ITS413 – Mobile IP Example

Internet Technologies and Applications, Semester 2, 2010

Prepared by Steven Gordon on 21 December 2010
ITS413Y10S2H10, Steve/Courses/ITS413/Examples/mobileip-example.tex, r1582

1 Network Topology

Consider the example network topology in Figure 1. There are six routers, A to F, in the internet. The network mask /24 are used for all IP subnets. Next to each router there is an interface number. This interface number is used to determine the routers IP address. For example, router B has two IP addresses: `2.2.2.1` and `3.3.3.2`. Assume routing tables of all routers and hosts are constructed such that the path with least number of hops will be used.

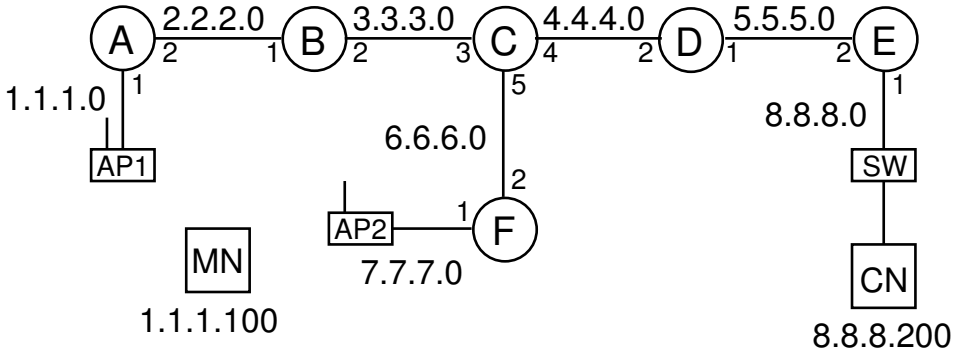


Figure 1: Network Topology

On subnet `1.1.1.0` there is a IEEE 802.11 wireless LAN access point as well as a Mobile Node with (home) address `1.1.1.100` (and with MAC address `00:17:31:12:34:56`—this is not shown). A correspondent node is in subnet `8.8.8.0`. We will consider a case where MN moves to a new IP subnet, `7.7.7.0`, attaching to the access point AP2. We will assume router A is the Home Agent (HA) of MN and router F is a Foreign Agent (FA).

2 Wireless LAN Handover

Although Mobile IP is independent of the wireless access technology (IEEE 802.11, 3G, ...), for this example we will illustrate IEEE 802.11 in use.

Assume MN is moving from near AP1 towards AP2. There are two simple techniques for MN to decide to initiate a handover:

1. If AP1 and AP2 are using different channels, then while associated with AP1, MN will not receive Beacons from AP2. In this case MN will only initiate a handover to a new AP once the signal strength from AP1 becomes too weak (or the signal is lost, i.e. no Beacons are received). When this occurs, the MN scans through the available channels trying to hear Beacons on each. It will eventually receive a Beacon from AP2 and initiate the association.

2. If AP1 and AP2 are using the same channel it is likely that MN will be receiving beacons from both APs. In this case the MN can be "smarter" and decide to initiate a handover to AP2 when it recognises the signal strength is stronger than that of AP1 (of course, some hysteresis should be used, such as "the signal strength of the past 3 Beacons from the potential new AP must be 10% stronger than the existing AP"). As soon as the MN decides to handover it can immediately initiate the association—there is no need to scan the channels for Beacons.

Figure 2 illustrates the wireless LAN handover. At step (1), after receiving Beacon frames from both APs the MN decides to handover to AP2 (this assumes the 2nd approach above). Then the authentication and association is performed. Assuming everything is successful, at step (2) MN is associated with AP2, and can now send IP datagrams on the subnet `7.7.7.0`.

