Project P912-PF

Security for mobility in IP

Deliverable 1

Security requirements for the introduction of mobility to IP

Suggested readers:

PNO security specialists, service solution designers, developers, standards bodies

For full publication

October 1999

EURESCOM PARTICIPANTS in Project P912-PF are:

- France Télécom
- Deutsche Telekom AG
- BT
- Telefónica S.A.
- Telenor AS

This document contains material which is the copyright of certain EURESCOM PARTICIPANTS, and may not be reproduced or copied without permission.

All PARTICIPANTS have agreed to full publication of this document.

The commercial use of any information contained in this document may require a license from the proprietor of that information.

Neither the PARTICIPANTS nor EURESCOM warrant that the information contained in the report is capable of use, or that use of the information is free from risk, and accept no liability for loss or damage suffered by any person using this information.

This document has been approved by EURESCOM Board of Governors for distribution to all EURESCOM Shareholders.

Preface

(Prepared by the EURESCOM Permanent Staff)

The Project investigates existing standards in the area of security protocols and IP mobility protocols. It analyses IPSec security protocols required for mobility and conducts a threat analysis related to the addition of mobility facilities in IP and identifies and evaluates the risks. The main objectives are to push vendors to develop more flexible and open systems and to define and provide security guidelines to PNOs for the introduction of mobility facilities on the Internet and the introduction of enhanced security policies.

The Project started in January 1999 and will end December 1999. It is a partially funded Project with an overall budget of 30 MM. The Participants in the Project are BT, DT, FT, NT and TE. Mr. Thierry Baritaud from FT leads the Project.

This is the first of two planned Deliverables of the Project and is titled: "Security requirements for the introduction of mobility to IP". The other Deliverable, D2 is titled: "Security guidelines for the introduction of mobility facilites on Internet.

This Deliverable contians an investigation of protocols for mobility management in both IPv6 and IPv4 and of security protocols (IPSec) required for mobility, as well as the identification of general security objectives for the introduction of IP mobility services. Furthermore it provides mobility scenarios and a threat analysis related to the addition of mobility facilities to IP. Risks for each threat are identified and evaluated. Finally if identifies security requirements for mobility.

 © 1999 EURESCOM Participants in Project P912-PF

Executive Summary

Internet development, and the increasing number of intranets combined with the multiplication of mobile equipment integrating the IP protocol suite creates for users the need for Internet mobility. This Internet mobility will be in line with the development of cordless communications and the development of personal mobility services. The expansion of mobility facilities on the Internet shall take into account security features and shall integrate security mechanisms at an early stage of development.

In light of this situation, the work undertaken within this project is to define requirements and security guidelines for PNOs for the introduction of mobility facilities to the Internet and for the enhancement of security policies. Readers who are unfamiliar with the basic operation of IP mobility would be well advised to consult an introduction to the subject, such as James Solomon's 'Mobile IP: The Internet Unplugged' (Prentice Hall, 1998), or Charles Perkins' 'Mobile IP: Design Principles and Practices' (Addison-Wesley, 1998). This document presents the results achieved as follows :

- Investigation of protocols for mobility management in both IPv6 and IPv4 and of security protocols (IPSec) required for mobility.
- Identification of general security objectives for the introduction of IP mobility services.
- Mobility scenarios and threat analysis related to the addition of mobility facilities to IP.
- Identification and evaluation of risks for each threat.
- Identification of security requirements for mobility.

General and specific security statements are identified for security policy and security objectives as selected by PNOs. These statements relate to security objectives for PNOs and for users, specific security objectives and management related security objectives.

A list of scenarios for two basic configurations is provided: static mobility (from a wired network to another wired network, and performed without repetitive movements between two or more networks) and dynamic mobility (which includes rapid movement over wireless connections). All scenarios are investigated within IPv4 and IPv6 environments and a detailed threat analysis is performed.

The likelihood of threats is evaluated and a risk assessment is provided for each threat in both IPv4 and IPv6 environments, on the basis of criteria defined within the project.

Seven classes of security requirements are identified and a list of security requirements is provided for each class. Finally, section 6 summarises results obtained during phase 1. These results are intended as input for the second phase of the project, where the main work assignments will be on investigation of security measures for selected threats, on definition of security services and guidelines, and for improvement of security policy for PNOs. These will be presented within the final deliverable "Security guidelines for introduction of mobility facilities to the Internet" to be delivered at the end of this project.

