Virginia Tech ■ ECE/CS 4570: Wireless Networks and Mobile Systems ■ Spring 2006

In-class Laboratory Exercise 11 (L11)

Part I – Objectives and Laboratory Materials

Objectives

The objectives of this laboratory are to:

- ❑ Familiarize you with the operation of Mobile IP; and
- ❑ Investigate the delay, throughput, and overhead associated with Mobile IP.

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

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

Hardware Used in this Laboratory Assignment

Each student group needs the following hardware.

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

The following hardware will be provided by the GTA.

- ❑ Two Intel IEEE 802.11b access points
- ❑ One Dell Latitude C640 notebook computer equipped with an IEEE 802.11b card

Software Used in this Laboratory Assignment

We will use the following software.

- ❑ Operating System: Red Hat Linux 9
- ❑ Tools: Dynamics Mobile IP package, Ethereal network analyzer, iperf

Part II – Pre-laboratory Assignment

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

Reading Assignment

- ❑ Read the tutorial: C. E. Perkins, "Mobile Networking through Mobile IP," *Internet Computing*, vol. 2, no. 1, pp. 58-69, January/February 1998. This tutorial is available at the class web site and through IEEE Xplore at http://ieeexplore.ieee.org/search/wrapper.jsp?arnumber=656077.
- ❑ Browse the following online resources for more information on Mobile IP.

  i) IETF Mobile IP Working Group (http://www.ietf.org/html.charters/mip4-charter.html)

  ii) Dynamics Mobile IP package (http://dynamics.sourceforge.net/)

Other Tasks

The following steps are required to configure the Dynamics Mobile IP package to prepare for the in-class laboratory experiment. ***You must complete these tasks <u>before</u> the in-class laboratory session.***

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

Table I. Dynamics Mobile IP Components

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*).

- ***Save backup copies of the configuration files for the home agent, foreign agent, and mobile node.*** You will change these as instructed below. Make a backup copy of each before making the changes.

- Use the **vi**, **kedit**, or similar 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. ***Be sure to save a backup copy of the configuration file before making changes.***

1) Locate the INTERFACES_BEGIN/INTERFACES_END section. Delete the entry for interface **eth0**. 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. 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) Do ***not*** change any other settings in the home agent configuration file.

- ❑ Open the configuration file for the **foreign agent** and make the following modifications. ***Be sure to save a backup copy of the configuration file before making changes.***

  1) Locate the INTERFACES_BEGIN/INTERFACES_END section. Delete the entry for interface **eth0**. 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) Do ***not*** change any other settings in the foreign agent configuration file.

- ❑ Open the configuration file for the mobile node and make the following modifications. ***Be sure to save a backup copy of the configuration file before making changes.***

  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) Do ***not*** change any other settings in the configuration file.

- ❑ 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 Laboratory 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 network and foreign network 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.

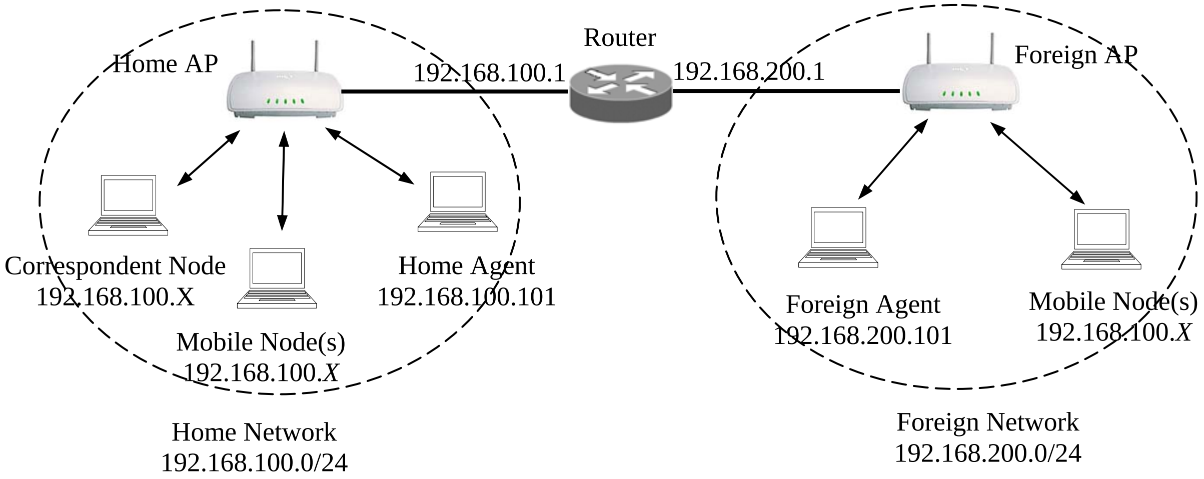

Figure 1. Network configuration for Mobile IP experiment.