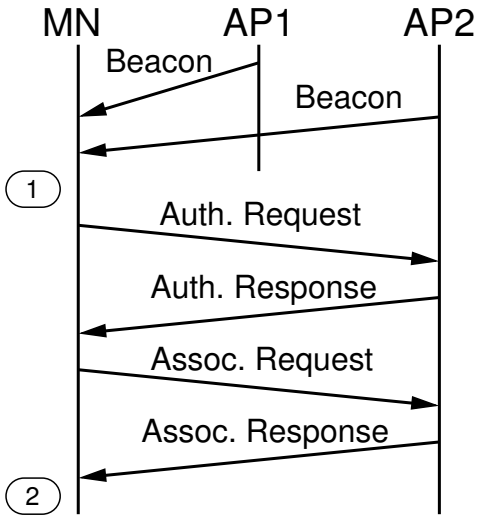


Figure 2: Wireless LAN Handover

From now on, for simplicity and clarity, we will hide the communications with the AP, showing only packets sent across a subnet.

3 Foreign Agent Discovery

How does the MN know it is in a new subnet? Either:

1. MN receives a Router Advertisement from a new FA;
2. No Router Advertisement is received from the old FA after some period, triggering the MN to send a Router Solicitation to see if it is in a new subnet; or
3. The Layer 2 protocol (wireless LAN in our example) is adapted to inform the MN that is in a new subnet (e.g. the Beacon frames could carry information indicating the IP subnet).

Figure 3, which continues on from step (2) in Figure 2, illustrates a case when either option 2 above are used. The MN broadcasts a Router Solicitation on the IP subnet. The

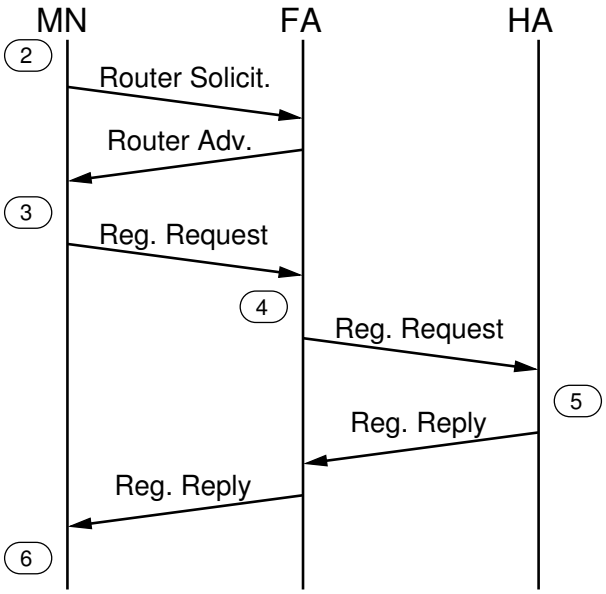


Figure 3: Foreign Agent Discovery

```
+------+------+
|  IP  | ICMP |
+------+------+
  |
  |- src = 0.0.0.0
  |- dst = 255.255.255.255
```

Figure 4: Router Solicitation Packet

structure of the Router Solicitation is shown in Figure 4. Only header fields important for this example are shown.

All nodes on the subnet `7.7.7.0` will receive the Router Solicitation; only the FA will respond (with a Router Advertisement). The Router Advertisement is broadcast by the FA; the structure of the packet is shown in Figure 5.

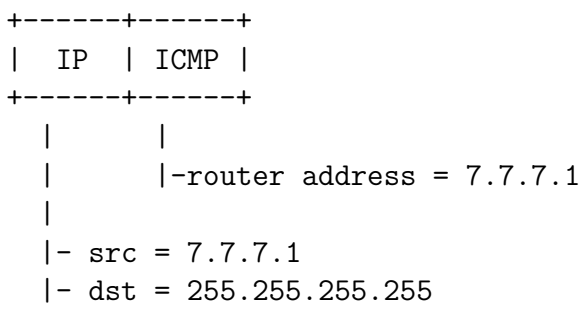


Figure 5: Router Advertisement Packet

The ICMP packet includes a field indicating the address of the router/FA. In this case it is the same as the IP source address. However in practice it can be more complex than described in this example (e.g. multiple router addresses can be advertised; multicast can be used instead of local broadcast).

Now the MN has discovery a FA (`7.7.7.1`) in this foreign network. Next at step (3) Mobile IP registration starts.

4 Registration

Mobile IP registration involves the MN registering as a visitor on the foreign network, as well as informing the HA where it is. This must include authentication to make sure the MN is allowed to use the foreign network—this detail is hidden from the example (we assume the MN is allowed).