 © 1999 EURESCOM Participants in Project P912-PF

List of Authors

Thierry Baritaud and Olivier Charles (France Télécom)

Carlos Leon (Telefonica)

Matthew Ford (BT)

Henning Wright Hansen (Telenor)

Hartmut Brandt, Petia Todorova and Peter Hofmann (Deutsche Telekom)

Table of Contents

Preface i

Executive Summary iii

List of Authors v

Table of Contents vi

Abbreviations viii

Definitions ix

1 Introduction 1

2 Security policy and objectives for IP mobility 3
- 2.1 Introduction 3
  - 2.1.1 Solution flexibility 3
  - 2.1.2 Overview 4
- 2.2 Security policy 4
- 2.3 Security objectives 5
  - 2.3.1 How we selected security objectives 5
  - 2.3.2 General security objectives 5
  - 2.3.3 Specific security objectives 6
  - 2.3.4 Security management objectives 7

3 Threat identification for different mobility scenarios 9
- 3.1 Mobility scenarios 9
  - 3.1.1 Goal and structure of mobility scenarios 9
  - 3.1.2 Actors influencing mobility scenarios 9
  - 3.1.3 Description of the basic network configuration for mobility 10
- 3.2 Scenario analysis 12
- 3.3 Threats 12
  - 3.3.1 IP version features influencing mobility related threats 13
  - 3.3.2 Loss of confidentiality/Session stealing/Spoofing of the mobile node 13
  - 3.3.3 Loss of confidentiality/Session stealing/Spoofing of the foreign-agent 14
  - 3.3.4 Loss of confidentiality/Session stealing/Spoofing of the home-agent 14
  - 3.3.5 Loss of confidentiality/Session stealing/Spoofing of other hosts on the foreign network 14
  - 3.3.6 Loss of security features provided by the home network 14
  - 3.3.7 DoS/Flooding of the mobile node 14
  - 3.3.8 DoS/Flooding of the home agent 14
  - 3.3.9 DoS/Flooding of the foreign agent (IPv4 environment) 14
  - 3.3.10 DoS/Flooding of the correspondent (IPv6 environment) 14
  - 3.3.11 Tracking of mobile node 15

4 Risk assessment and evaluation of the likelihood of threats 17
- 4.1 Introduction to risk assessment 17
- 4.2 List of criteria 17
- 4.3 Levels of risk 17
- 4.4 Threat notation 18

5 Security requirements for mobility 19

 © 1999 EURESCOM Participants in Project P912-PF

5.1 Introduction 19
5.2 Security requirements identification 19
5.3 Security requirements 19
5.3.1 Confidentiality 19
5.3.2 Integrity 20
5.3.3 Authentication 20
5.3.4 Availability 21
5.3.5 Authorised access 21
5.3.6 Accountability 21
5.3.7 Assurance 22

6 Conclusions 23
6.1 Identification of general security objectives for introduction of mobility IP services 23
6.2 Threat analysis related to the addition of mobility facilities on Internet 23
6.3 Identification and evaluation of risks for each threats 23
6.4 Identification of security requirements for mobility 24

7 References 25
7.1 IPSEC 25
7.2 IP Routing for Wireless / Mobile Hosts (Mobile IP) 25

Appendix 1: Detailed list of mobility scenarios 27
A1.1 Static mobility scenarios 27
A1.2 Dynamic mobility scenarios 31
A1.3 Communication between two mobiles of different home networks 34
A1.4 Communication between two mobiles of the same home network 37

Appendix 2: Detailed description of selected mobility scenarios and respective threat analysis 41
A.2.1 Scenario 1.2.2.2 41
A2.2 Scenario 1.2.3.2 49

Appendix 3 - Risk Assessment Details 58
A3.1 Detailed description of risk assessment criteria 58
A3.2 Threat/Risk Matrices for Mobile IPv4 and Mobile IPv6 60

Abbreviations

AH	Authentication Header
CN	Correspondent Node
DoS	Denial of Service
FA	Foreign Agent
GSM	Global System for Mobile Communications
HA	Home Agent
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITSEC	Information Technology Security Evaluation and Certification
LAN	Local Area Network
MN	Mobile Node
MSC	Message Sequence Chart
PKI	Public-Key Infrastructure
PNO	Public Network Operator
RFC	Request for Comments (Internet Standards)
TCP	Transport Control Protocol
VPN	Virtual Private Network

 © 1999 EURESCOM Participants in Project P912-PF

Definitions

Internet related definitions

Internet

The group of networks over IP technology. It uses RFC standards.

IP

The Internet Protocol, defined in STD 5, RFC 791, is the network layer for the TCP/IP Protocol Suite. It is a connectionless, best-effort packet switching protocol.

RFC

The Request For Comments document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all (in fact very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs.

Security related defintions

Risk

The likelihood of threat occurrence.

