.

5. TTL must be high enough so the packet can reach the tunnel endpoint.

6. The next field, here denoted with IP-in-IP, is the type of the protocol used in the IP payload. This field is set to 4, the protocol type for IPv4 because again an IPv4 packet follows after this outer header.

7. IP checksum is calculated as usual.

8. The next fields are the tunnel entry as source address (the IP address of the HA) and the tunnel exit point as destination address (the COA).

9. If no options follow the outer header, the inner header starts with the same fields as just explained.

10. This header remains almost unchanged during encapsulation, thus showing the original sender CN and the receiver MN of the packet. The only change is TTL which is decremented by 1.

11. This means that the whole tunnel is considered a single hop from the original packet's point of view. This is a very important feature of tunneling as it allows the MN to behave as if it were attached to the home network.

12. No matter how many real hops the packet has to take in the tunnel, it is just one (logical) hop away for the MN.

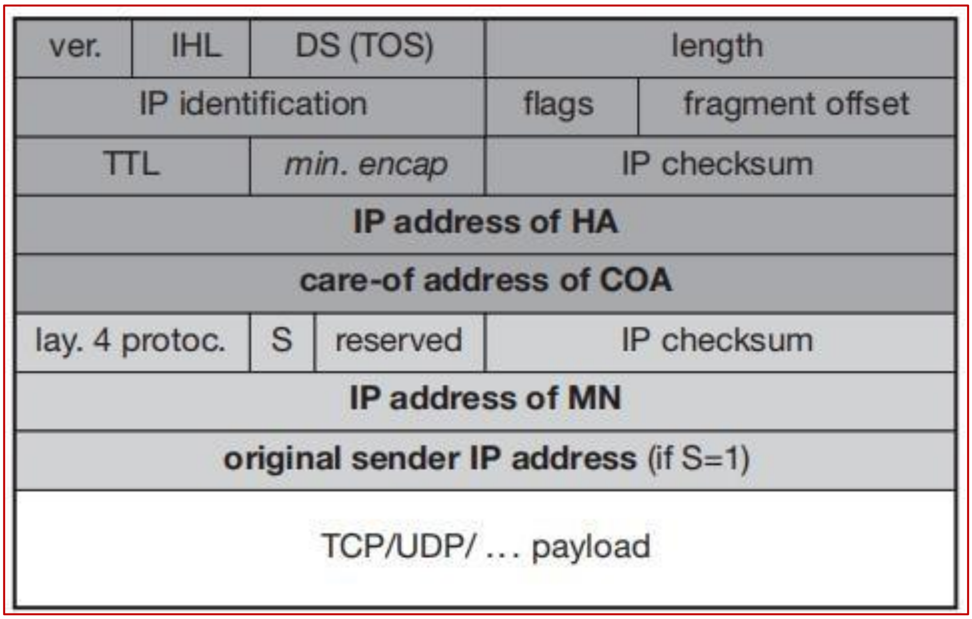
13. Finally, the payload follows the two headers.

Minimal encapsulation

As seen with IP-in-IP encapsulation, several fields are redundant.

For example, TOS is just copied, fragmentation is often not needed etc.

Therefore, minimal encapsulation (RFC 2004) as shown in Figure 6 is an optional encapsulation method for mobile IP.



<table>
<tr><td colspan="2">ver.</td><td colspan="2">IHL</td><td colspan="4">DS (TOS)</td><td colspan="8">length</td></tr>
<tr><td colspan="8">IP identification</td><td colspan="3">flags</td><td colspan="5">fragment offset</td></tr>
<tr><td colspan="4">TTL</td><td colspan="4"><i>min. encap</i></td><td colspan="8">IP checksum</td></tr>
<tr><td colspan="16"><b>IP address of HA</b></td></tr>
<tr><td colspan="16"><b>care-of address of COA</b></td></tr>
<tr><td colspan="4">lay. 4 protoc.</td><td colspan="1">S</td><td colspan="3">reserved</td><td colspan="8">IP checksum</td></tr>
<tr><td colspan="16"><b>IP address of MN</b></td></tr>
<tr><td colspan="16"><b>original sender IP address</b> (if S=1)</td></tr>
<tr><td colspan="16">TCP/UDP/ … payload</td></tr>
</table>

Fig 6: Minimal Encapsulation

1. The tunnel entry point and endpoint are specified.

2. In this case, the field for the type of the following header contains the value 55 for the minimal encapsulation protocol.

3. The inner header is different for minimal encapsulation.

4. The type of the following protocol and the address of the MN are needed.

5. If the S bit is set, the original sender address of the CN is included as omitting the source is quite often not an option.

6. No field for fragmentation offset is left in the inner header and minimal encapsulation does not work with already fragmented packets.

Generic routing encapsulation

While IP-in-IP encapsulation and minimal encapsulation work only for IP, the following encapsulation scheme also supports other network layer protocols in addition to IP.

Generic routing encapsulation (GRE) allows the encapsulation of packets of one protocol suite into the payload portion of a packet of another protocol suite.
Figure 7 shows this procedure.

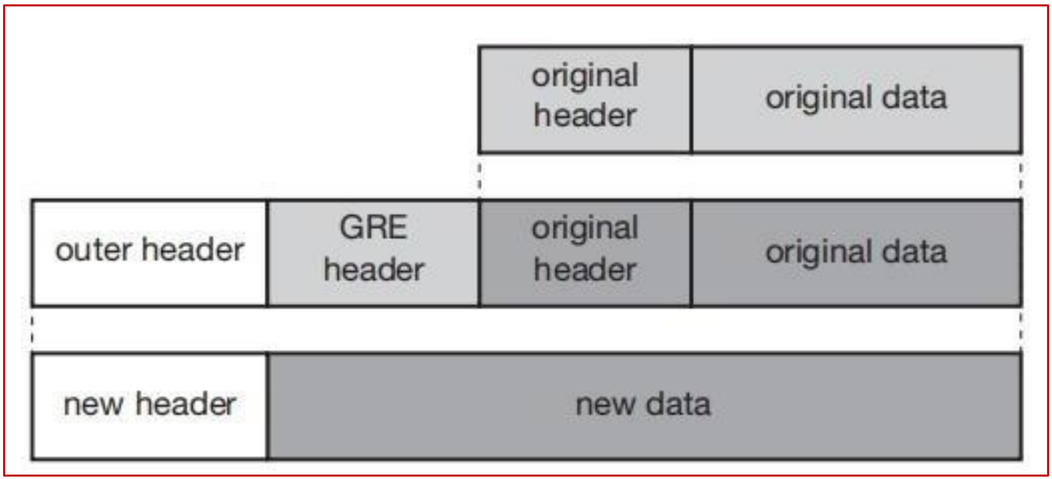


Fig 7: Generic Routing Encapsulation

The packet of one protocol suite with the original packet header and data is taken and a new GRE header is prepared.

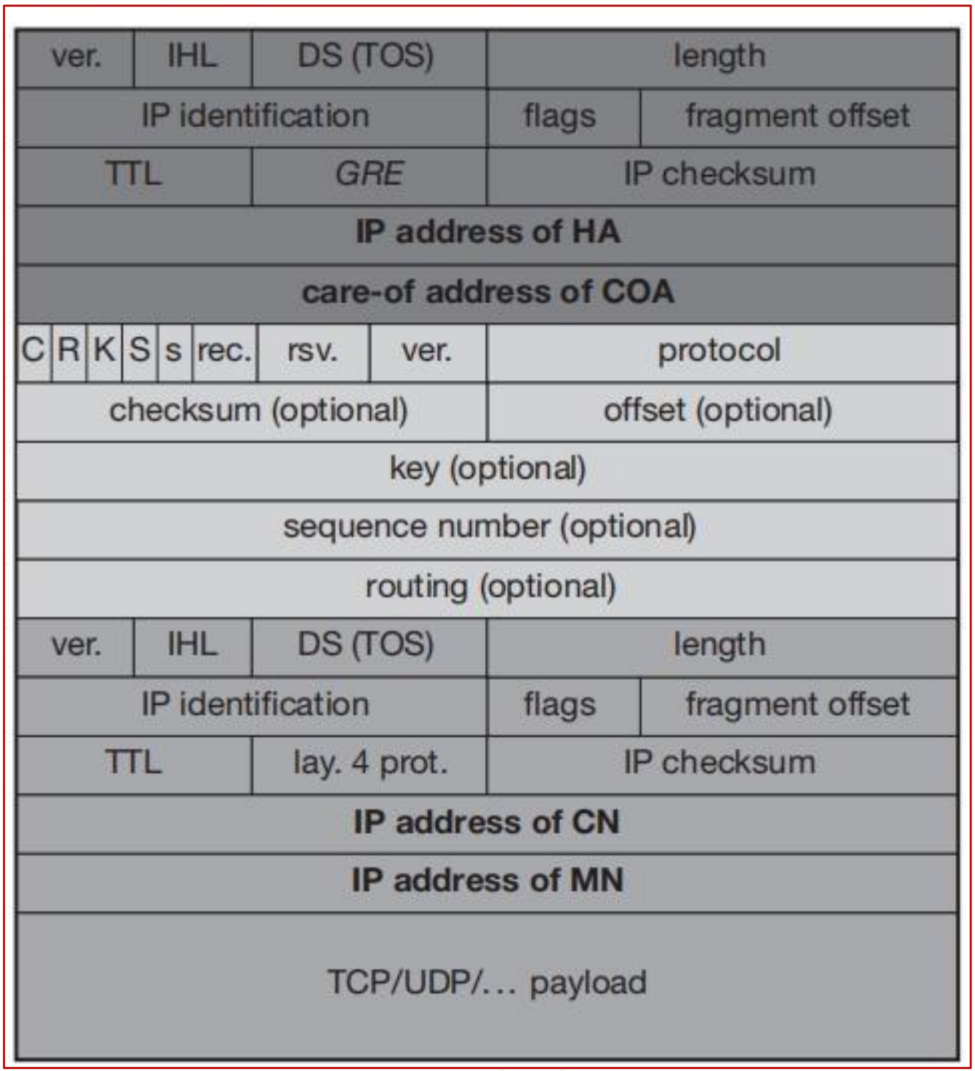
Together this forms the new data part of the new packet.

