The Mobile-IP Testbed of the HP-OVUA

Stephen Heilbronner
MNM Team
heilbron@informatik.uni-muenchen.de

March 25, 1997

Abstract

Within the HP-OUA a special interest group on Mobility was founded in 1995. One of the main goals of this group was to set up a Mobile-IP testbed in order to examine and to do research on this new Internet protocol. This paper gives a short overview of Mobile-IP and the testbed set up locally in Munich as well as between the HP Labs and the Universities of Munich and Rennes. In order to be of practical relevance it also approaches real-world constraints as imposed by switched LANs, security-conscious configured routers as well as packet-filtering firewalls. After examining some of the difficulties involved during testing and the derived solutions it gives areas for future research. It is assumed that the reader has a basic understanding of the Internet Protocol Suite as well as ARP and Mobile-IP.

1 Introduction

During the HP-OUA general assembly in 1995 the topics Security, Mobility, and Mobile Computing Systems (among others) were considered important enough to have a special interest group within the HP-OUA that focus on these. After a workshop on "Security in Mobile Data Networks" the HP Labs Bristol, the University of Munich, and the University of Rennes decided to set up an Internet-wide testbed in order to examine issues related to the above mentioned topics.

The testbed consists of several HP-PCs running the UNIX-like operating system Linux. Besides the normal networking software on these machines implementations of the new Internet protocol *Mobile-IP* [Per96a] were installed. The HP-Mobile-IP software was developed by Manuel Rodriguez et al. at the HP Labs Bristol. The Linux implementation used at the universities' side is the one from the University of Singapore for Linux 1.3 kernels.

2 Testbed layout

The Internet wide view on the testbed is given in Figure 1. For the sake of completeness the University of Singapore's setup is also shown since they temporarely involved in testing, too.

The (expanded view of the) local testbed at the University of Munich is depicted in Figure 2.It mainly consists of a *Home Agent* **pchegering2**, a *Foreign Agent* **pchegering9**, a router **pchegering8** with interfaces to the departemental subnet 129.187.214.0 as well as the private Class-C-Network 192.168.214.0. Mobility is simulated by moving the *Mobile Node* **pchegering4** between these two subnetworks.

In order to do the Internet-wide interoperability testing the role of the router **pchegering8** was changed in order to turn it into a (simulated) Mobile Node that came from one of the foreign networks.

3 Problems and Solutions

This section describes the main difficulities experienced during testing and whether and how they were resolved. If difficulties are inherent to the definition of the Mobile-IP protocol or other causes that could not be influenced by the testbed partcipants this is stated, too.

3.1 Interoperability Issues and Software Design

Since two different implementations of Mobile-IP were used in the testbed (HP and Singapore) several problems related to software incompatibilities and interpretation of the Mobile-IP standard had to be resolved before testing could be continued. The incompatibilites led to failure in authentication and registration requests between Mobile Node, Foreign Agent and Home Agent. After that, several other incompatibilties were discovered, too, but all have been resolved.

The main difference between the HP and Singapore version is that the HP version runs in user space whereas the Singapore version runs in the kernel. The tradeoffs in terms of security, stability and performance in general are well known, however the main impact on the testbed was that the HP version by this design could not support bidirectional tunneling as described in Chapter 3.4.

3.2 ARP caching

ARP caching allows for the optimization of the mapping between IP and Ethernet adress. Since the Home Agent takes over the role of the Mobile Node when it leaves care should be taken that the corresponding fixed hosts on the local network do not keep the cached entry for the Mobile Node Ethernet adress for too long. In switched networks the Home Agent therefor has to make sure that the ARP caches of all corresponding fixed hosts are cleared as soon as it receives a registration from the Mobile Node while abroad. This is achieved by issuing an ARP request for the Mobile Node's IP adress with the Mobile Node's IP adress and the Home Agent's Ethernet adress as the source. Corresponding hosts usually then update their ARP cache. If not, communication with the Mobile Node will be impossible until the ARP cache entry is timed out.