All student groups are expected to perform the following tasks together. Cooperation is critical to the success of this laboratory assignment. The GTA will assign one group to act as the home agent and another group to act as the foreign agent. Other groups will form teams of two groups each. Every team will include 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 Test Procedures

Perform the following steps only on the notebook computer serving as the home agent. Procedures for the foreign agent, mobile nodes, and correspondent nodes are given in later sections.

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

```
# iwconfig  eth1  mode managed  essid  HOME key ABCDEF4570 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, be sure to **disable** the following options.

   - Capture packets in promiscuous mode (the driver does not properly support this mode)
   - 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 commands available in the *dynha_tool* utility include *status*, *list*, and *show*. Use “*help <command>*” to get more information about these and other commands.

```
# 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. Record information as requested in the form at the end of this document. ***Submit your results to the GTA for verification.***

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

    b) 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.

    c) 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.

    d) ARP request and reply message for mobile nodes roaming in the foreign network. Which interface's hardware address was returned for the mobile nodes?

    e) Examine some IP-within-IP (tunneled) packets to calculate the overhead of tunneling in Mobile IP.

    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 Test Procedures

Perform the following steps only on the notebook computer serving as the foreign agent.

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

```
# iwconfig eth1  mode managed  essid  FOREIGN key ABCDEF4570 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, be sure to **disable** the following options.

    - Capture packets in promiscuous mode (the driver does not properly support this mode)
    - 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*, and *show*. Use the "*help <command>*" to get more information about these and other commands.

```
# 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. Record information as requested in the form at the end of this document. ***Submit your results to the GTA for verification.***

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

   b) 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.

   c) Examine some IP-within-IP (tunneled) packets to calculate the overhead of tunneling in Mobile IP.

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

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

Mobile and Correspondent Node Setup and Test Procedures

Perform the following steps only on the notebook computers serving as either a mobile node or a correspondent node.

1. Do either step (a) for correspondent nodes or step (b) for mobile nodes.

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

```
# iwconfig  eth1  mode managed  essid HOME  key ABCDEF4570  txpower 1mW
# ifconfig eth1 192.168.100.xxx  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 (*yyy* represents **150** plus your group number).

```
# iwconfig eth1  mode managed  essid HOME  key ABCDEF4570 txpower 1mW
# ifconfig eth1 192.168.100.yyy  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 and begin tracing using the wireless interface **eth1**. In the "Capture options" dialog, be sure to **disable** the following options.

   - Capture packets in promiscuous mode (the driver does not properly support this mode)
   - 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. Record information as requested in the form at the end of this document. ***Submit your results to the GTA for verification.***

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

   b) 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 Ethereal. Then, connect the mobile node to the access point on the foreign network as follows.

   ```
   # iwconfig eth1  mode managed  essid FOREIGN key ABCDEF4570
   ```

   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 a 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*, and *show*. Use the "*help <command>*" to get more information about these and other commands.

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

8. Stop tracing with Ethereal, identify and examine the following messages. Record information as requested in the form at the end of this document. ***Submit your results to the GTA for verification.***

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

   b) 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.

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 another mobile node 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.

In-class Laboratory Results for L12

Group Members: ________________________________ ________________________________

For the Home Agent (see step 4 of the home agent setup and test procedures section):

a) Care-of-address in home agent advertisement message: ____________________

b) From home agent registration request and reply messages for a node in the *home* network:

Care-of-address: ____________________

Home address: ____________________

Home agent address: ____________________

c) From home agent registration request and reply messages for a node in the *foreign* network:

Care-of-address: ____________________

Home address: ____________________

Home agent address: ____________________

d) Interface's hardware address: ____________________

For the Foreign Agent (see step 4 of foreign agent setup and test procedures section)

a) Care-of-address in foreign advertisement message: ____________________

b) From foreign agent registration request and reply messages:

Care-of-address: ____________________

Home address: ____________________

Home agent address: ____________________

For the Mobile Nodes and Correspondent Nodes (see step 5 and step 8 of the mobile node and correspondent node setup and test procedures)

For registration with the home agent in the home network (see step 5):

a) Care-of-address in home agent advertisement message: ____________________

b) From home agent registration request and reply messages:

Care-of-address: ____________________

Home address: ____________________

Home agent address: ____________________

For registration with the home agent in the home network (see step 8):

a) Care-of-address in home agent advertisement message: ____________________

b) From home agent registration request and reply messages:

Care-of-address: ____________________

Home address: ____________________

Home agent address: ____________________