Threat

The potential for compromise of confidentiality, integrity, or availability of a security subject.

Authentication

Security service providing assurance of the identity of a person or a system.

Confidentiality

Security service protecting against information being disclosed or revealed to unauthorized entities.

Integrity

Security service protecting against data being changed, deleted, or substituted without authorization.

Flooding

An attack that involves sending messages to a network node sufficiently frequently that node functionality is impaired.

IPSec

Internet Protocol Security. A developing standard for security at the network or packet processing layer of network communication. IPSec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of the data as well.

Non-repudiation

The facility to prove that past transactions did, in fact, take place.

Spoofing

An attack that involves masquerading as a network node in order to obtain, manipulate or destroy data.

Virtual Private Network

A network configuration that makes use of firewalls and/or encrypted and authenticated links to provide privacy over the public network infrastructure.

Mobile IP terms and definitions

Correspondent node

A peer node with which a mobile node is communicating. The correspondent node may be either mobile or stationary.

Foreign link

Any link other than the mobile node's home link.

Home subnet prefix

The IP subnet prefix corresponding to a mobile node's home address.

Home link

The link on which a mobile node's home subnet prefix is defined. Standard IP routing mechanisms will deliver packets destined for a mobile node's home address to its home link.

MobileIP

The name given to a group of internetworking protocols, including, for example, those specified in RFC 2002 and RFC 2005.

Home address

An IP address assigned to a mobile node within its home link.

Mobile node

A node that can change its point of attachment from one link to another, while still being reachable via its home address.

Movement

A change in a mobile node's point of attachment to the Internet such that it is no longer connected to the same link as it was previously. If a mobile node is not currently attached to its home link, the mobile node is said to be away from home.

 © 1999 EURESCOM Participants in Project P912-PF

1 Introduction

This deliverable presents the analysis and conclusions of Eurescom project P912. This group has developed security guidelines for mobile IP. This deliverable identifies and evaluates the security afforded by MobileIP and it defines security requirements for IP mobility.

The conclusions and requirements developed within this document will be used to inform the second deliverable from the P912 working group, but they might also be used by other working groups.

The first chapters cover the evaluation, study and identification of the problem. The last chapters present the identified requirements and conclusions. Readers who are unfamiliar with the basic operation of IP mobility would be well advised to consult an introduction to the subject, such as James Solomon's 'Mobile IP: The Internet Unplugged' (Prentice Hall, 1998), or Charles Perkins' 'Mobile IP: Design Principles and Practices' (Addison-Wesley, 1998).

This project has not attempted any analysis of the security afforded by the introduction of Mobile IP to UMTS as proposed by the 3GPP (Third-Generation Partnership Project). The documentation specifying this technology is not yet stabilised and is, therefore, not suitable for detailed analysis. Readers wishing to familiarise themselves with this documentation should consult ftp://ftp.3gpp.org/TSG_SA/WG2_Arch/ S2MobileIp/ where the latest documentation is available.

 © 1999 EURESCOM Participants in Project P912-PF

2 Security policy and objectives for IP mobility

2.1 Introduction

IP security was not particularly important in the past because IP was primarily used in academic environments where the traditional security services of confidentiality, integirty and availability were not needed. Now this has all changed; IP is being used by business and security is needed. Furthermore, IP mobility introduces the need for extra security because the point of attachment is not fixed, so the link between the mobile node and its home network should be considered insecure. In all cases, the physical security afforded by traditional local area networks where buildings are protecting the node and hidden wires protect the local connections is made weaker by the introduction of IP mobility.

This chapter presents PNOs security objectives with regard to the introduction of mobility services to the Internet. It details, at a high level, the key requirements for the development of a secure mobile IP standard.

IP mobility (or IP roaming) is an increasingly sought after service, as the number of mobile workers increases, and their dependence on the home network (for such services as e-mail and access to corporate information) grows. In all potential mobile-IP scenarios, security will be a critical service enabler, ensuring that the mobile operator can communicate over IP without putting at risk the confidentiality, integrity, or availability of the home network and the information it contains. Accountability is also a necessary element in any comprehensive security solution and will be an important contributor to the overall security of the mobile-IP service.

It is important that the security solution is assurable (within the context of the ITSEC Common Criteria) and takes account of current and evolving European legislation concerning the responsibilities of telcos with regard to the security of their networks.

Requirements are especially important when accessing the home network. Usually the home network (Intranet) is protected by a firewall. Opening up the Intranet to Mobile IP clients might introduce a dangerous security problem if not handled properly.