Finally, the header of the second protocol suite is put in front.

Figure 8 shows on the left side the fields of a packet inside the tunnel between home agent and COA using GRE as an encapsulation scheme according to RFC 1701.

1. The outer header is the standard IP header with HA as source address and COA as destination address.

2. The protocol type used in this outer IP header is 47 for GRE.



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

Fig 8: Protocol fields for GRE

3. The other fields of the outer packet, such as TTL and TOS, may be copied from the original IP header. However, the TTL must be decremented by 1 when the packet is decapsulated to prevent indefinite forwarding.

4. The GRE header starts with several flags indicating if certain fields are present or not.

5. A minimal GRE header uses only 4 bytes;

6. The C bit indicates if the checksum field is present and contains valid information. If C is set, the checksum field contains a valid IP checksum of the GRE header and the payload.

7. The R bit indicates if the offset and routing fields are present and contain valid information.

8. The offset represents the offset in bytes for the first source routing entry.

9. The routing field, if present, has a variable length and contains fields for source routing.

10. If the C bit is set, the offset field is also present and, vice versa, if the R bit is set, the checksum field must be present. The only reason for this is to align the following fields to 4 bytes.

11. The checksum field is valid only if C is set, and the offset field is valid only if R is set respectively.

12. GRE also offers a key field which may be used for authentication. If this field is present, the K bit is set.

13. The sequence number bit S indicates if the sequence number field is present, if the s bit is set, strict source routing is used.

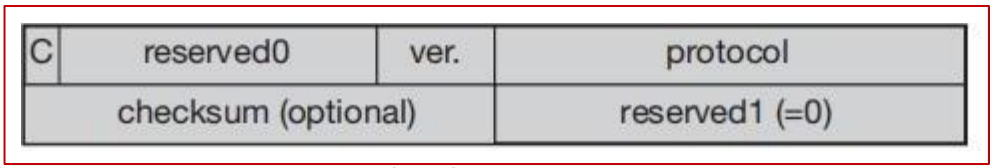
14. Sequence numbers may be used by a decapsulator to restore packet order.

15. The recursion control field (rec.) is an important field that additionally distinguishes GRE from IP-in-IP and minimal encapsulation.
16. This field represents a counter that shows the number of allowed recursive encapsulations.

17. As soon as a packet arrives at an encapsulator it checks whether this field equals zero.

18. If the field is not zero, additional encapsulation is allowed – the packet is encapsulated and the field decremented by one. Otherwise the packet will most likely be discarded. This mechanism prevents indefinite recursive encapsulation which might happen with the other schemes if tunnels are set up improperly

Figure 8.12 shows the simplified header of GRE following RFC 2784 (Farinacci, 2000), which is a more generalized version of GRE compared to RFC 1701.



C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

Fig 9: Protocol fields for GRE according to RFC 2784

1. This version does not address mutual encapsulation and ignores several protocol-specific nuances on purpose.

2. The field C indicates again if a checksum is present.

3. The next 5 bits are set to zero, then 7 reserved bits follow.

4. The version field contains the value zero.

5. The protocol type, again, defines the protocol of the payload following RFC 3232 (Reynolds, 2002).

6. If the flag C is set, then checksum field and a field called reserved1 follows.

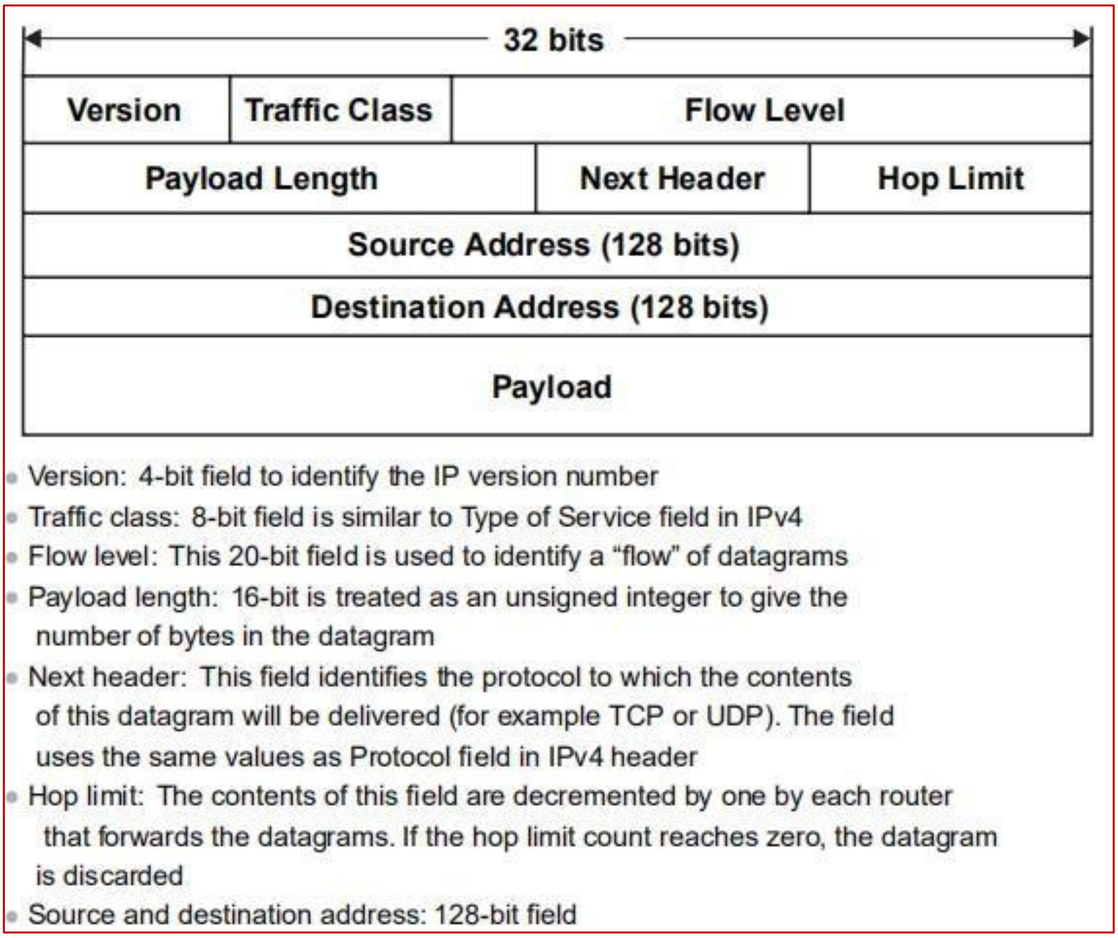
7. The latter field is constant zero set to zero follow. RFC 2784 deprecates several fields of RFC 1701, but can interoperate with RFC 1701-compliant implementations.

IPv6

The single most significant advantage IPv6 offers is increased destination and source addresses.

IPv6 quadruples the number of network address bits from 32 bits in IPv4 to 128 bits, which provides more than enough globally unique IP addresses for every network device on the planet.

- A key part of IPv6 design is its ability to integrate into and coexist with existing IP networks.
- IPv6 does not allow for fragmentation and reassembly at an intermediate router; these operations can be performed only by the source and destination.
- If an IPv6 datagram received by a router is too large to be forwarded over the outgoing link, the router simply drops the datagram and sends a *packet too big* ICMP message back to sender.
- The checksum field in IPv4 was considered redundant and was removed because the transport layer and data link layer protocols perform checksum.



