■ ECE/CS 4984: Wireless Networking and Mobile Systems ■

Pre-lab and In-class Laboratory Exercise 9 (L9)

Part I – Objectives and Lab Materials

Objective

The objectives of this lab are to:

- Familiarize students with the operation of Mobile IP.
- Investigate delay, throughput and overhead of Mobile IP.

After completing the assignment, the student should be able to:

- Explain the operation of the home agent, the foreign agent and the mobile node in Mobile IP.
- Understand the routing and tunneling operation in Mobile IP.
- Configure the Dynamics Mobile IP package in Linux.

Hardware to be used in this lab assignment

Each student group needs the following hardware:

- One (1) Dell Latitude C640 notebook computer (*with a fully charged battery*)
- One (1) Xircom 802.11b wireless Ethernet adapter

The following hardware will be provided by the GTA:

- Two (2) Intel 802.11b access points
- One (1) Dell Latitude C640 notebook computer equipped with 802.11b card

Software to be used in this lab assignment

- OS: Red Hat Linux 7.3
- Tools: Dynamics mobile IP package, Ethereal Network Analyzer, iperf

Part II – Pre-lab Assignment

This portion of the assignment ***must*** be completed ***prior*** to the in-class lab session.

Reading assignment

- Read the tutorial by Charles E. Perkins, "Mobile Networking through Mobile IP". Available at http://www.computer.org/internet/v2n1/perkins.htm.
- Browse the following online resources for more information on mobile IP:

  IETF Mobile IP Working Group (http://www.ietf.org/html.charters/mobileip-charter.html)

  Dynamics Mobile IP package (http://www.cs.hut.fi/Research/Dynamics/index.html)

Tasks

The following steps configure the Dynamics Mobile IP package for the in-class lab experiment. Complete these tasks ***before*** the in-class lab session.

- The Dynamics Mobile IP package is pre-installed on the Linux system. The executable files are located in the directory **/usr/local/sbin/**, and the configuration files are located in the directory **/usr/local/etc/**. The following table lists the major components of the Dynamics Mobile IP package and their corresponding daemon executables, configuration files and debugging tools.

Component	*Executable*	*Configuration File*	*Debug Tool*
Home Agent	/usr/local/sbin/dynhad	/usr/local/etc/dynhad.conf	dynha_tool
Foreign Agent	/usr/local/sbin/dynfad	/usr/local/etc/dynfad.conf	dynfa_tool
Mobile Node	/usr/local/sbin/dynmnd	/usr/local/etc/dynmnd.conf	dynmn_tool

  The manuals provide more information on using the Dynamics Mobile IP package. Use the **man** command to view the manual for **dynhad**, **dynfad** and **dynmnd** (e.g., *man dynhad*).

- Use the **vi** or **pico** text editor to open the configuration file for the **home agent**. In the configuration file, all comment lines begin with the '#' character. In most cases, the configuration keys are followed by their values. Note that the comments provide useful information on the settings. You can refer to the manual pages for the configuration file (e.g., *man dynhad.conf*) for additional information. Make modifications to the configuration file according to the procedures below. ***Save backup copies of these files before making changes.***

  1) Locate the INTERFACES_BEGIN/INTERFACES_END section. Delete the entry for interface **eth0**, and edit the entry for interface **eth1** as follows.

```
INTERFACES_BEGIN
# interface     ha_disc     agentadv     interval     force_IP_addr
eth1            1           1            10
INTERFACES_END
```

  The wireless interface **eth1** will be connected to the wireless local network. The above settings enable home agent discovery and advertisement in the home network through the **eth1** interface.

  2) Locate the AUTHORIZEDLIST_BEGIN/AUTHORIZEDLIST_END section, then edit the entry for Security Parameter Index (SPI) 1000 as follows.

```
AUTHORIZEDLIST_BEGIN
1000            192.168.100.0/24
AUTHORIZEDLIST_END
```

  The home network 192.168.100.0/24 uses SPI 1000. The shared keys and other settings for SPI 1000 are defined in the SECURITY_BEGIN/SECURITY_END section. The mobile node needs to know the shared key when trying to connect to the home agent. Security can also be enabled on the foreign agents in the Dynamics package, but this feature will not be used in this experiment.

  3) All other settings in the configuration file should ***not*** be changed.

- Open the configuration file for the **foreign agent** and make the following modifications.