2.1.1 Solution flexibility

Building security into the network IP layer improves efficiency and flexibility of application design and allows the tiering of application layer security solutions to satisfy various customer requirements. In order for IP layer security to provide this flexibility, the security design for mobile IP must ensure that high levels of modularity and configurability are present in the solution. Security options designed to support mobile IP should support the tailoring of security solutions to various customer requirements to the greatest possible extent.

Thus, PNOs security requirements for mobile IP are related to the maintenance of confidentiality, integrity, availability and accountability of data transmitted over the IP link, to a level consistent with stated customer requirements. Hence, PNOs requirements necessitate a security design for mobile IP that is flexible and capable of supporting a wide range of security solutions. At one end of the spectrum, one might envisage a mobile-IP configuration that provided guaranteed confidentiality and integrity (perhaps based upon strong public-key encryption and strong authentication mechanisms), very high availability, and assurance to a set of common criteria (ITSEC). Other users may be willing to accept less sophisticated (and expensive)

confidentiality and integrity mechanisms and/or a lower guaranteed level of availability in return for cost savings and ease of maintenance. The security design for mobile IP must be able to support this variation in customer requirements.

2.1.2 Overview

This chapter presents PNOs high-level security policy and more detailed security objectives. PNOs general security policy is described in terms of general statements and mobility-related statements.

Security objectives are defined in terms of confidentiality, integrity, authentication, authenticity, availability, authorised access, accountability, assurance, and security management objectives. Every security objective has been evaluated according to a rating with three possible values:

- Primary or major relevance;
- Secondary or medium relevance; and,
- Low relevance within this context.

Only security objectives of primary or major relevance are presented hereunder.

2.2 Security policy

General and mobility-related security policy includes the following statements :

- Security must prevent and detect the occurrence of security breaches as well as minimizing the consequences.
- Security must guarantee the confidentiality, integrity and availability of sensitive information and valuable resources.
- The security level required for implementing mobility facilities should not be less than the security level achieved within the home network.
- The security level must be maintainable and adaptable over a long period of time.
- The strength and costs of each security solution should be in balance with the security risk the solution encounters.
- A security solution should put minimum constraints on the quality of service, as it would be when security aspects were not considered.
- The use of security solutions must be in accordance with legislative obligations and constraints (privacy law, wiretapping by authorised organisations).
- The security solutions applied should take into account both current IP protocols (IPv4) and future IP protocols (IPv6).
- The use of security should put minimum constraints on the involvement of other parties (service providers, manufacturers...).
- The security solutions applied should not block the interoperability of visited networks.
- Security solutions should be fully scalable to, at least, mid-term system demand projection.

 © 1999 EURESCOM Participants in Project P912-PF

2.3 Security objectives

We have selected the most important security objectives for the introduction of mobility to the Internet. The list of objectives is a structured list, with no specific prioritisation made among the different objectives. The list is structured into several groups for easy identification.

2.3.1 How we selected security objectives

All PNOs involved in this project proposed the security objectives they consider as the most relevant. All the proposed security objectives have been grouped into a very broad list of security objectives. The project has then selected the commonly agreed most important security objectives, according to a detailed rating.

This rating was based on the following levels:

- Primary or major relevance

  The security objective is essential. An adequate security measure has to be implemented to prevent any threats related to this objective. Implementation and usage of threat countermeasures is mandatory.

- Secondary or medium relevance

  This security objective may be essential in certain cases. Implementation and usage of threat countermeasures is not mandatory but security measures should be defined and may be implemented in cases where a serious impact on the overall system will be expected if associated attacks occur.

- Low relevance within this context

  The security objective is less important. The security level may be considered as adequate. The investigation of related threats and possible countermeasures is not a priority for the operator.

The security objectives presented in this document are the results of the evaluation described hereabove.

2.3.2 General security objectives

2.3.2.1 General security objectives for PNOs

Protection of the PNO Network

Security must protect information and resources in proportion to the anticipated risk.

Ease of Implementation

Security must be cost-effective, quantifiable and assurable, scalable and flexible, as well as based on standardised technologies.

Protection of stored information

Security must prevent unauthorised disclosure, modification, or destruction of protected information and resources.

Security Services

The PNO must offer the services required by different actors:

- The PNO must follow requirements from law enforcement agencies;
- The PNO must offer secure tunnelling or other secured services for its unsecured users;
- The PNO must allow the users to define their own security policy to be enforced by the PNO.

2.3.2.2 General security objectives for users

Security must prevent unauthorised disclosure, modification, or destruction of user information (i.e. both the user's data traffic, and the information relating to the user held in the network) and resources. To protect user privacy, the identity of the users should be protected from exposure. This means that information identifying the users, as well as transmitted data, must be protected both in databases and during transit. Users must be protected from other users in order to get secured access to services and to prevent fraudulent behaviour. Confidentiality of information relating to the user's location and/or usage profile must be maintained.