At step (3) in Figure 3 the MN sends a Registration Request to the FA. This message is carried inside a UDP datagram (which is in an IP datagram). The Registration Request is shown in Figure 6.

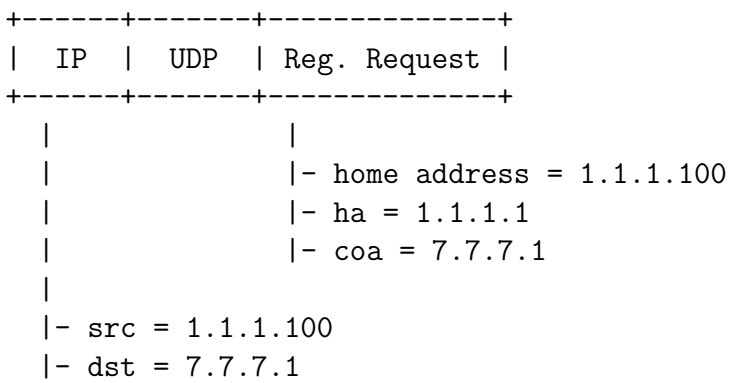


Figure 6: Mobile IP Registration Request

Three important fields are in the Registration Request:

Home Address: Home IP address of the MN

Home Agent: IP address of the MN's HA

Care-of Address: CoA the MN will use in the foreign network

In this example we assume the MN will the FA's address as the CoA (an alternative is for the FA to assign a unique CoA to the MN). But this is strange: now both the FA and the MN will have the same IP address (`7.7.7.1`). And if there are multiple visiting MNs in this network, they will also have the same IP address (`7.7.7.1`). How does this work? For example, an IP datagram arrives with destination address `7.7.7.1`—which node is the real destination? We will see shortly that since all packets to/from this address go via the FA, the FA can determine who the real source/destination as it keeps track of the home addresses and MAC addresses.

At step (4) upon receiving the Registration Request, after checking for correct authentication, the FA sends a new Registration Request to the HA. It structure is similar to that in Figure 6 except the IP source and destination address will be `7.7.7.1` and `1.1.1.1`, respectively.

At step (5) upon receiving the Registration Request, if everything is successful the HA sends a Registration Reply (see Figure 7). In addition, the HA updates its *Mobility Binding Table*.

```
+------+-------+--------------+
|  IP  |  UDP  | Reg. Request |
+------+-------+--------------+
  |               |
  |               |- home address = 1.1.1.100
  |               |- ha = 1.1.1.1
  |
  |- src = 1.1.1.1
  |- dst = 7.7.7.1
```

Figure 7: Mobile IP Registration Reply

The Mobility Binding Table at the HA is the HA's record of the location of its (away) MNs. The important information stored is shown in Figure 8. (Other information may also be stored, such as the lifetime of the binding; if the lifetime expires before any update is received from the MN, the HA will remove the entry from the table.)

When the Registration Reply is received by the FA, the FA updates its list of visiting MNs, i.e. the *Visitors List* as illustrated in Figure 9.

Finally, at step (6) the Registration Reply is received by the MN. The MN now knows that the registration was successful and can start sending IP datagrams on the network.

5 Tunnelling

Recall that the aim of Mobile IP is that the CN and MN can continue to communicate (sending IP datagrams to each other) as a MN moves between IP subnets *without the*