  1) Locate the INTERFACES_BEGIN/INTERFACES_END section. Delete the entry for interface **eth0**, and edit the entries for interface **eth1** as follows.

```
INTERFACES_BEGIN
# interface     type        agentadv    interval    force_IP_addr
eth1            1           1           20
INTERFACES_END
```

  The wireless interface **eth1** will be connected to the foreign network and used to send advertisements for the mobile nodes.

  2) Change the value of key "**HighestFAIPAddress**" to 192.168.200.101. The Dynamics mobile IP package supports a hierarchy tree of foreign agents. In this experiment, we will use only the highest foreign agent for all mobile nodes.

  3) Change the value of key "**UpperFAIPAddress**" to 192.168.200.101. Since it will be the only foreign agent in the hierarchy tree, the UpperFAIPAddress value refers to itself.

  4) All other settings in the configuration file should ***not*** be changed.

- Open the configuration file for the **mobile node** and make the following modifications:

  1) Change the value of key "**MNHomeIPAddress**" to 192.168.100.*X*, where *X* equals 150 plus your group number. This is the fixed home network IP address assigned to the mobile node.

  2) Change the value of key "**HAIPAddress**" to 192.168.100.101, which is the IP address of the home agent.

  3) Change the value of key "**HomeNetPrefix**" to 192.168.100.0/24.

  4) All other settings in the configuration file should ***not*** be changed.

- Generate the RSA key configuration file **/etc/dynfad.key** using the following command. This key file is used by the foreign agent daemon.

```
# rsakeygen  /etc/dynfad.key 512
```

Part III – In-class Lab Assignment

Overview

The network scenario used in this lab is shown in Figure 1. The home network (192.168.100.0/24) and the foreign network (192.168.200.0/24) are two separate IP networks that are connected via an IP router. The home and foreign networks could be separated by multiple intermediate networks, but we omit those networks for this experiment. When a mobile node travels to a foreign network without changing the network configuration, in normal situations, it will not able to continue communicating with other hosts in the home network and other hosts will not be able to send packets to the mobile node using its normal home address. Mobile IP solves this problem by setting up home agents and foreign agents to forward packets between the mobile node in the foreign network and the correspondent nodes in the home network, thus providing a mobile networking environment.

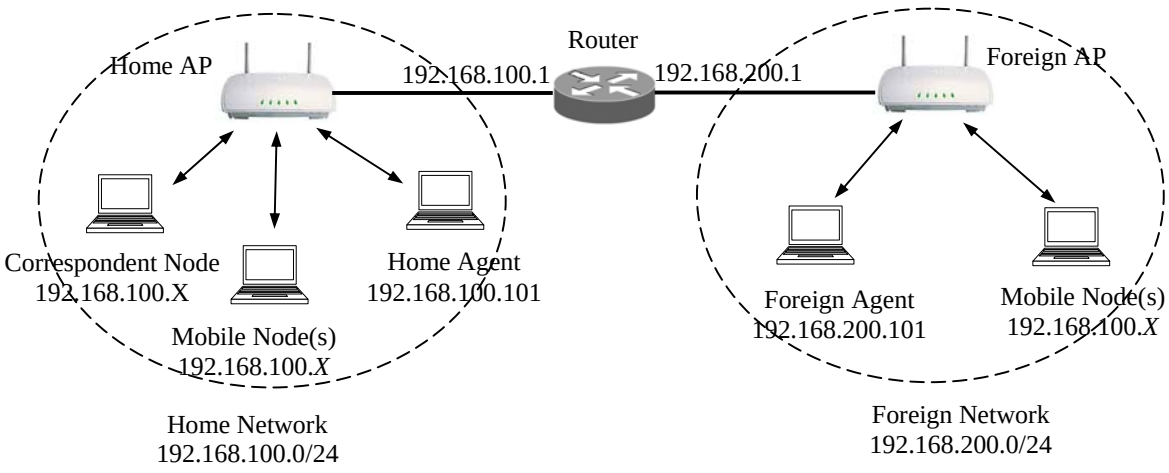

Figure 1. Network scenario for mobile IP

All student groups are expected to perform the following tasks together. Cooperation is important to this lab experiment. The GTA will assign one group to setup the home agent and another group to setup the foreign agent. Other groups will form teams of two groups each. Every team will setup a correspondent node and a mobile node. The GTA is responsible for setting up the access points and the router.