2.3.2.3 General security objectives for other actors

Commercial security (service provider)

Security must protect the information and resources of the service provider. Security must prevent the unauthorised disclosure, modification, or destruction of service provider data and unaccountable actions effecting service provider information and resources.

Legal security (regulatory agencies)

Security must not prejudice the activities of private or public organisations or service providers at the expense of other such organisations. Security must conform to existing national and international legislation. Law enforcement agencies and regulators should be given the opportunity to access the information they have legal access to.

2.3.3 Specific security objectives

This section details security specific to IP mobility. These are intended to apply to any IP mobility protocol or implementation and should not be interpreted as referring to any specific protocol or implementation.

2.3.3.1 Confidentiality

All transferred data will be protected to the same level of confidentiality or higher as the home network. All mobility management information will be protected from any unauthorised disclosure, whether in transit or storage at any point in the network. The PNOs protect packets they forward on behalf of their users by encrypting this traffic during exchanges with other PNOs.

2.3.3.2 Integrity

All transferred data and databases will be protected against any unauthorised modification or deletion. This is particularly important when exchanging accounting

 © 1999 EURESCOM Participants in Project P912-PF

related information, and information about the movement of the users. It must also be possible to prove the integrity of data for non-repudiation purposes.

2.3.3.3 Authentication

All network elements (nodes and clients) and network users will have associated authenticators that can be directly and unambiguously attributed to those elements and users. The home network should authenticate all information (packets) before allowing these to enter its internal network, in order to protect this internal network and its users.

2.3.3.4 Authenticity

The PNOs must make sure that all its stored information is authentic. The PNOs must be able to verify the authenticity of users requiring their services. This does not necessarily mean that the PNO must authenticate the user directly, (which would mean that the identity of the user is revealed to the PNO in question).

2.3.3.5 Availability

All information, resources and network services will be protected from DoS (Denial of Service) attacks.

The PNOs must provide services to its users according to a given policy. In general users should have rights giving them guaranteed access to services which they are paying for.

2.3.3.6 Authorised access

A PNO must ensure that users are authorised to access the services that they require.

Users that have subscribed to services on their home network should be able to access these services at the visited PNO (if possible). This requires that the PNO is able to get some kind of authorisation from the visitor's home network, or another trusted party.

All PNOs must ensure that all claims to access confidential data are requested by those authorised to do so before granting access to this data.

2.3.3.7 Accountability

All network users actions will be directly and unambiguously attributable to those users responsible. The PNO must make sure the users can be held accountable for their use of resources.

2.3.3.8 Assurance

Security solutions will be assurable within the context of the ITSEC Common Criteria v2.0. Security solutions will specify which Assurance Level they are to be evaluated against.

2.3.4 Security management objectives

This section details security objectives for the secure management of a network supporting IP Mobility.

2.3.4.1 Key management

Secure key management procedures and principles must be applied.

The confidentiality, integrity and availability of all key management information and the keys themselves must meet the necessary assurance criteria. The key management systems must be flexible enough to allow for introduction of new services.

2.3.4.2 Security modules management

The PNOs must agree on a minimum set of Security Modules to be used in order to ensure technological interoperability between different PNOs. All security modules must be tamper-proof. Security modules must be designed to prevent reverse engineering.

2.3.4.3 Mobility information management

All data stored on network nodes and mobile clients for the purposes of establishing, authenticating and securing mobile connections will be considered to have very high integrity, availability and confidentiality requirements. All changes to IP mobility management information must be extensively logged in tamper-proof, high-integrity logs.

The PNOs must keep the communication between different security domains to a minimum, reducing the traffic load between different PNOs.

2.3.4.4 Rights and profiles management

Generation, distribution, storage, alteration, and revocation of user profiles and privileges will be securely managed to ensure accountability, authentication, and assurance policies are adhered to. User account and privilege management logs will be regularly audited.

 © 1999 EURESCOM Participants in Project P912-PF

3 Threat identification for different mobility scenarios

The analysis of the mobility scenarios highlights several potential threats. These threats concern the mobile node, the home network, the correspondent network or the visited network. Each entity can be the victim or can be considered as the point of attack.

3.1 Mobility scenarios

3.1.1 Goal and structure of mobility scenarios

This chapter sketches out the main scenarios for mobility over IP protocols. These scenarios will be the basis for discussion within P912 project 'Security for Mobility in IP'. They give a theoretical framework in which mobility takes place. At this time we do not distinguish between IPv4 and IPv6. Indeed, study should be guided by the usage of mobility rather than by the technology.

