

MOBILE IPv4 – SIMULATION AND IMPLEMENTATION

Michal Skořepa

Doctoral Degree Programme(1), FEEC BUT
E-mail: michal.skorepa@phd.feec.vutbr.cz

Supervised by: Karol Molnár

E-mail: molnar@feec.vutbr.cz

ABSTRACT

The purpose of this paper is to show how mobility (in sense of utilizing MIPv4 protocol) can be simulated in simulation environment OPNET Modeler 14.0 and also practically implemented using Cisco network components. The first part of the paper briefly describes the principles of MIPv4 protocol. The second part shows the way of simulation of MIPv4 protocol in OPNET Modeler and provides results that illustrate the protocol's features. The final chapter shows the implementation of MIPv4 in real network consisting of Cisco network components.

1. INTRODUCTION

In these days users of information and communication services lay big stress on them to be mobile. It means that during the operation of their mobile devices they need to roam among various networks (with different network addresses) or access technologies. But roaming to a different network and getting a new IP address means that the running application needs to be restarted which is not really convenient. The MIPv4 protocol ensures that the mobile device keeps its IP address all the time so the application does not have to be restarted and roaming becomes for the user transparent.

2. MIPv4 – BASIC FACTS

Mobile IPv4 protocol is a layer 3 protocol and is independent on the physical technology. The architecture of the MIPv4 protocol basically consists of three entities – Mobile Node (MN), Home Agent (HA) and Foreign Agent (FA) [1], [2]. There is one extra node used in connection with MIPv4 protocol which does not implement this protocol – Correspondent Node (CN). It is a server or workstation that the MN communicates with. The basic topology is shown in Figure 1.

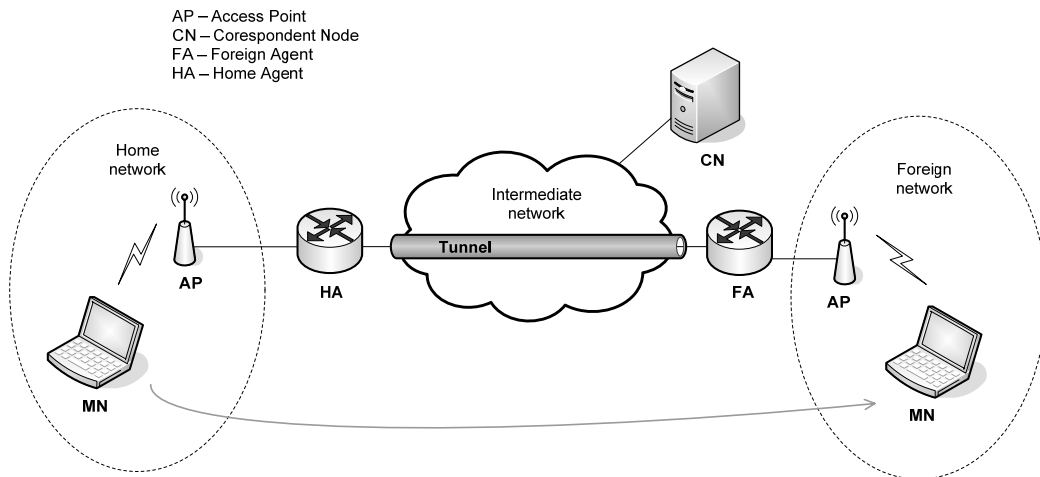


Figure 1: Network topology using MIPv4

In a nutshell the MIPv4 works as follows (detailed description [1], [2], [3] is not a goal of this paper). When the MN stays in its home network data are routed in standard way and the MIPv4 protocol does not apply. As soon as the MN roams to a foreign network (covered by FA), using MIPv4 it registers at the serving FA and its HA. After successful registration so called Care of Address (CoA) is assigned to MN. Usually the CoA is the address of FA. Then an IP tunnel between HA and FA is created. Because CN is not aware of MN's new location it keeps sending data to its home network. HA tunnels the data to FA (to MN's CoA) that delivers it to MN. In the opposite direction, data is routed directly from MN to CN unless reverse tunneling is required (e.g. because of firewall settings). While staying in the foreign network, the MN needs to re-register after a certain period. When a MN roams to another foreign network it re-registers using its new FA and a new IP tunnel is created. After MN returns to its home network it un-registers at the HA and the communication continues without using MIPv4.

3. MIPv4 IN OPNET MODELER 14.0

OPNET Modeler is a simulation environment that allows detailed simulation of computer networks of various kinds and complexity. Designing and testing the network before its realization is very convenient.