HomeIP	CoA
1.1.1.100	7.7.7.1

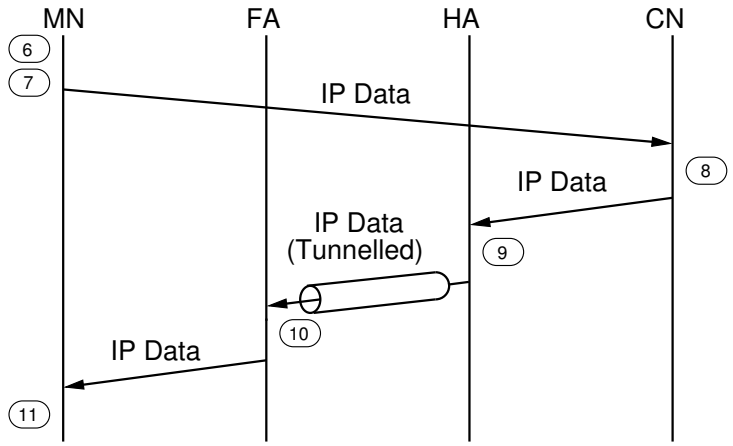
Figure 8: Mobile Binding Table at HA

HomeIP	HA	MAC
1.1.1.100	1.1.1.1	00:17:31:12:34:56

Figure 9: Visitors List at FA

applications knowing of a change of IP address. That is, the change of IP subnet is hidden from the transport protocol (e.g. TCP or UDP) and application. We will see this when we see the source/destination addresses of the packets sent/received by the MN and CN.

Figure 5 shows the path of IP datagrams (carrying application data) in the direction from MN to CN and from CN to MN. Consider first sending MN to CN, starting at step (7).



The application on the MN creates data, delivering it to the transport protocol (TCP in this example) which then delivers the segment to IP, indicating the destination IP address of the CN (`8.8.8.200`). This procedure remains the same no matter where the MN is: in its home network or away in a foreign network. The IP datagram created is shown in Figure 10 ("App. Data" could be a in fact the header for a specific application protocol such as HTTP as well as the data).

Now lets consider how this IP datagram is forwarded to the CN (refer to the routing tables in Figure 11). First the MN looks up its routing table to determine where to send to reach network `8.8.8.0`. The routing table should be configured such that FA/Router F is the default router/gateway. That is, to reach any network (except its own) send datagrams to `7.7.7.1`.

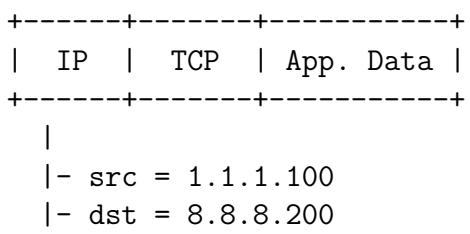


Figure 10: IP Datagram from MN to CN

MN:

Dest.	Next
7.7.7.0	direct
*	7.7.7.1

CN:

Dest.	Next
8.8.8.0	direct
*	8.8.8.1

A:

Dest.	Next
1.1.1.0	direct
2.2.2.0	direct
*	2.2.2.1

B:

Dest.	Next
2.2.2.0	direct
3.3.3.0	direct
1.1.1.0	2.2.2.2
*	3.3.3.3

C:

Dest.	Next
3.3.3.0	direct
4.4.4.0	direct
6.6.6.0	direct
1.1.1.0	3.3.3.2
2.2.2.0	3.3.3.2
5.5.5.0	4.4.4.2
8.8.8.0	4.4.4.2
7.7.7.0	6.6.6.2

D:

Dest.	Next
4.4.4.0	direct
5.5.5.0	direct
8.8.8.0	5.5.5.2
*	4.4.4.4

E:

Dest.	Next
5.5.5.0	direct
8.8.8.0	direct
*	5.5.5.1

F:

Dest.	Next
6.6.6.0	direct
7.7.7.0	direct
*	6.6.6.5

Figure 11: Routing Tables of All Nodes

MN sends the IP datagram to router F (the FA). Note that many routers with access networks attached are configured to drop (disallow) datagrams that have a source address that doesn't match the access networks subnet address. That is, router F would normally only expect to receive datagrams on interface 1 with source address `7.7.7.0`. But in this instance the source address is `1.1.1.100`. In this special case router F allows the datagram because this source address is registered in the Visitors List. Router F then uses its routing table to forward the datagram to router C.

Router C now has an IP datagram (shown in Figure 10) with destination address `8.8.8.200`. The router uses its routing table to determine to forward the datagram to router D. This is the normal IP routing procedure. Following the routing tables, the IP datagram will be eventually delivered to the destination, CN at `8.8.8.200`. The datagram traversed the path of routers F–C–D–E, which is the optimal path (least number of hops). Nothing special was needed in this case; normal IP routing delivered the datagram to the correct destination. The IP datagram received by the CN has the same source/destination addresses as an IP datagram sent by the MN if it was in its home network (or any other foreign network). That is, the CN doesn't know the MN has changed networks.