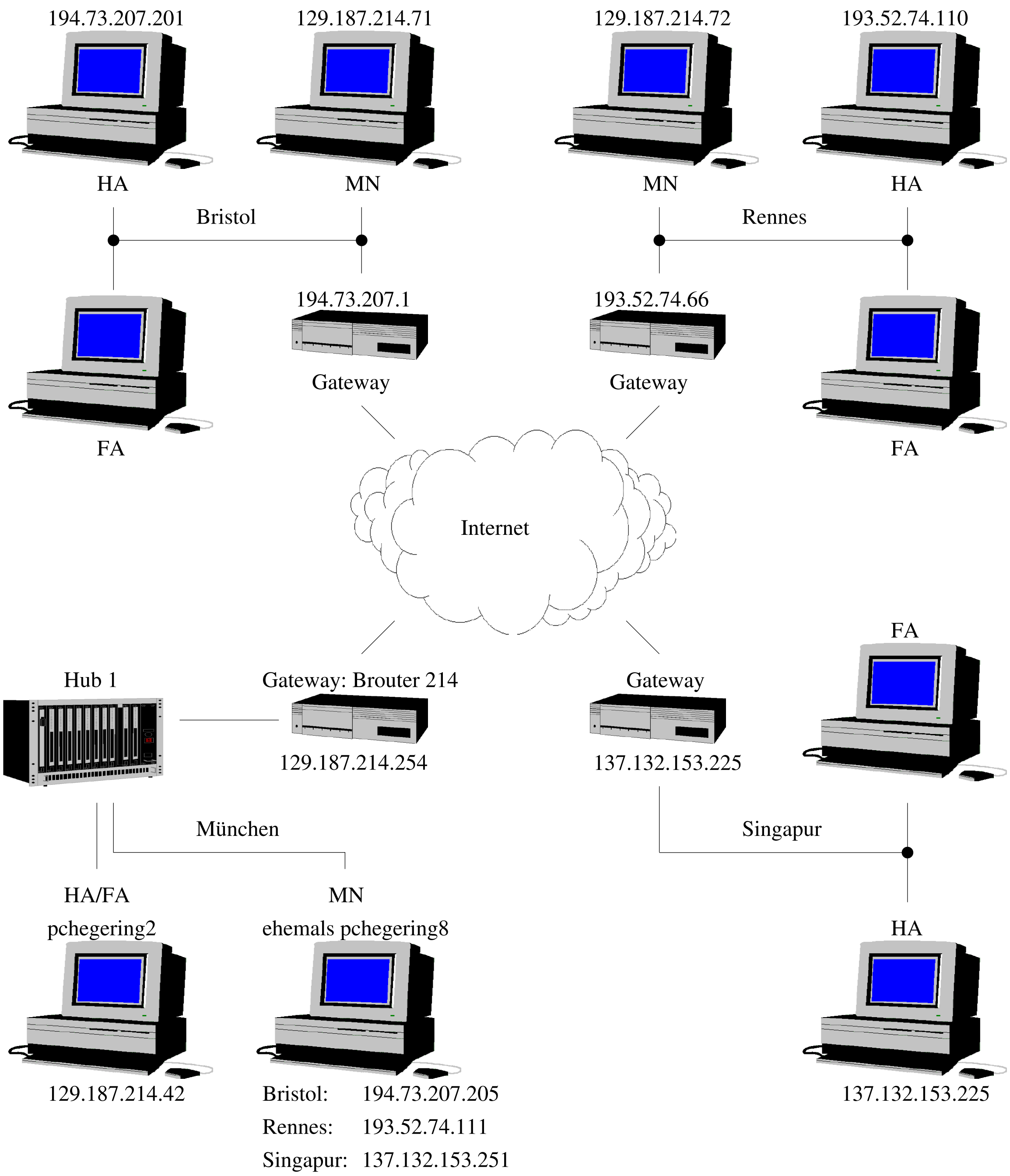

Figure 1: The Mobile-IP Testbed of the HP Labs and the Universities of Rennes and Munich (in German)