- Version: 4-bit field to identify the IP version number
- Traffic class: 8-bit field is similar to Type of Service field in IPv4
- Flow level: This 20-bit field is used to identify a "flow" of datagrams
- Payload length: 16-bit is treated as an unsigned integer to give the number of bytes in the datagram
- Next header: This field identifies the protocol to which the contents of this datagram will be delivered (for example TCP or UDP). The field uses the same values as Protocol field in IPv4 header
- Hop limit: The contents of this field are decremented by one by each router that forwards the datagrams. If the hop limit count reaches zero, the datagram is discarded
- Source and destination address: 128-bit field

Fig 10: IPv6 Packet Format

- One issue is security with regard to authentication, which is now a required feature for all IPv6 nodes.

- No special mechanisms as add-ons are needed for securing mobile IP registration.

- Every IPv6 node masters address auto configuration – the mechanisms for acquiring a COA are already built in.

- Neighbor discovery as a mechanism mandatory for every node is also included in the specification; special foreign agents are no longer needed to advertise services.

- Combining the features of auto configuration and neighbor discovery means that every mobile node is able to create or obtain a topologically correct address for the current point of attachment.

- Every IPv6 node can send binding updates to another node, so the MN can send its current COA directly to the CN and HA.

- These mechanisms are an integral part of IPv6.

- A soft handover is possible with IPv6. The MN sends its new COA to the old router servicing the MN at the old COA, and the old router encapsulates all incoming packets for the MN and forwards them to the new COA.

- Altogether, mobile IP in IPv6 networks requires very few additional mechanisms of a CN, MN, and HA.

- The FA is not needed any more. A CN only has to be able to process binding updates, i.e., to create or to update an entry in the routing cache.

- The MN itself has to be able to decapsulate packets, to detect when it needs a new COA, and to determine when to send binding updates to the HA and CN. A HA must be able to encapsulate packets.

Network Layer in the Internet

The IP provides the basis for the interconnections of the Internet. IP is a datagram protocol. The packets contain an IP header.

The basic header, without options, is shown in Figure 14.4.

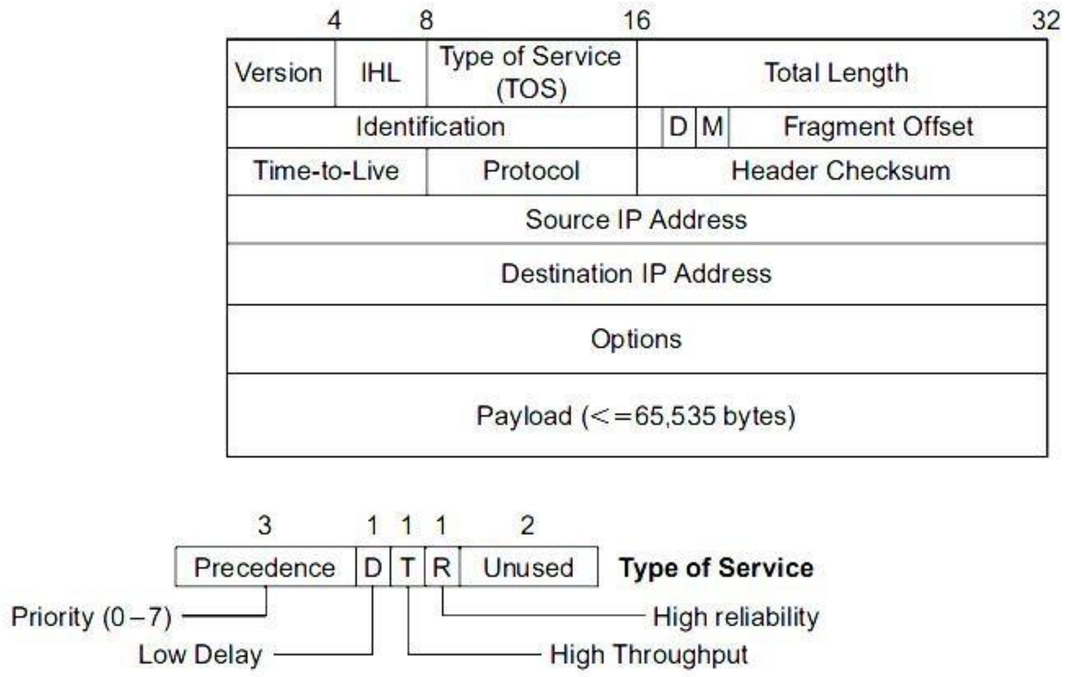


Fig 11: IP Header

The ***version*** field contains the version of IP—IPv4 or IPv6.

The ***internet header length* (IHL)** field specifies the actual length of the header in multiples of 32-bit words. The minimum length is 5. The maximum permissible length is 15.

The ***type of service* (TOS)** field allows an application protocol/process to specify the relative priority of the application data and the preferred attributes associated with the path to be followed.

The ***total length*** field defines the total length of the initial datagram including the header and payload parts. When the contents of the initial datagram need to be transferred in multiple packets, then the value in this field is used by the destination host to reassemble the payload contained within each smaller packet — known as a fragment — into the original payload.

The ***identification*** field enables the destination host to relate each received packet fragment to the same original datagram.

Don't fragment* or *D-bit is set by a source host and is examined by routers. A D-bit indicates that the packet should not be fragmented.

More fragment* or *M-bit is used during the reassembly procedure associated with data transfers involving multiple smaller packets/fragments. It is set to 1 in all but the last packet/fragment in which it is set to 0.

The ***fragment offset*** field is used to indicate the position of the first byte of the fragment contained within a smaller packet in relation to the original packet payload. All fragments except the last one are in multiples of 8 bytes.

The ***time-to-live*** field defines the maximum time for which a packet can be in transit across the Internet. The value is in seconds and is set by the IP in the source host. It is decremented by each gateway and router by a defined amount and should the value become zero, the packet is discarded.

The ***protocol*** field is used to enable the destination IP to pass the payload within each received packet to the same (peer) protocol that sent the data. This can be an internal network layer protocol such as the ICMP or a higher-layer protocol such as TCP or UDP.

The ***header checksum*** applies just to the header part of the datagram and is a safeguard against corrupted packets being routed to incorrect destinations.

The ***source and destination*** Internet addresses indicate the sending host and the intended recipient host for this datagram.

The ***options*** field is used in selected datagrams to carry additional information relating to security, source routing, loose source routing, route recording, stream identification, and time-stamp.

The last field is the ***payload***. A symbolic address, or name, of the form user@domain can be used instead of an Internet address. It is translated into an Internet address by directory tables that are organized along the same hierarchy as the addressing.

With best-effort delivery service (optional quality of service (QoS)), IP packets may be lost, corrupted, delivered out-of-order, or duplicated. The upper layer entities should anticipate and recover on an end-to-end basis.

Internet Addresses

Three classes of Internet addresses (unicast) are used (see Figure below):

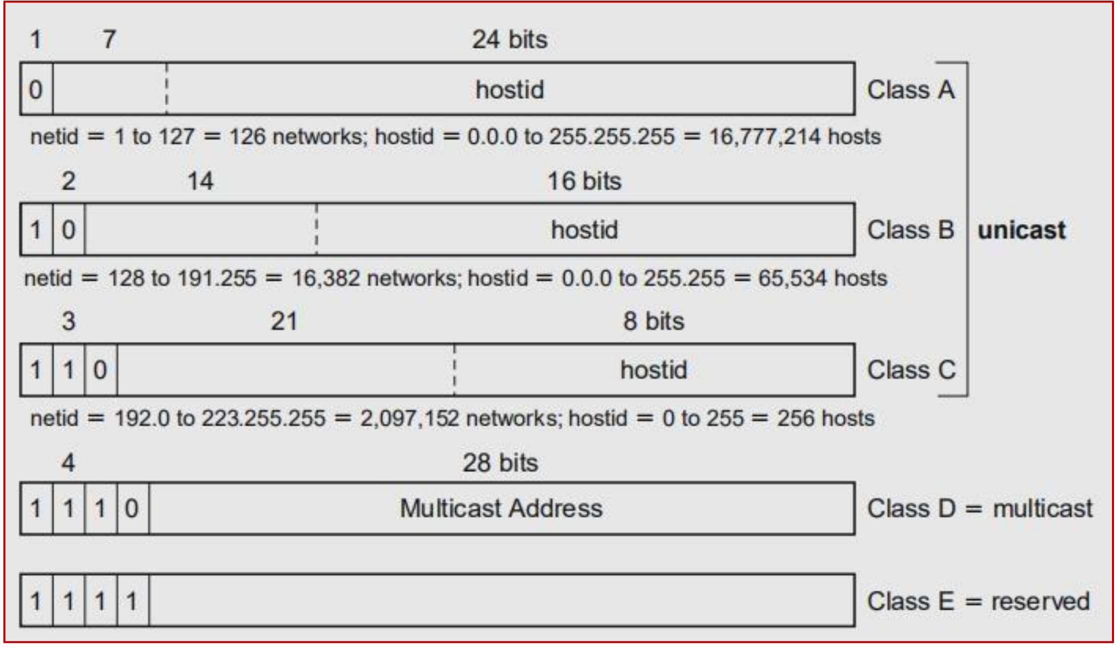
Class A — 7 bits for *netid* and 24 bits for *hostid*, they are used with networks having a large number of hosts (224)

Class B — 14 bits for *netid* and 16 bits for *hostid*, they are used with networks having a medium number of hosts (216)

Class C — 21 bits for *netid* and 8 bits for *hostid*, they are used with networks having a small number of hosts (2_8)

It should be noted that the *netid* and *hostid* with all 0s or all 1s have special meaning.