Section 3.1.2 is a brief presentation of the main "actors" in IP Mobility : the user, the type of applications the user may want to use, the type of mobile end-device (cellular telephone, laptop) and the type of connections used to connect to the Internet (Ethernet, GSM, etc).

Section 3.1.3 sets out the two basic mobility types identified for mobility analysis. Three types of network configuration based on these two mobility types are then detailed.

3.1.2 Actors influencing mobility scenarios

This section provides descriptions of the different elements having specific roles in the mobility scenarios.

3.1.2.1 User

The typical user of Mobile IP has got an IP address on his home network and is likely to be physically connected to a foreign subnetwork. For example, they may be a commercial traveller using their laptop while visiting customers. They might use the protocol from a train with a GSM handset to read their e-mail. They might also be physically connected to the customer's Ethernet network and be able to receive the same network environment as if they were at their own office. They are able to get information from their own Intranet, make transactions with their own remote databases. In fact, due to the growth of mobility facilities, anybody who is likely to get connected to the Internet away from home or office might be a Mobile IP user.

3.1.2.2 Application

The IP layer is never used directly by Mobile IP users. They use it from the top-level application layer. That is why we must consider the applications as the real interface over Mobile IP.

We should assume that any kind of IP applications that are able to run on a mobile laptop (e-mail, world wide web or ftp but also business applications like database access, secure transactions, electronic payment) could be a "mobile" application.

3.1.2.3 Connection

We can distinguish between two types of IP layer mobility:

- Static mobility or nomadism: the user connects their laptop on a remote LAN (e.g. an ethernet network) on which they are not usually registered. Afterwards they stay connected on this LAN.
- Dynamic mobility: the user uses a wireless connection to reach the Internet and crosses several networks while connected.

Static mobility can be performed over Ethernet, Token Ring, etc., while dynamic mobility takes place over GSM, Hiperlan or IEEE802.11 connections. Nomadic users may also use wireless network media, although this is unlikely to be commonplace.

Dynamic mobility implies the possible existence of several IP/medium interfaces, especially when considering IPv6, at the same time. It may also imply that the connection point changes quickly.

3.1.2.4 Hardware

The most common way to be a Mobile IP user is to use a laptop connected to the Internet over different media (ethernet, GSM, radio, etc). Vendors have developed cellular phones with a small screen allowing reduced web surfing capabilities and this kind of device could obviously be used for Mobile IP.

Although we are mainly interested in the IP aspect of mobility, we should take the link-layer and below into account. The specific security weaknesses of the laptop or of the GSM coud render IP layer security ineffective.

3.1.3 Description of the basic network configuration for mobility

Two basic mobility types have been identified for analysis:

- Static mobility is a slow mobility from a wired network to another wired network. Static mobility is performed without frequent movements between two or several networks. This is, for instance, the situation of a laptop connected to another network for a relatively long time.
- Dynamic mobility which includes high-speed movement over wireless connections, for example local radio networks.

Based on these two mobility types, three types of network configuration can be considered :

- Network scheme for static mobility with a fixed correspondent (figure 3.1)
- Network scheme for dynamic mobility with a fixed correspondent (figure 3.2)
- Network scheme for mobility between two mobiles (figure 3.3)

For each of these configurations, the correspondent can be in the home/foreign/visited network; the mobile node can move between home and foreign networks or between two foreign networks; and both the mobile or the correspondent can start the communication. This leads to ninety seven possible scenarios.

All these scenarios have been investigated in detail and are summarised in Appendix 1.

 © 1999 EURESCOM Participants in Project P912-PF

In this section we only provide the main categories of scenarios. Details can be found in Appendix 1.