If time allows, it is recommended each that group go through all the procedures for the home agent, foreign agent, and mobile nodes.

Home Agent Setup and Procedures

1. On the notebook computer that runs the ***home agent daemon***, log into Linux as user **root**. Insert the 802.11b card and setup the wireless interface **eth1** as shown below.

```
# iwconfig  eth1  mode managed  essid  HOME key ABCDEF4984 txpower 1mW
# ifconfig  eth1 192.168.100.101  netmask 255.255.255.0
# ping 192.168.100.1
```

2. Start the Ethereal network analyzer and begin tracing packets on the wireless interface **eth1**. In the "Capture options" dialog, remember to **disable** the following options.
   - ✧ Capture packets in promiscuous mode (the driver does not support this mode well)
   - ✧ Enable network name resolution (to load the trace file faster)

   Hint: Enable the "Update list of packets in real time" option to allow real-time analysis.

3. Setup the default route, enable IP forwarding, and then start the home agent daemon as shown below. The IP forwarding option must be enabled for the home agent to work properly.

```
# route add default gw 192.168.100.1
# echo 1 > /proc/sys/net/ipv4/ip_forward
# dynhad --fg --debug
```

Open another command console and use the *dynha_tool* utility to monitor the home agent daemon. The available commands in the *dynha_tool* utility include *status*, *list*, *show*, etc. Use "*help <command>*" to get more information.

```
# dynha_tool
> status
> list
> show <MobileNodeAddress>
```

4. Wait until the foreign agent has started and some mobile nodes have moved to the foreign network, then stop tracing with Ethereal. Identify and examine the following messages from the packet trace.
    1) Home agent advertisement message sent to the home network. Record the care-of-address specified in the advertisement.
    2) Registration request message from mobile nodes ***in the home network*** and the corresponding registration reply message. Record the care-of-address specified in the registration request message. Record the home address and home agent address in these messages.
    3) Registration request message from mobile nodes ***roaming in the foreign network*** and the corresponding registration reply message. Record the care-of-address specified in the registration request message. Record the home address and home agent address in these messages.
    4) ARP request and reply message for mobile nodes roaming in the foreign network. Which interface's hardware address was returned for the mobile nodes?
    5) Examine some IP-within-IP packets to calculate the overhead of tunneling in Mobile IP.
    6) Have the GTA verify these results.

    Hint: You may want to start and stop tracing with Ethereal in coordination with other groups to finish these steps.
5. Use the *iptunnel* command to check the IP-within-IP tunnel configurations. Use the *route* command to verify the routing table entries for the mobile nodes roaming in the foreign network. Use the *traceroute* command to check the route to the mobile nodes in the foreign network.

Foreign Agent Setup and Procedures

1. On the notebook computer that runs the ***foreign agent daemon***, log into Linux as user **root**. Insert the 802.11b card and setup the wireless interface **eth1** using the following procedures.

```
# iwconfig eth1  mode managed  essid  FOREIGN key ABCDEF4984 txpower 1mW
# ifconfig eth1 192.168.200.101  netmask 255.255.255.0
# ping 192.168.200.1
```

2. Start the Ethereal Network Analyzer and begin tracing packets on the wireless interface **eth1**. In the "Capture options" dialog, remember to **disable** the following options.
    - ✧ Capture packets in promiscuous mode (the driver does not support this mode well)
    - ✧ Enable network name resolution (to load the trace file faster)

    Hint: Enable the "Update list of packets in real time" option to allow real-time analysis.

3. Set up the default route, enable IP forwarding, and then start the foreign agent daemon as shown below. The IP forwarding option must be enabled for the foreign agent to work properly.

```
# route  add default  gw 192.168.200.1
# echo 1 > /proc/sys/net/ipv4/ip_forward
# dynfad --fg  --debug
```

   Open another command console and use the *dynfa_tool* utility to monitor the foreign agent daemon. The available commands in the *dynfa_tool* utility include *status*, *list*, *show*, etc. Use the "*help <command>"* to get more information.

```
# dynfa_tool
> status
> list
> show <MobileNodeAddress>
```

4. Wait until the home agent has started and some mobile nodes have moved to the foreign network, then stop tracing with Ethereal. Identify and examine the following messages from the packet trace.
   1) Foreign agent advertisement sent to the foreign network. Record the care-of-address specified in the advertisement.
   2) Registration request messages from the mobile nodes and the corresponding registration reply messages. Record the care-of-address specified in the registration request message. Record the home address and the home agent address in these messages.
   3) Examine some IP-within-IP packets to calculate the overhead of tunneling in Mobile IP.
   4) Have the GTA verify these results.