- An address with *hostid* of all 0s is used to refer to the network in netid part rather than a host
- An address with a *netid* of all 0s implies the same network as the source network/netid
- An address of all 1s means broadcast the packet over the source network
- An address with a *hostid* of all 1s means broadcast the packet over the destination network in netid part.
- A class A address with a *netid* of all 1s is used for test purposes within the protocol stack of the source host. It is known as the loop-back address.



netid = 1 to 127 = 126 networks; hostid = 0.0.0 to 255.255.255 = 16,777,214 hosts

netid = 128 to 191.255 = 16,382 networks; hostid = 0.0.0 to 255.255 = 65,534 hosts

netid = 192.0 to 223.255.255 = 2,097,152 networks; hostid = 0 to 255 = 256 hosts

Fig 12: Internet Address

IP Adjunct Protocols

Address resolution protocol (ARP) and reverse ARP (RARP) are used by IP in hosts that are attached to a broadcast LAN (such as Ethernet or token ring) in order to determine the physical MAC address of a host or gateway given its IP address (ARP), and, in case of the RARP, the reverse function.

Open shortest path first (OSPF) protocol is a routing protocol used in the global internetwork. Such protocols are present in each internetwork router. They are used to build up the contents of the routing table used to route packets across the global internetwork.

Internet control message protocol (ICMP) is used by the IP in a host or gateway to exchange errors and other control messages with IP in another host or gateway.

Internet group message protocol (IGMP) is used with multicasting to enable a host to send a copy of a datagram to the other hosts that are part of the same multicast group.

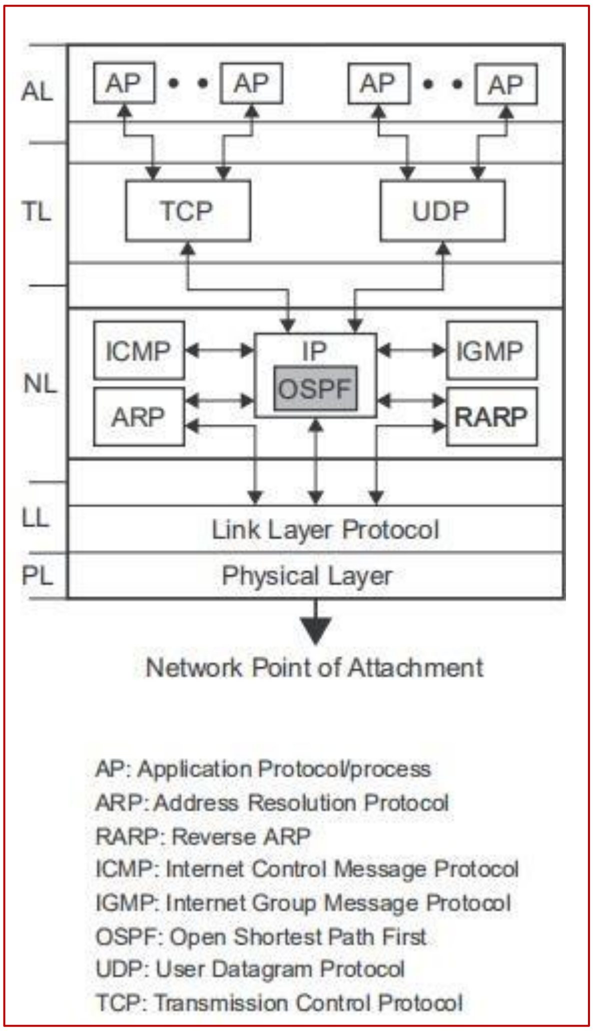

AL
TL
NL
LL
PL
AP
AP
AP
AP
TCP
UDP
ICMP
IP
OSPF
IGMP
ARP
RARP
Link Layer Protocol
Physical Layer
Network Point of Attachment
AP: Application Protocol/process
ARP: Address Resolution Protocol
RARP: Reverse ARP
ICMP: Internet Control Message Protocol
IGMP: Internet Group Message Protocol
OSPF: Open Shortest Path First
UDP: User Datagram Protocol
TCP: Transmission Control Protocol

Fig 13: Adjunct Protocols

The ICMP forms an integral part of all IP implementations. It is used by hosts, routers, and gateways for a variety of functions, and especially by network management.

The main functions associated with the ICMP are as follows:

Error reporting
Reachability testing
Congestion control
Route-change notififi cation
Performance measuring
Subnet addressing

The standard way to send an IP packet over any point-to-point link is either dial-up modems (e.g., asynch framing), leased lines (e.g., bit synchronous framing), or ISDN, IS-99 CDMA (e.g., octet-synchronous framing).

The ***link control protocol* (LCP)** runs during initial link establishment and negotiates link-level parameters (e.g., maximum frame size, etc.).

The ***IP control protocol* (IPCP)** establishes the IP address of the client (the point-to-point (PPP) server, allocates a temporary address, or the client notifies the server of the fixed address) and negotiates for the use of TCP/IP header compression.

QoS Support in the Internet

QoS requirements include a defined minimum mean packet throughput rate and a maximum end-to-end packet transfer delay.

To meet the varied set of QoS requirements, two schemes have been standardized:

Integrated Services (IntServ)
Differentiated Services (DiffServ)

Integrated Services (*IntServ*)

The ***IntServ*** solution defines three different classes of service:

- ***Guaranteed*:** It specifies maximum delay and jitter, and an assured level of bandwidth is guaranteed.
- ***Controlled load* (also known as predictive)**: No firm guarantee is provided but the flow obtains a constant level of service equivalent to that obtained with the best-effort service at light loads.
- ***Best-effort*:** This is intended for text-based applications.

Differentiated Service (*DiffServ*)

Incoming packet flows relating to individual calls are classified by the router/gateway at the edge of the *DiffServ* compliant net/Internet into one of the defined service/traffic classes by examining selected fields in various headers in the packet.

The *TOS* field in the IP packet header is replaced by a new field called the *differentiated service* (*DS*) field.

Within the *DiffServ* network, a defined level of resources in terms of buffer space within each router and the bandwidth of each output line is allocated to each traffic class.

Mobile IP (MIP) and Session Initiation Protocol (SIP)

Mobile IP is a key technology for managing mobility in wireless networks.

At the same time, the SIP is the key to realizing and provisioning services in IP-based mobile networks.

The need for mobility of future real-time service independent of terminal mobility requires SIP to seamlessly interwork with MIP operations.

Mobile IP

- The connections in an IP network use *sockets* to communicate between clients and servers.
- A socket consists of *source IP address, source port, destination IP address*, and *destination port*.
- A TCP connection cannot survive any address change because it relies on the socket to determine a connection.
- However, when a terminal moves from one network to another, its address changes.
- A mobile node (MN) is a terminal than can change its location and thus its point of attachment. The partner for communication is called the *correspondent node*

Mobile IP is designed to support host mobility on the Internet.

In order for an MN to move across different connection points while maintaining connectivity with other nodes on the Internet, the MN needs to maintain the same address.

Two versions of MIP are defined depending on IP version used in the network:
MIPv4 for IPv4 networks
and
MIPv6 for IPv6 networks.

- Mobile IP implies that a user is connected to one or more applications across the Internet, that the user's point of attachment changes dynamically, and that all connections are automatically maintained despite the change.
- When MN moves its attachment point to another network, it is considered a foreign network for this host.

- Once the mobile is reattached, it makes its presence known by registering with a network node, typically a router, on the foreign network known as a ***foreign agent*** **(FA)**.

- The mobile then communicates with a similar agent on the user's home network, known as a ***home agent*** (**HA**), giving the home agent the ***care-of address*** (**CoA**) of the mobile node; the care-of address identifies the foreign agent's location.

- A home agent tracks a mobile host's location. The mobile host is affiliated with a static IP address on the home network and a foreign agent supports mobility on a foreign network by providing routing to a visiting mobile host.