Now consider the reverse direction (step (8) in Figure 5): CN sending an IP datagram, illustrated in Figure 12, to MN. The datagram destination address is the home address of the MN.

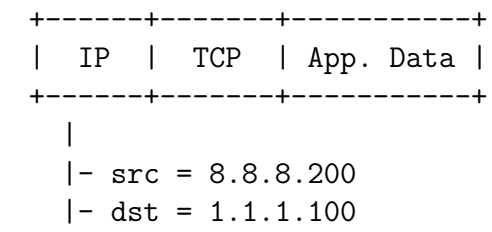


Figure 12: IP Datagram from CN to MN (sent by CN)

Now following the routing tables we can see that this datagram will traverse the path of routers E–D–C–B–A (since the destination is on network `1.1.1.0`). The routers E, D, C and B do not know about the mobility of MN, and hence deliver the datagram to the home network.

At step (9) router A receives the datagram. Normally, router A would look in its routing table and determine to send directly to the destination. But since router A is also a HA, it first consults its Mobility Binding Table (Figure 8). Router A sees that the destination of this datagram, `1.1.1.100`, is not home, but visiting a foreign network. From the Mobility Binding Table the HA knows the CoA of the MN is `7.7.7.1`. So HA constructs a *tunnel* to the CoA by placing the original IP datagram inside another IP datagram as illustrated in Figure 13.

The outer IP header indicates the source is the HA and the destination is the CoA (the FA). This datagram is then sent. Following the routing tables, the datagram will be delivered to router F via the path B–C (note the routers B and C only look at the outer header; they don't care about the contents of the IP datagram, which is in fact another IP datagram). Router F is the destination of this datagram and hence removes the IP header to find another IP datagram (shown in Figure 14). Since router F is a FA it compares the destination address of the remaining IP datagram (`1.1.1.100`) with its Visitors List.

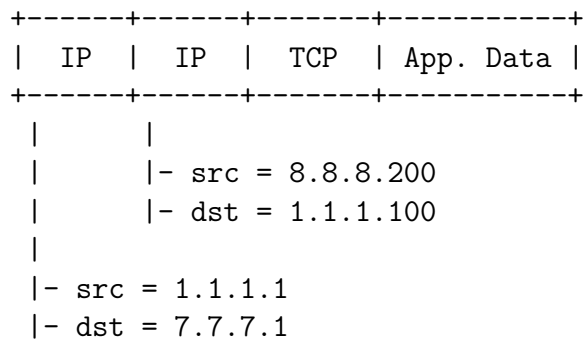


Figure 13: IP Datagram from CN to MN (sent by HA)

The destination is in the list. Therefore instead of using its routing table (which would send the datagram back to router A), router F realises from the Visitors List that the datagram must be sent direct to the host (with MAC address `00:17:31:12:34:56`). The datagram is sent on the LAN and will be received by the MN.

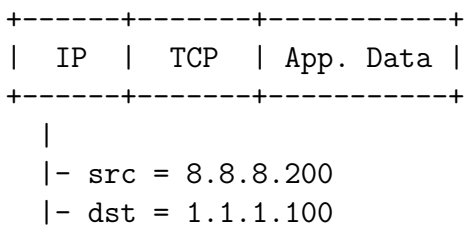


Figure 14: IP Datagram from CN to MN (sent by FA)

Again, look at the datagrams sent by CN and received by MN: both are identical and use the home IP address of MN. That is, from the CN and MN transport/application perspective, the datagram has been delivered as if the MN was still home. The goal of Mobile IP has been achieved: datagrams are delivered to mobile nodes no matter where they are in the Internet, without the application being aware of the mobility.

This example aimed to illustrate the key operations in Mobile IP. Some details have been hidden to make it easier to understand. It should be clear that sending data from CN to MN may result in extra (significant) delay since the datagram must go via the HA. There are more mechanisms within Mobile IP (and Mobile IPv6) to try to optimise the performance of data delivery to mobile nodes in the Internet. See links on the course website or talk to me if you are interested.