   Hint: You may want to start and stop tracing with Ethereal several times in coordination with other groups to finished these procedures.

5. Use the *iptunnel* command to check the IP-within-IP tunnels.

Mobile/Correspondent Node Setup and Procedures

1. Do either step (a) or (b).

   (a) On the notebook computers to be used as the ***correspondent node***, log into Linux as user **root**. Insert the 802.11b card and setup the wireless interface **eth1** as shown below (### should be replaced by **200** plus your group number).

```
# iwconfig  eth1  mode managed  essid HOME  key ABCDEF4984  txpower 1mW
# ifconfig eth1 192.168.100.###  netmask 255.255.255.0
# ping 192.168.100.1
```

   (b) On the notebook computer to be used as the ***mobile node***, set up the wireless interface **eth1** and connect the mobile node to the home network (### represents **150** plus your group number).

```
# iwconfig eth1  mode managed  essid HOME  key ABCDEF4984 txpower 1mW
# ifconfig eth1 192.168.100.###  netmask 255.255.255.0
# ping 192.168.100.1
```

2. Use the *ping* command to measure the delay between the mobile node and the correspondent node. Use the *iperf* command to measure the UDP throughput between the mobile node and the correspondent node. Run the *iperf* server on the mobile node and the *iperf* client on the correspondent node.

3. On the notebook computer that is serving as the ***mobile node***, start Ethereal Network Analyzer and begin tracing on the wireless interface **eth1**. In the "Capture options" dialog, remember to **disable** the following options.

   - ✧ Capture packets in promiscuous mode (the driver does not support this mode well)
   - ✧ Enable network name resolution (to load the trace file faster)

   Hint: Enable the "Update list of packets in real time" option to allow real-time analysis.

4. Wait until other groups start the home agent and foreign agent. Then, on the notebook computer serving as the ***mobile node***, start the mobile node daemon as follows.

```
# dynmnd --fg   --debug
```

5. Note the debug messages printed on the console. After the home agent finishes the registration process, stop tracing with Ethereal to identify and examine the following messages.

   1) Home agent advertisement message sent to the home network. Record the care-of-address specified in the advertisement.

   2) Registration request message to the home agent and the corresponding registration reply message. Record the care-of-address specified in the registration request message. Record the home address and home agent address in these messages.

6. On the ***mobile node***, start tracing on the wireless interface **eth1** with the Ethereal network analyzer. Then, connect the mobile node to the access point on the foreign network as follows.

```
# iwconfig eth1  mode managed  essid FOREIGN key ABCDEF4984
```

   This can be viewed as moving the mobile node from its home network to the foreign network. Note that we do not change the IP configuration on the mobile node. In more realistic scenario, the client could automatically attach to an access point with the same ESSID (or by accepting any ESSID), but on a different IP network.

   The mobile nodes in the foreign network and the correspondent nodes in the home network should be able to ping each other if the mobile node daemon successfully registers with the home agent.

7. Open another command console and use the *dynmn_tool* utility to monitor the mobile node daemon. The available commands in the *dynmn_tool* utility include help, list, show, etc.

```
# dynmn_tool
> status
> list
> show <ForeignAgentAddress>
```

8. Stop tracing with Ethereal, identify and examine the following messages:

   1) Foreign agent advertisement sent to the foreign network. Record the care-of-address specified in the advertisement.

   2) Registration request messages to the home agent and the corresponding registration reply messages. Record the care-of-address specified in the registration request message. Record the home address and the home agent address in these messages.

3) Have the GTA verify these results.

9. Use the *ping* command to measure the delay between the mobile node and the correspondent node. Use the *iperf* command to measure the UDP throughput between the mobile node and the correspondent node. Run the *iperf* server on the mobile node and the *iperf* client on the correspondent node. Compare the throughput results with the previous measurement when both the correspondent node and the mobile node were on the same network.
10. On the ***mobile node***, use the *traceroute* command to inspect the routing from the mobile node to the correspondent node and to other mobile nodes roaming in the foreign network. On the ***correspondent node***, use the *traceroute* command to inspect the routing from the correspondent node to the mobile node.