- Network supporting mobile IP will have to create foreign agents to deliver packets of information to the mobile host.

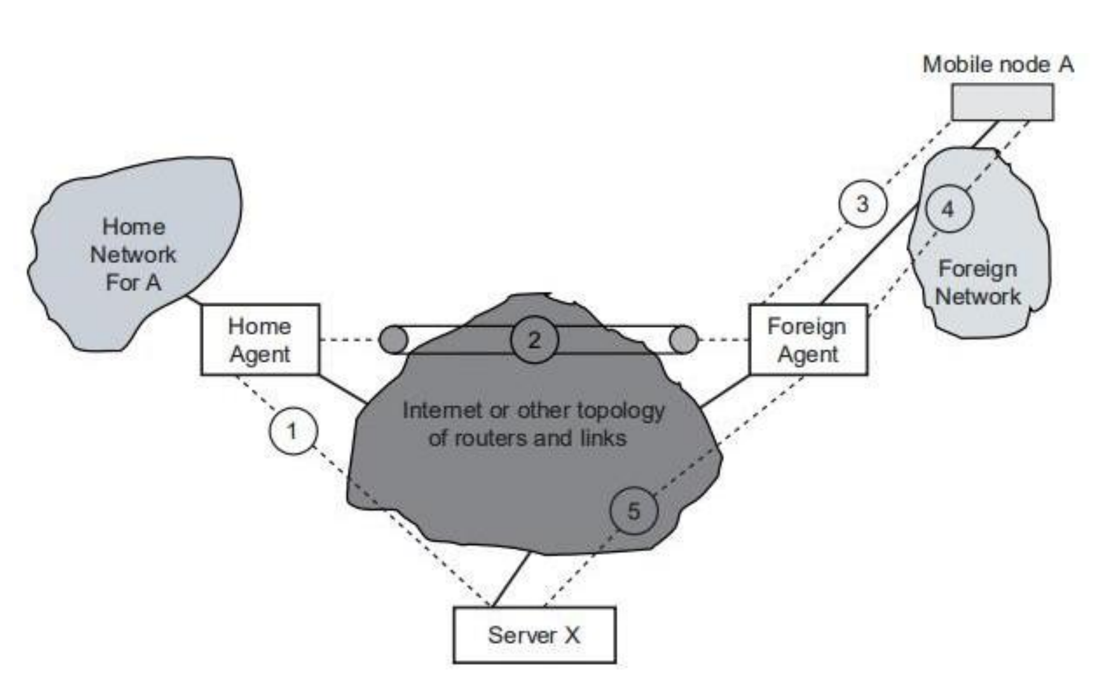


Fig 14: Mobile IP Scenario

Figure 14 shows an MIP scenario that includes the following steps:

1. Server X transmits an IP datagram destined for mobile node A, with A's home address in the IP header. The IP datagram is routed to A's home network.

2. At the home network, the incoming IP datagram is intercepted by the home agent. The home agent encapsulates the entire datagram inside a new IP datagram which has the A's care-of address in the header, and retransmits the datagram. The use of an outer IP datagram with a different destination IP address is known as *tunneling*. This IP datagram is routed to the foreign agent.

3. The foreign agent strips off the outer IP header, encapsulates the original IP datagram in a network-level packet data unit (PDU), and delivers the original datagram to A across the foreign network.

4. When A sends the IP datagram to X, it uses X’s IP address. This is a fixed address; that is, X is not a mobile node. Each IP datagram is sent by A to a router on the foreign network to X. Typically, this router is also the foreign agent.

5. The IP datagram from A to X travels directly across the Internet to X, using X’s IP address.

- In MIPv4, MN registers with an FA that becomes the point of contact for the MN.

- Subsequently, the MN updates its HA, which is a router on the home network that forwards packets meant for the MN’s home address (HoA) to theMN’s current point of attachment (i.e., the CoA of the FA).

- This allows the MN to remain “always on” — always reachable at its HoA.

- MIPv6 also supports direct peer-to-peer communication, called route optimization, between the MN and its core networks without having to traverse the HA.

- In this way, the MN uses the HoA for communication with a core network (CN) and the CoA for routing purposes.

- Since MIP operates at the network layer, any change of CoA is transparent to the transport protocols and applications.

- Hence, all applications in the MN and CN can ignore the mobility of the MN and do not have to deal with a change of network attachment.

- MIPv4 has been a standard for some years; MIPv6 is currently becoming a standard.

Mobile IP Capabilities

Three basic capabilities of MIP are registration, discovery, and tunneling.

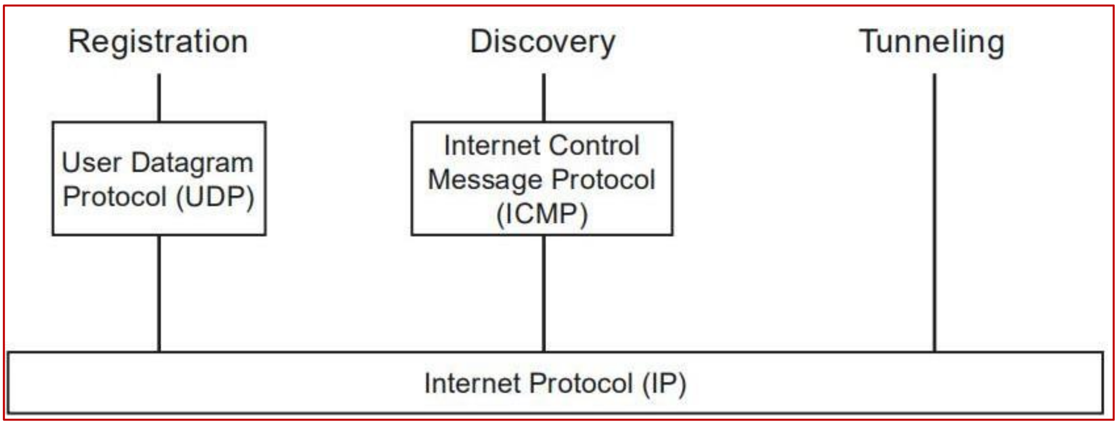

Registration
Discovery
Tunneling
User Datagram Protocol (UDP)
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)

Fig 15: Mobile IP Capabilities

Registration: A mobile node uses an authenticated registration procedure to inform its home agent of its care-of address.

Discovery: A mobile node uses a discovery procedure to identify a prospective home agent and foreign agent.

Tunneling: Tunneling is used to forward IP datagrams from a home address to a care-of address.

The discovery for a mobile node is a continuous process. Figure 16 shows the flow diagram for the agent discovery procedure.