For simulating the MIPv4 protocol the following scenario has been created (Figure 2). It consist of eight wireless access points, one Ethernet router that interconnects them, three wireless workstations and two servers of which one is wireless and one is fixed. As a wireless technology the IEEE 802.11b has been used. Each access point serves to a different IP network. The three access points on the top of the figure have Home Agent functionality enabled whereas the rest of them are Foreign Agents. According to the colored marking, wireless workstation *MN_1* and wireless server *MN_server* belong to the network of access point *AP1_HA1*. Similarly *MN_2* belongs to network of *AP2_HA2* and *MN_3* to *AP3_HA3*.

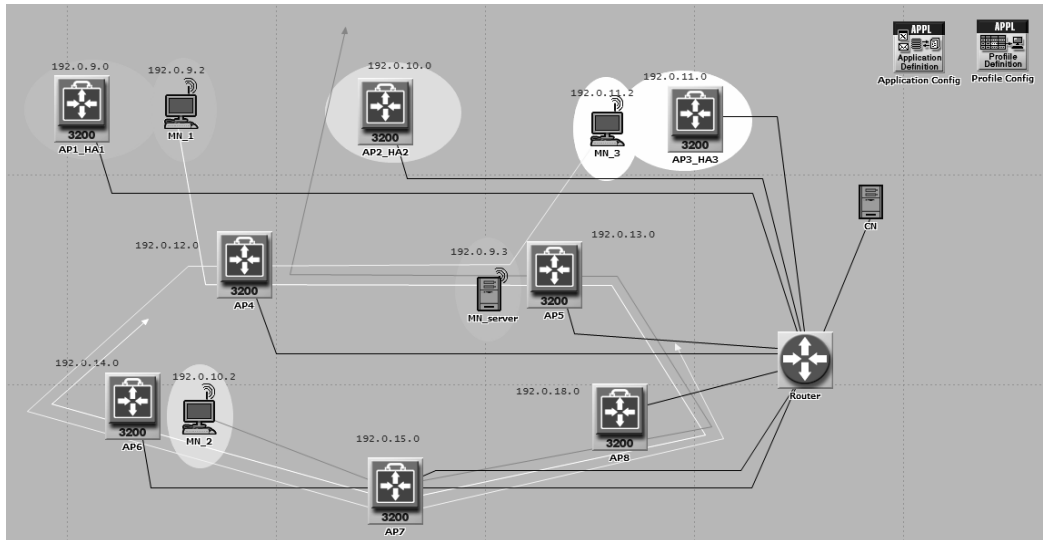


Figure 2: Scenario of MIPv4 simulation

The servers *MN_server* and *CN* work as FTP servers and in terms of MIPv4 they are Correspondent Nodes. The *MN_server* shows that Correspondent Node doesn't need to be just a fixed node in the network as it is usually described, but can also be mobile and working outside its home network.

During the simulation *MN_1* is accessing the FTP server at *MN_server*, the other two mobile nodes are accessing the FTP server at *CN*. The mobile nodes are also moving along defined trajectories with average speed around 7 km/h. After completing the simulation the following characteristics can be obtained (Figure 3).

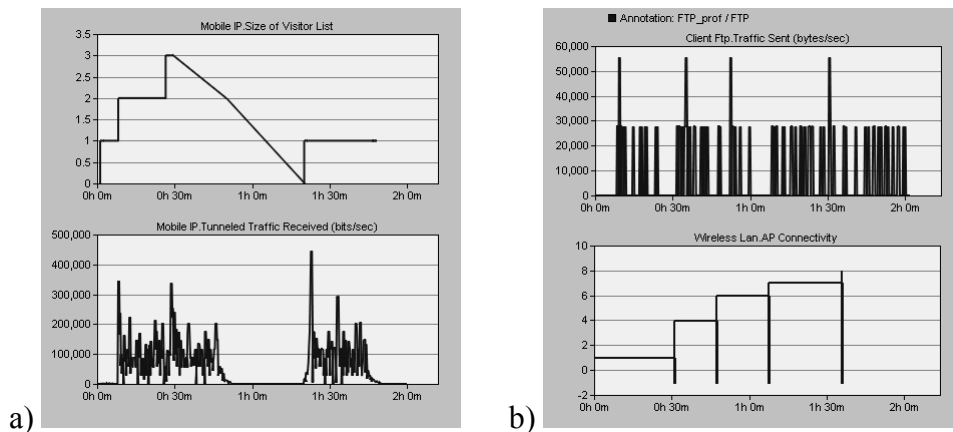


Figure 3: a) Characteristics of *AP4*, b) characteristics of *MN_1*

The graph on the top of Figure 3a) shows the size of binding table in *AP4* during the simulation. We can see that after about 30 minutes of simulation there are 3 mobile nodes hosting on *AP4*. After a while one of the mobile nodes leaves *AP4*'s network which can be seen as a decrease of the size of the binding table. Of course the decrease is not linear, it is just the way of OPNET interpretation. After about 50 minutes of simulation all mobile nodes leave *AP4* so the size binding table decreases to zero. This can be proved by the bottom part of Figure 3a) that shows tunneled traffic received by Foreign Agent at *AP4*. As long as there are mobile nodes connected to *AP4*, respectively to its Foreign Agent, there is

data tunneled to *AP4*. After all nodes leave this access point there is no more data to be tunneled here and the characteristics goes to zero.