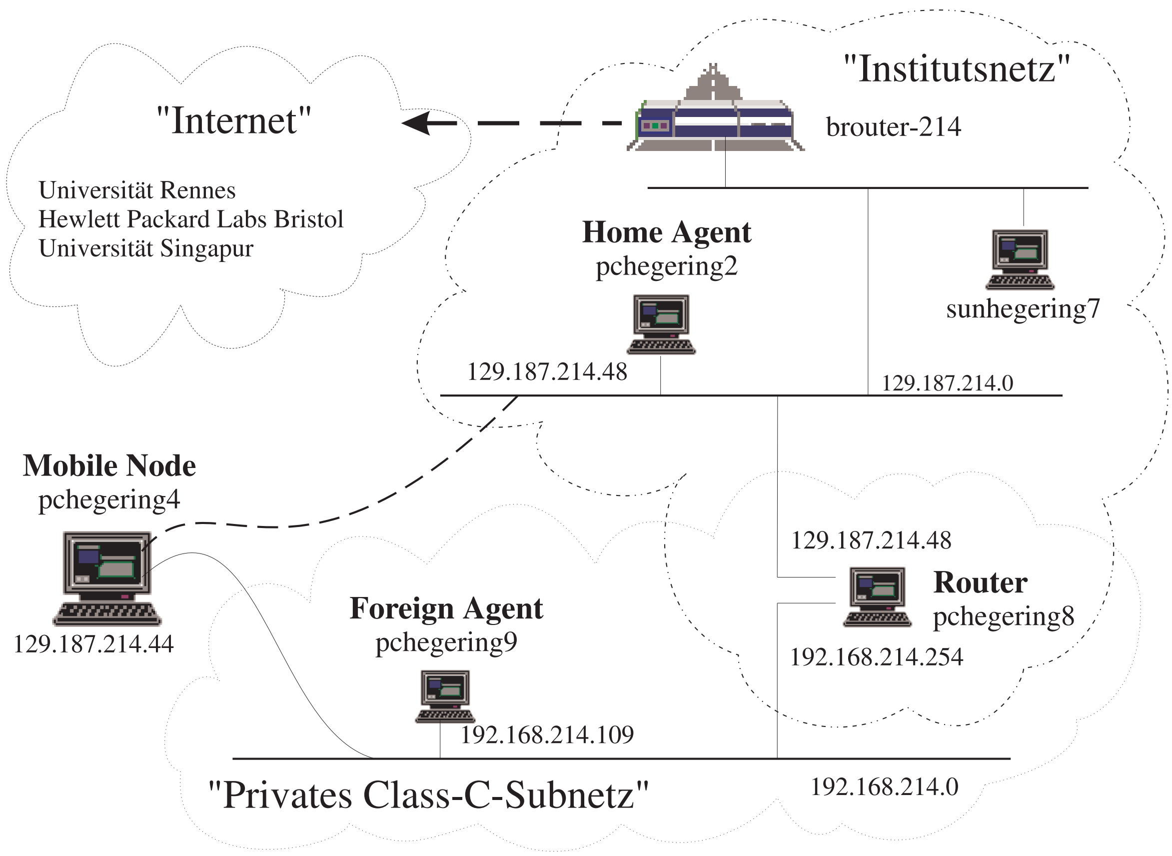

Figure 2: The Mobile-IP Testbed at the University of Munich (in German)

In classical Ethernet (broadcast) LANs the Ethernet hardware of the Home Agent could theoretically be reconfigured to also accept packets to the Mobile Node's Ethernet adress. It is unknown to the author whether such hardware and operating systems exist.

[Plu82]

3.3 Local Router Configuration

In order to prevent unintentionally misconfigured hosts, i.e. configured with an IP address not belonging to the local subnet, routers are sometimes configured not to answer ARP requests for their Ethernet adress from hosts with an IP adress not from the local subnet. This hinders the Mobile Node to directly communicate with other hosts outside the local subnet.

This obstacle can be circumvented by configuring the Foreign Agent host rather than the actual router as a gateway on the Mobile Node.

According to Manuel Rodriguez there is another reason why Foreign Agents must not be implemented on the routers. If this rule is not obeyed the Mobile Node obtains an undesired route optimization when it communicates with the local network. But when the Mobile Node moves away from that network, local hosts are not able to communicate with the mobile node, because the Foreign Agent/router thinks the Mobile Node is on that network. This occurs until the Foreign Agent realises the Mobile Node is not there because it receives no more (periodic) registration requests.