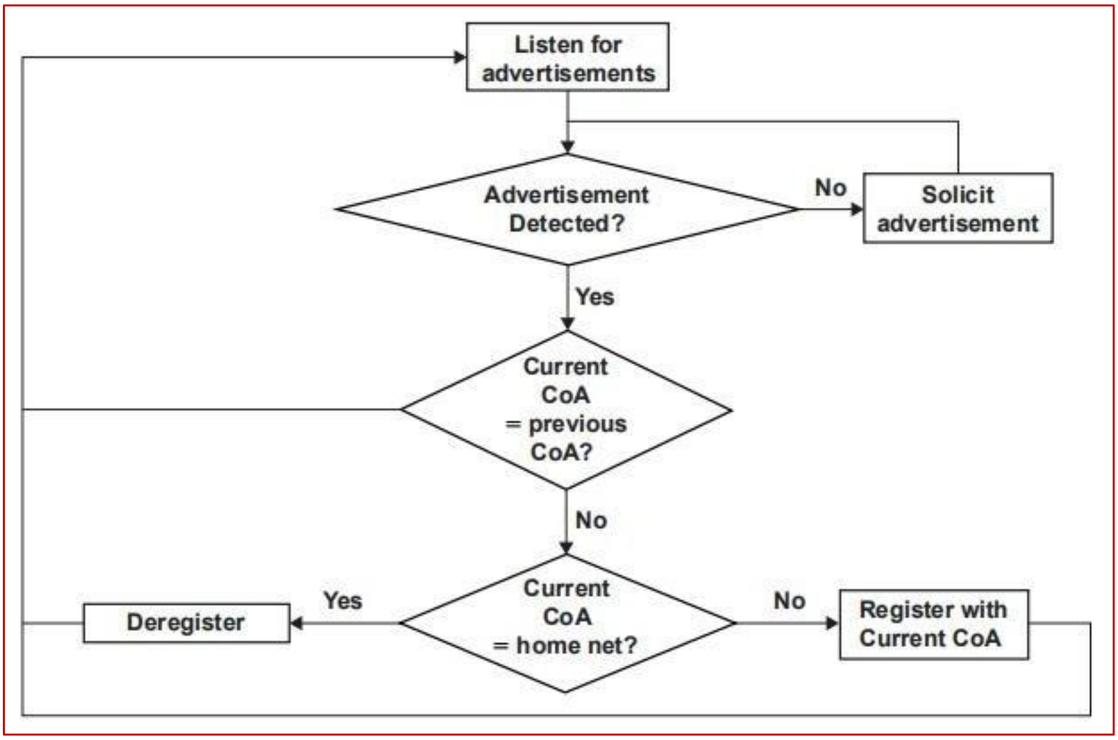


Fig 16: Agent Discovery Procedure

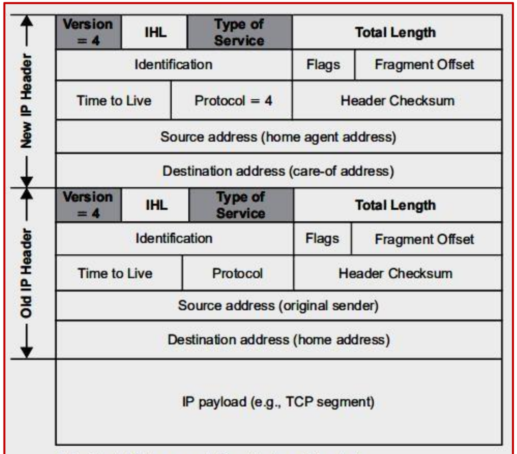
- ➢ Location management in MIP is achieved via a registration process and an agent advertisement.
- ➢ FAs and HAs periodically advertise their presence using agent advertisement messages.
- ➢ The same agent may act as both an HA and an FA — mobility extensions to ICMP messages which are used for agent advertisements.
- ➢ The messages contain information about the CoA associated with the FA, whether the agent is busy, whether minimal encapsulation is permitted, whether registration is mandatory, and so on.
- ➢ The agent advertisement packet is a broadcast message on the link.

- ➢ If the mobile node gets an advertisement from its HA, it must deregister its CoA and enable a gratuitous ARP.
- ➢ If a mobile node does not hear any advertisement, it must solicit an agent advertisement using ICMP.
- ➢ Once an agent is discovered, the MN performs either registration or deregistration with the HA, depending on whether the discovered agent is an HA or an FA. The MN sends a registration request using UDP to HA through the FA (or directly, if it is a co-located CoA).
- ➢ The HA creates a mobility binding between the MN's home address and the current CoA that has a fixed lifetime.
- ➢ The mobile node should register before expiration of the binding. A registration reply indicates whether the registration is successful.
- ➢ A rejection is possible by either the HA or FA for such reasons as insufficient resources, the home agent is unreachable, there are too many simultaneous bindings, failed authentication, and so on.

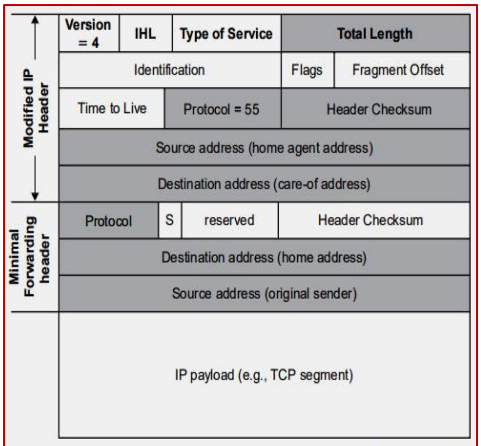
Each FA maintains a list of visiting mobiles containing the following information:

- ● Link-layer address of the mobile node
- ● Mobile node home IP address
- ● UDP registration request source port
- ● Home agent IP address
- ● An identification field
- ● Registration lifetime
- ● Remaining lifetime of pending or current registration

Need to explain the concept of IP in IP encapsulation and Minimal Encapsulation explained in pg no 13&14.



Note: Shaded fields are copied from the Inner IP header to the Outer IP header.


Modified IP Header
Version = 4
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol = 55
Header Checksum
Source address (home agent address)
Destination address (care-of address)
Minimal Forwarding header
Protocol
S
reserved
Header Checksum
Destination address (home address)
Source address (original sender)
IP payload (e.g., TCP segment)

Note: Shaded fields in the inner IP header are copied from the original IP header. Shaded fields in the outer IP header are modifed from the original IP header.

Session Initiation Protocol (SIP)

- SIP is used for provisioning services in IP-based mobile networks.

- SIP specifications define an architecture of user agents and servers (proxy server, redirect server, register) that support communications between SIP peers through user tracking, all routing, and so on.

- In SIP, each user is uniquely identified by an SIP universal resource indicator, which is used as the identifier to address the called user when the sending session initiation requests.

- However, an IP address is associated with the user in order to route SIP signaling from the SIP register.

- A SIP user registers with the SIP register to indicate its presence in the network and its willingness to receive incoming session initiation requests from other users.

- A typical session in SIP begins with a user sending an INVITE message to a peer through SIP proxies.

- When the recipient accepts the request and the initiator is notified, the actual data flow begins, usually taking a path other than the one taken by the SIP signaling messages.

- An INVITE message typically carries a description of the session parameters.

- In particular, each media component of the SIP session is described in terms of QoS parameters.

- The user can modify the parameters regarding an existing session by adding or removing media components or modifying the current QoS using a re-INVITE message.

- SIP also supports personal mobility by allowing a user to reregister with an SIP register on changing its point of attachment to the network, in particular on changing its IP address.

- A user could also change point of attachment during an active session provided the user reinvites the session providing the new parameters.

Mobile ad-hoc networks (MANET)

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes that acts as both router and hosts in an ad hoc wireless network and that dynamically self - organize in a wireless network without using any pre-established infrastructure.

Mobile IP requires, e.g., a home agent, tunnels, and default routers.

DHCP requires servers and broadcast capabilities of the medium reaching all participants or relays to servers.

Cellular phone networks require base stations, infrastructure networks etc.

- However, there may be several situations where users of a network cannot rely on an infrastructure, it is too expensive, or there is none at all.
- In these situations mobile ad-hoc networks are the only choice.
- The ad-hoc setting up of a connection with an infrastructure is not the main issue here.
- These networks should be mobile and use wireless communications.

Examples for the use of such mobile, wireless, multi-hop ad-hoc networks, which are only called ad-hoc networks here for simplicity, are:

1. **Instant infrastructure**:

   - ✓ Unplanned meetings, spontaneous interpersonal communications etc. cannot rely on any infrastructure.
   - ✓ Infrastructures need planning and administration.
   - ✓ It would take too long to set up this kind of infrastructure; therefore, ad-hoc connectivity has to be set up.

2. **Disaster relief:**

   - ✓ Infrastructures typically break down in disaster areas.
   - ✓ Hurricanes cut phone and power lines, floods destroy base stations, fires burn servers.
   - ✓ Emergency teams can only rely on an infrastructure they can set up themselves.
   - ✓ No forward planning can be done, and the set-up must be extremely fast and reliable.
   - ✓ The same applies to many military activities, which is, to be honest, one of the major driving forces behind mobile ad-hoc networking research.

3. Remote areas:

- ✓ Even if infrastructures could be planned ahead, it is sometimes too expensive to set up an infrastructure in sparsely populated areas.
- ✓ Depending on the communication pattern, ad-hoc networks or satellite infrastructures can be a solution.

4. Effectiveness:

- ✓ Services provided by existing infrastructures might be too expensive for certain applications.
- ✓ If, for example, only connectionoriented cellular networks exist, but an application sends only a small status information every other minute, a cheaper ad-hoc packet-oriented network might be a better solution.
- ✓ Registration procedures might take too long, and communication overheads might be too high with existing networks.
- ✓ Application-tailored ad-hoc networks can offer a better solution.