3.1.3.1 Network scheme for static mobility with a fixed correspondent

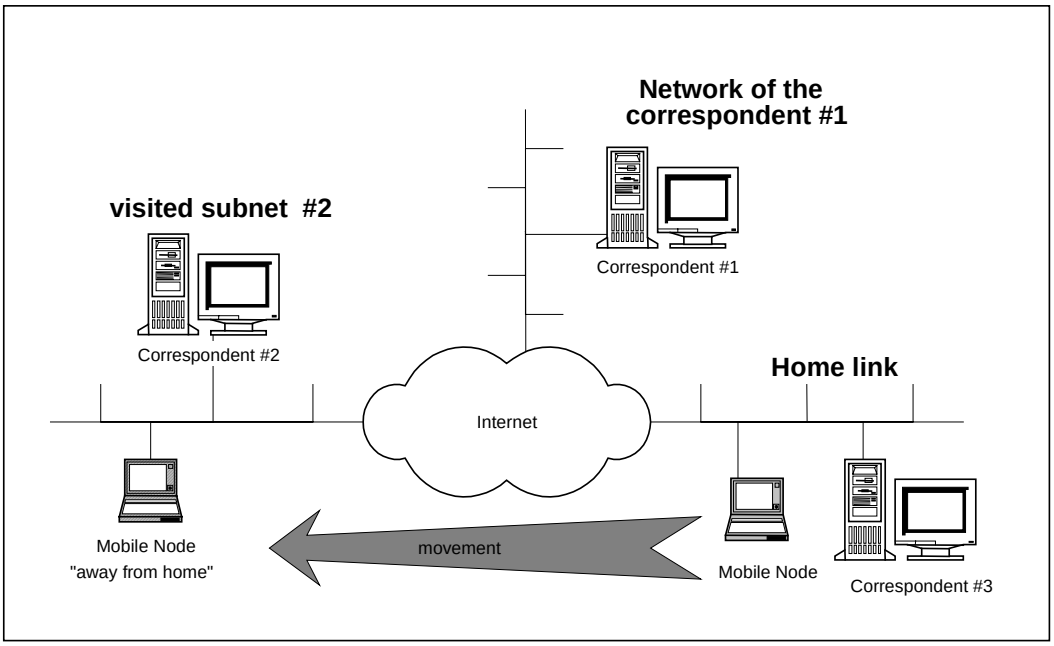


Figure 3.1

3.1.3.2 Network scheme for dynamic mobility with a fixed correspondent

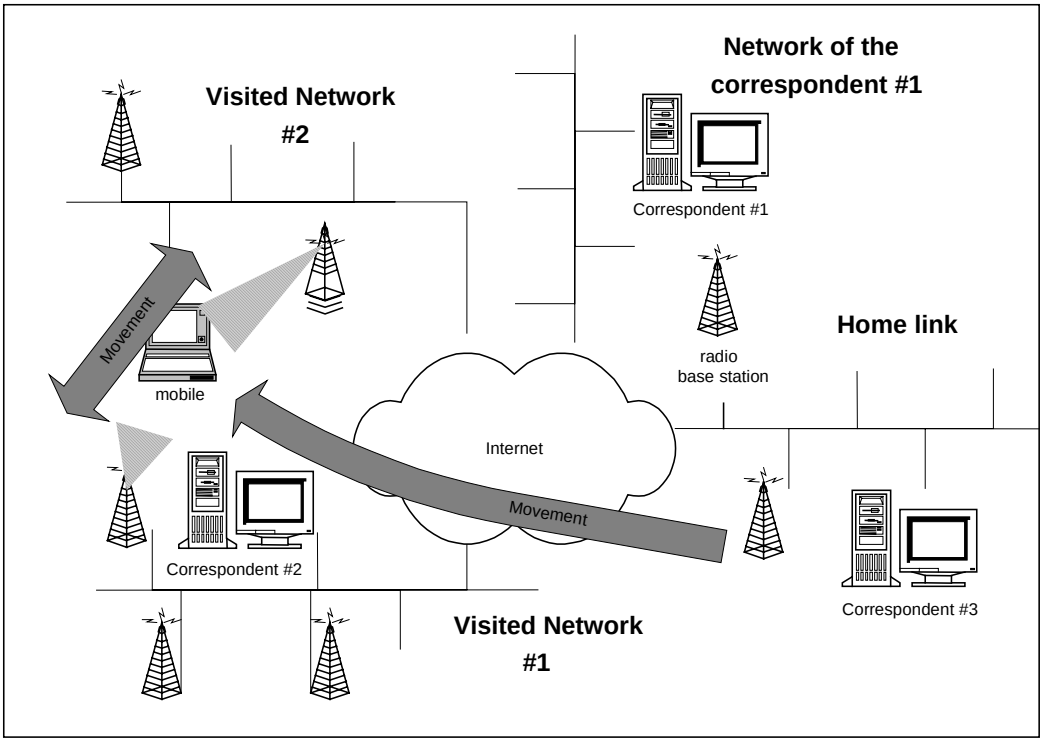


Figure 3.2

3.1.3.3 Network scheme for mobility between two mobiles

For clarity of purpose, mobile#1 and mobile#2 are respectively drawn as dynamic and static mobiles. However, they can both be static or dynamic.