3.4 Packet Filtering Firewalls

Internet router security guidelines recommend not to forward any IP packets out of an Autonomous System (iėȧ local network) if they have a source address not belonging to the Autonomous System. Since Mobile Nodes emit packets with their home adress as source adress this packets will be dropped leaving the Autonomous System. This keeps them from communicating with any Internet host not in the network they are visiting.

To circumvent this obstacle *bidirectional tunneling* is necessary, in which case the packet to be emitted will be first tunneled back to the Home Agent before being "let out" on the Internet. Bidirectional tunneling was not foreseen in the original Mobile-IP standard, but has since been defined by an Internet Draft. It is foreseeible that bidirectional tunneling is absolutely necessary if Mobile-IP is to be deployed successfully. The HP implementation does not yet support it which kept interoperability testing from succeeding with Bristol beyond simple registration.

Bidirectional tunneling has enormous tradeoffs in terms of security and performance. Security holes developing due to misconfigured tunnels or insecure tunneling methods could let attackers access the Internal network. Bitunneling therefor needs to be used only if a Secure-IP infrastructure [Atk95] is in place. This is one of the issues mentioned in chapter 4 (Conclusions).

3.5 Disruption of TCP connections

Due to security considerations (time windows for IP spoofing) it seems arguable whether TCP connections are intended to be kept alive while the Mobile Node is roaming. However, the disappearing of a Mobile Node from a subnet cannot be seem from the corresponding fixed host anyway, a teardown of the connection only makes sense if either the Mobile Node or the present Home or Foreign Agent perform it. Since this action cannot be guaranteed to happen within a reasonably short time frame, TCP connections might be kept alive during roaming anyway.

In the first versions of the Singapore Mobile-IP stack this was not supported. However, the current version (1.2) handles roaming transparently as it is expected by most users.

4 Conclusions

The testbed is continued to be used within the research and teaching at the University of Munich. Examples of issues being examined consist of:

- Configuration management tasks for a Mobile-IP infrastructure and their support by standardized protocols such as DHCP [Dro93]
- Examination of diverse security protocols such as IPsec, SSL and others
- Research on the effects and security impacts inflicted by the use of tunneling protocols [Per96b, Per96c]
- Research on the Next Generation Internet Protocol IPv6 [DH96] and related protocols. Special focus on the management of migration involving renumbering and migration issues

In general we want to focus on the management issues evolving from the use of the above mentioned protocols. Most interesting areas consist of configuration, accounting, and security. The importance of performance and fault management stills seems a little unclear. Our impression is that these can only be tackled if the problems in the areas mentioned before are solved.

This work would not have been possible without the strong support and the efforts from the Mobile-IP development team at the University of Singapore, namely Li Yunzhou and Jiang Ming Liang. Students and employees at both Universities also contributed in the setup and carrying out the testing, among them Thomas Lankes, Robert Hoffmann, Thomas Lopatic, Sylvain Gombault, and Stephanie Ginguenes. Manuel Rodriguez of the HP Labs was very helpful when interoperability issues had to be resolved. The work would not have been possible without the HP-OUA donations.

References

[Atk95] R. Atkinson. RFC 1825: Security architecture for the Internet Protocol. Technical report, IAB, August 1995.

[DH96] S. Deering and R. Hinden. RFC 1883: Internet protocol, version 6 (IPv6) specification. Technical report, IAB, January 1996.

[Dro93] R. Droms. RFC 1541: Dynamic host configuration protocol. Technical report, IAB, October 1993.

[Per96a] C. Perkins. RFC 2002: IP mobility support. Technical report, IAB, October 1996.

[Per96b] C. Perkins. RFC 2003: IP encapsulation within IP. Technical report, IAB, October 1996.

[Per96c] C. Perkins. RFC 2004: Minimal encapsulation within IP. Technical report, IAB, October 1996.

[Plu82] D. Plummer. RFC 826: Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit ethernet address for transmission on Ethernet hardware. Technical report, IAB, November 1982.