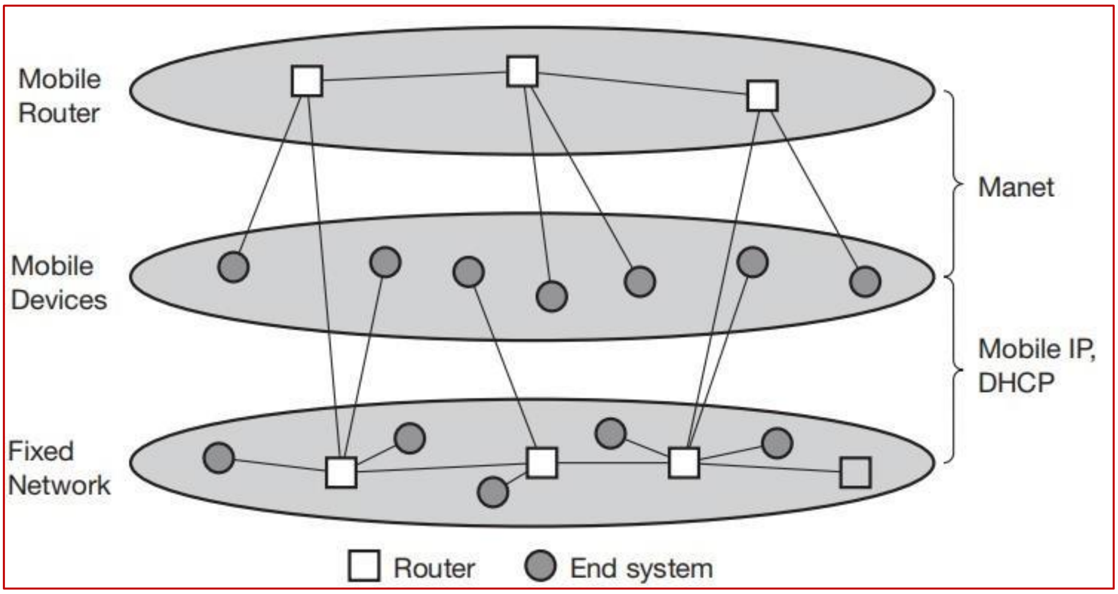


Fig 17: MANETS and MobileIP

- The above figure shows the relation of MANET to mobile IP and DHCP.
- While mobile IP and DHCP handle the connection of mobile devices to a fixed infrastructure, MANET comprises mobile routers, too.
- Mobile devices can be connected either directly with an infrastructure using Mobile IP for mobility support and DHCP as a source of many parameters, such as an IP address.

- *One of the first ad-hoc wireless networks was the packet radio network started by ARPA in 1973.*
- *It allowed up to 138 nodes in the ad-hoc network and used IP packets for data transport.A variant of distance vector routing was used in this ad-hoc network.*
- *In this approach, each node sends a routing advertisement every 7.5 s. These advertisements contain a neighbor table with a list of link qualities to each neighbor.*
- *Each node updates the local routing table according to the distance vector algorithm based on these advertisements. Received packets also help to update the routing table.*
- *A sender now transmits a packet to its first hop neighbor using the local neighbor table.*
- *Each node forwards a packet received based on its own local neighbor table.*
- *Several enhancements to this simple scheme are needed to avoid routing loops and to reflect the possibly fast changing topology.*

Routing

In an ad-hoc network, a destination node might be out of range of a source node transmitting packets.

Routing is needed to find a path between source and destination and to forward the packets appropriately.

In the case of ad-hoc networks, each node must be able to forward data for other nodes. This creates many additional problems that are discussed in the following paragraphs.

Figure 18 gives a simple example of an ad-hoc network.

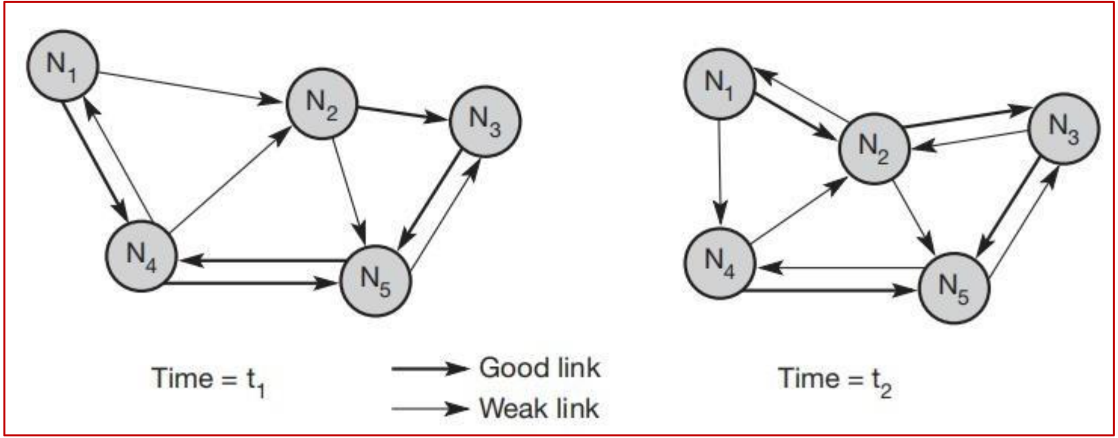


Fig 18: example ad-hoc network

1. At a certain time t1 the network topology might look as illustrated on the left side of the figure.

2. Five nodes, N1 to N5, are connected depending on the current transmission characteristics between them.

3. In this snapshot of the network, N4 can receive N1 over a good link, but N1 receives N4 only via a weak link.

4. Links do not necessarily have the same characteristics in both directions.

5. The reasons for this are, e.g., different antenna characteristics or transmit power. N1 cannot receive N2 at all, N2 receives a signal from N1.

6. This situation can change quite fast as the snapshot at t2 shows.

7. N1 cannot receive N4 any longer, N4 receives N1 only via a weak link.

8. But now N1 has an asymmetric but bi-directional link to N2 that did not exist before.

This very simple example already shows some fundamental differences between wired networks and ad-hoc wireless networks related to routing.

Asymmetric links: Node A receives a signal from node B. But this does not tell us anything about the quality of the connection in reverse. B might receive nothing, have a weak link, or even have a better link than the reverse direction.

Routing information collected for one direction is of almost no use for the other direction. However, many routing algorithms for wired networks rely on a symmetric scenario.

Redundant links: Wired networks, too, have redundant links to survive link failures. However, there is only some redundancy in wired networks, which, additionally, are controlled by a network administrator.

1. In ad-hoc networks nobody controls redundancy, so there might be many redundant links up to the extreme of a completely meshed topology.

2. Routing algorithms for wired networks can handle some redundancy, but a high redundancy can cause a large computational overhead for routing table updates.

Interference: In wired networks links exist only where a wire exists, and connections are planned by network administrators. This is not the case for wireless ad-hoc networks.

1. Links come and go depending on transmission characteristics, one transmission might interfere with another, and nodes might overhear the transmissions of other nodes.

2. Interference creates new problems by ‘unplanned’ links between nodes: if two close-by nodes forward two transmissions, they might interfere and destroy each other.

3. On the other hand, interference might also help routing. A node can learn the topology with the help of packets it has overheard.

Dynamic topology: The greatest problem for routing arises from the highly dynamic topology.

1. The mobile nodes might move as shown in Figure 18 or medium characteristics might change.

2. This results in frequent changes in topology, so snapshots are valid only for a very short period of time.

3. In ad-hoc networks, routing tables must somehow reflect these frequent changes in topology, and routing algorithms have to be adapted.

4. Routing algorithms used in wired networks would either react much too slowly or generate too many updates to reflect all changes in topology.

5. Routing table updates in fixed networks, for example, take place every 30 seconds.

6. This updating frequency might be too low to be useful for ad-hoc networks.

7. Some algorithms rely on a complete picture of the whole network. While this works in wired networks where changes are rare, it fails completely in ad-hoc networks.

8. The topology changes during the distribution of the ‘current’ snapshot of the network, rendering the snapshot useless.

Let us go back to the example network in Figure 18 and assume that node N1 wants to send data to N3 and needs an acknowledgement.

- If N1 had a complete overview of the network at time t1, which is not always the case in ad-hoc networks, it would choose the path N1, N2, N3, for this requires only two hops (if we use hops as metric).

- Acknowledgements cannot take the same path, N3 chooses N3, N5, N4, N1. This takes three hops and already shows that routing also strongly influences the function of higher layers.

- TCP, for example, makes round trip measurements assuming the same path in both directions.

- This is obviously wrong in the example shown, leading to misinterpretations of measurements and inefficiencies.

- Just a moment later, at time t2, the topology has changed. Now N3 cannot take the same path to send acknowledgements back to N1, while N1 can still take the old path to N3.
- Although already more complicated than fixed networks, this example still assumes that nodes can have a complete insight into the current situation.
- The optimal knowledge for every node would be a description of the current connectivity between all nodes, the expected traffic flows, capacities of all links, delay of each link, and the computing and battery power of each node.
- While even in fixed networks traffic flows are not exactly predictable, for ad-hoc networks link capacities are additionally unknown.
- The capacity of each link can change from 0 to the maximum of the transmission technology used.
- In real ad-hoc networks no node knows all these factors, and establishing up-to-date snapshots of the network is almost impossible.

Challenges:

- Ad-hoc networks using mobile nodes face additional problems due to hardware limitations. Using the standard routing protocols with periodic updates wastes battery power without sending any user data and disables sleep modes.
- Periodic updates waste bandwidth and these resources are already scarce for wireless links.
- An additional problem is interference between two or more transmissions that do not use the same nodes for forwarding.
- If, for example, a second transmission from node N4 to N5 (see Figure 18) takes place at the same time as the transmission from N1 to N3, they could interfere.
- Interference could take place at N2 which can receive signals from N1 and N4, or at N5 receiving N4 and N2. If shielded correctly, there is no interference between two wires.