In the Figure 3b) on the bottom we can see to which access points (according to their BSS identifiers; *AP1_HA1* \approx 1, *AP2_HA2* \approx 2, etc.) the mobile node *MN_1* connects during the simulation. On the top of Figure 3b) there is FTP traffic sent by *MN_1* to the FTP server. When compared to the AP connectivity on the bottom of the picture it is clear that the mobile node keeps communicating also after leaving its home network with BSS ID = 1.

In further research the dependency of MIPv4 on the network load will also be tested.

4. IMPLEMENTATION OF MIPv4

The mobile IPv4 protocol has been implemented in a laboratory on Cisco 1841 routers equipped with IOS software version 12.4(5b). The tested topology is in the Figure 4. So far the mobility support has been tested through the fixed interface (by plugging the Ethernet cable of MN to different routers), not in a wireless environment like in the simulation.

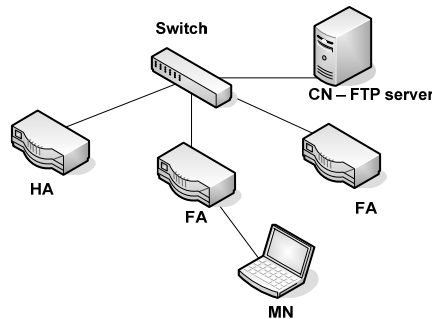



Figure 4: Laboratory topology for MIPv4

The tested topology consists of three Cisco 1841 routers, a switch that interconnects them and two computers. One of the computers works as a mobile node, the other one works as a correspondent node with running FTP server. Two of the routers work as Foreign Agents, one is Home Agent. The HA and FA functionality on the routers is enabled by entering appropriate IOS commands in the console [1]. For example, when configuring HA the router has to be set to use MIPv4 first (command: *router mobile*), then the HA functionality can be enabled (*ip mobile home-agent*). After that hosts belonging to HA network are specified (*ip mobile host [ip address] [interface]*) and their security associations are set (*ip mobile secure host [ip address] spi [spi] key hex [key] algorithm hmac-md5*). The MIPv4 functionality on the mobile node is enabled by a software client – Cisco Mobile Client (Figure 5a). The main parameters to be set in the client are home address (with subnet mask and default gateway), HA address and security association between MN and HA.

a) 

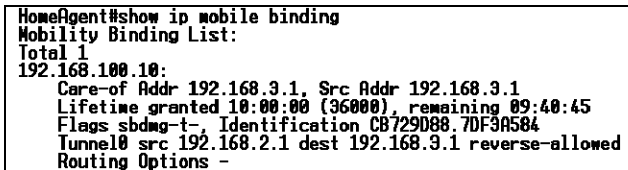
b) 

Figure 5: a) Cisco Mobile Client configuration, b) binding table in HA

After successful configuration of Home Agent, Foreign Agent and Mobile Node the Mobile Node can be connected to a foreign network. As described above in this paper the MN registers with FA and HA. The binding table of the HA in the tested network is shown in Figure 5b).

5. CONCLUSION

The performed simulation of MIPv4 protocol in OPNET Modeler and successful implementation of this protocol in real computer network are very important starting points for further research and development in the field of mobility. The simulation can be conveniently used for optimization of agents in wireless domain. It means for example optimizing the handover or IRDP parameters to get the highest performance as far as data loss, delay and jitter are concerned. This can be further used in the laboratory computer network for testing usability of Mobile IP protocol for real-time applications like VoIP.

The following research work will also be focused on implementing IP Mobility functions to IP Multimedia Subsystem (IMS). For this goal the simulation environment with perfectly running MIPv4 simulation is absolutely necessary.

ACKNOWLEDGEMENT

This paper was created in support of GAČR project 102/06/1569.

REFERENCES

- [1] RAAB, Stefan. Cisco: Mobilní IP technologie a aplikace, Grada, 2007, 299 s., ISBN: 978-80-247-1611-4
- [2] PRASAD A.R., PRASAD N.R.: 802.11 WLANs and IP Networking - Security, QoS, and mobility, Artech House, Boston, 2005, ISBN 1-58053-789-8
- [3] Jani Puttonen, Jyväskylä Polytechnic: Mobile IPv6 in heterogeneous environments
- [4] OPNET Technologies, Inc: OPNET Modeler Release 12 Product documentation, 2006