Considering all the additional difficulties in comparison to wired networks, the following observations concerning routing can be made for ad-hoc networks with moving nodes.

- Traditional routing algorithms known from wired networks will not work efficiently (e.g., distance vector algorithms such as RIP converge much too slowly) or fail completely (e.g., link state algorithms such as OSPF exchange complete pictures of the network). These algorithms have not been designed with a highly dynamic topology, asymmetric links, or interference in mind. Routing in wireless ad-hoc networks cannot rely on layer three knowledge alone. Information from lower layers concerning connectivity or interference can help routing algorithms to find a good path.

- Centralized approaches will not really work, because it takes too long to collect the current status and disseminate it again. Within this time the topology has already changed.

- Many nodes need routing capabilities. While there might be some without, at least one router has to be within the range of each node. Algorithms have to consider the limited battery power of these nodes.

- The notion of a connection with certain characteristics cannot work properly. Ad-hoc networks will be connectionless, because it is not possible to maintain a connection in a fast changing environment and to forward data following this connection. Nodes have to make local decisions for forwarding and send packets roughly toward the final destination.

A last alternative to forward a packet across an unknown topology is flooding. This approach always works if the load is low, but it is very inefficient. A hop counter is needed in each packet to avoid looping, and the diameter of the ad-hoc network, i.e., the maximum number of hops, should be known. (The number of nodes can be used as an upper bound.) Hierarchical clustering of nodes might help. If it is possible to identify certain groups of nodes belonging together, clusters can be established. While individual nodes might move faster, the whole cluster can be rather stationary.

Routing between clusters might be simpler and less dynamic.

The following sections give two examples for routing algorithms that were historically at the beginning of MANET research, **DSDV and DSR**, and useful metrics that are different from the usual hop counting.

Destination sequence distance vector

Destination sequence distance vector (DSDV) routing is an enhancement to distance vector routing for ad-hoc networks.

DSDV can be considered historically, however, an on-demand version (ad-hoc on-demand distance vector, AODV) is among the protocols currently discussed.

Distance vector routing is used as routing information protocol (RIP) in wired networks. It performs extremely poorly with certain network changes due to the count-to-infinity problem. Each node exchanges its neighbor table periodically with its neighbors. Changes at one node in the network propagate slowly through the network (step-by-step with every exchange).

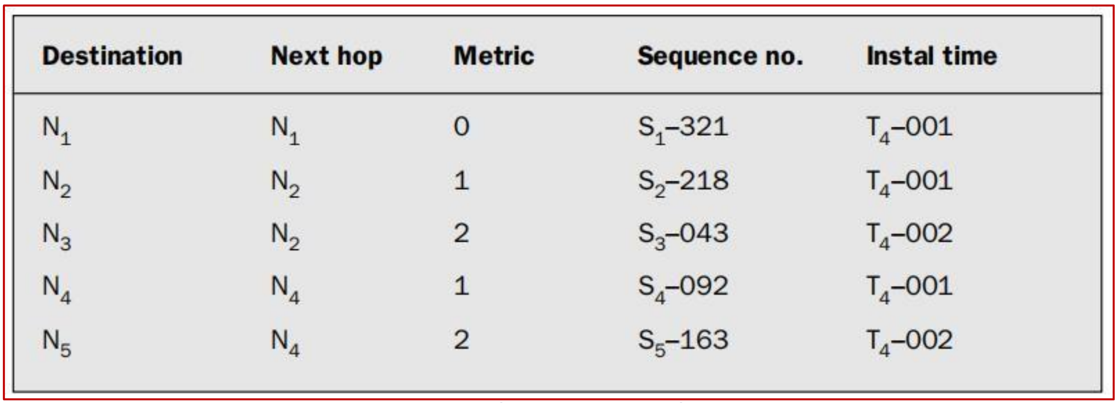
The strategies to avoid this problem which are used in fixed networks (poisoned-reverse/split horizon) do not help in the case of wireless ad-hoc networks, due to the rapidly changing topology. This might create loops or unreachable regions within the network.

DSDV now adds two things to the distance vector algorithm:

- Sequence numbers:
  1. Each routing advertisement comes with a sequence number.
  2. Within ad-hoc networks,advertisements may propagate along many paths.
  3. Sequence numbers help to apply the advertisements in correct order.
  4. This avoids the loops that are likely with the unchanged distance vector algorithm.

- Damping:
  1. Transient changes in topology that are of short duration should not destabilize the routing mechanisms.
  2. Advertisements containing changes in the topology currently stored are therefore not disseminated further.
  3. A node waits with dissemination if these changes are probably unstable.
  4. Waiting time depends on the time between the first and the best announcement of a path to a certain destination.

The routing table for N1 in Figure 8.20 would be as shown in Table 8.2.



Destination	Next hop	Metric	Sequence no.	Instal time
N_1	N_1	0	S_1–321	T_4–001
N_2	N_2	1	S_2–218	T_4–001
N_3	N_2	2	S_3–043	T_4–002
N_4	N_4	1	S_4–092	T_4–001
N_5	N_4	2	S_5–163	T_4–002

Table 1: Part of a Routing Table for DSDV

For each node N1 stores the next hop toward this node, the metric (here number of hops), the sequence number of the last advertisement for this node, and the time at which the path has been installed first.

The table contains flags and a settling time helping to decide when the path can be assumed stable.

Router advertisements from N1 now contain data from the first, third, and fourth column: destination address, metric, and sequence number.

Besides being loop-free at all times, DSDV has low memory requirements and a quick convergence via triggered updates.

IoT:COAP

Internet of Things : COnstrained Application Protocol

- Internet of Things (IoT) is represented as a global network which intelligently connects all the objects no matter devices, systems or human, it is with self-configuring capabilities based on standard and interoperable protocols and formats.

- Through smart sensing, identification technology and persuasive computing, IoT has been called the Third Wave in information industry following the computer and the Internet.

- There are hundreds of protocols supported by IoT.

- Of the many protocols, wireless protocols play an important role in IoT development.

- Some wireless protocols in different layers of IoT are introduced. One latest protocol for application layer CoAP is given and its features and functions are summarized.

- CoAP is one of the latest application layer protocol developed by IETF for smart devices to connect to Internet.

- As many devices exist as components in vehicles and buildings with constrained resources, it leads a lot of variation in power computing, communication bandwidth etc.

- Thus lightweight protocol CoAP is intended to be used and considered as a replacement of HTTP for being an IoT application layer protocol.

CoAP is an IoT protocol.

CoAP stands for Constrained Application Protocol, and it is defined in RFC 7252.

CoAP is a simple protocol with low overhead specifically designed for constrained devices (such as microcontrollers) and constrained networks.

This protocol is used in M2M data exchange and is very similar to HTTP, even if there are important differences that we will cover laters.

CoAP Features

1. With the completion of the CoAP specification, it is expected that there will be million of devices deployed in various application domains in the future.

2. These applications range from smart energy, smart grid, building control, intelligent lighting control, industrial control systems, asset tracking, to environment monitoring.

3. CoAP would become the standard protocol to enable interaction between devices and to support IoT applications.

4. The Constrained RESTful Environments (CoRE) is the workgroup in IEFT that is designing the CoAP protocol.

Security Protocol for CoAP

1. CoAP is now becoming the standard protocol for IoT applications.

2. Security is important to protect the communication between devices.

3. In the following part, a security protocol DTLS (Datagram Transport Layer Security) is introduced.

4. There are three main elements when considering security, namely integrity, authentication and confidentiality. DTLS can achieve all of them

CoAP Application for Smart Homes

1. Information appliance, control equipment and communication equipment in Smart home networks have the characters of low-cost and light weight.

2. Smart home network provide controlling and monitoring energy of home devices.

3. Energy control systems employ smart socket management and monitor power consuming equipment to provide voltage, current and other energy information.

4. It could realize accident warning, remote control and dynamic energy saving.

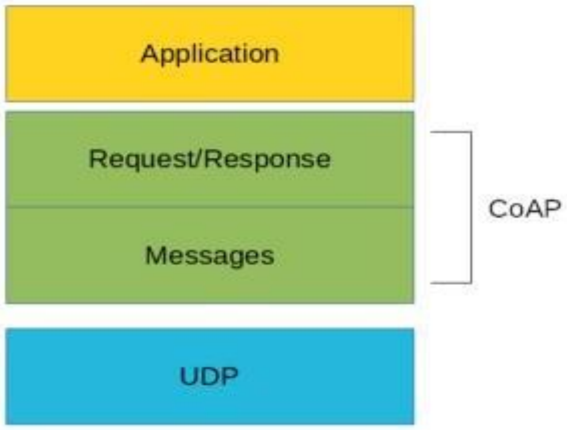


Fig 19: CoAP Abstraction Protocol La