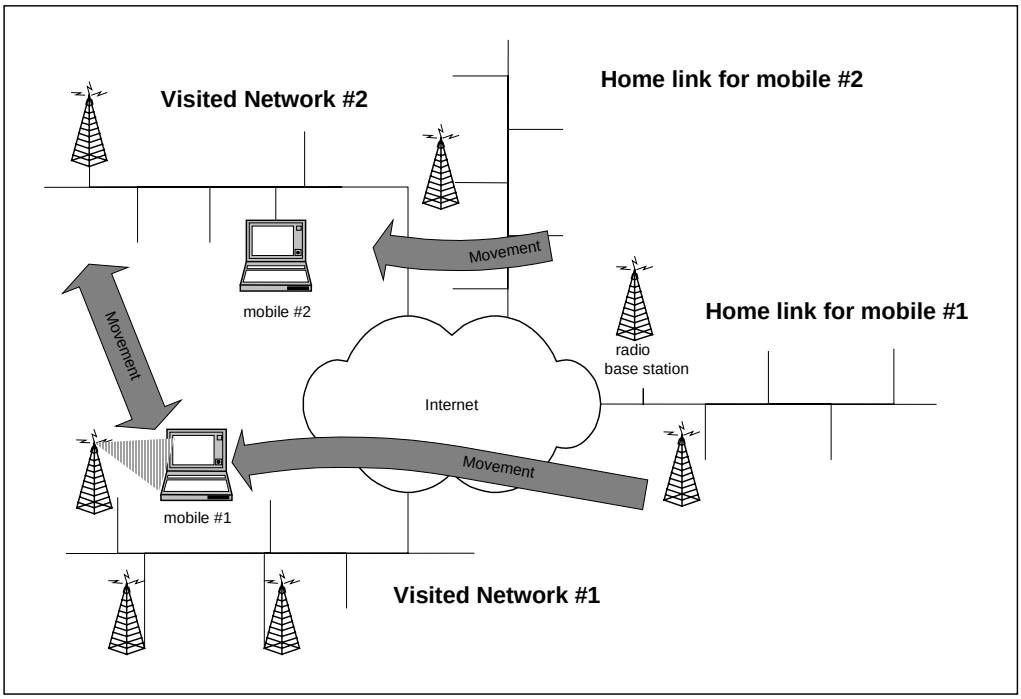


Figure 3.3

Mobility scenarios for static and dynamic mobiles have been investigated in detail. These scenarios and the respective figures can be found in Appendix 1.

3.2 Scenario analysis

During the project, the mobility scenarios identified in Section 3.1 and described in Appendix 1 have been investigated in detail. Each scenario has been investigated using IPv4 and IPv6.

Then a detailed threat analysis has been performed for each scenario. The results of each scenario threat analysis are presented in the following section.

Examples of scenario analysis can be found in Appendix 2. These examples comprise:

- textual description of the scenario using IPv4
- textual description of the scenario using IPv6
- graphical representation (MSC) of the scenario using IPv4
- graphical representation (MSC) of the scenario using IPv6
- threat analysis

3.3 Threats

In this section, we have concentrated on the mobility related threats identified within this project. More particularly, after considering the IP version features influencing mobility related threats, we only mention hereunder the Mobile IP related threats, and

 © 1999 EURESCOM Participants in Project P912-PF

we do not consider general IP networking (e.g. non mobility-specific) threats. Indeed, once connected to a foreign network, the mobile node can perform, and be a victim of, any generic IP networking attack, like any other fixed node. The investigation of these IP networking threats is out of the scope of our project.

In this section we provide the list of the most crucial threats which are the result of the threat analysis performed for each mobility scenario. Examples of detailled threat analyses for two specific scenarios can be found in Appendix 2.

3.3.1 IP version features influencing mobility related threats

Some mobility related threats are common to IPv4 and IPv6 environments and are linked to the global architecture of the networks involved in the communication. But some other mobility related threats are IP version specific.

The differences between Mobile IPv4 and Mobile IPv6 that may have an influence on potential attacks are listed hereunder :

- Possible existence of a foreign agent in IPv4. Mobile IPv6 (and also Mobile IPv4 in the co-located care-of-address case) assumes that the Mobile Node also plays the role of foreign agent.
- Weaknesses implied by IPv6 stateless autoconfiguration have also been omitted. Stateless autoconfiguration is the ability of an IPv6 host to get an IP address and other routing information as soon as it is plugged into a network. As a result, this procedure coud be concurrent with the Mobile IP procedure. The mobile nodes must not get permanent IP addresses but only care-of-addresses. Visiting nodes coud exploit this to behave as permanent nodes of the visited network (with full rights) instead of visiting nodes (with limited privileges). This has not been explored because these mobility features are very dependent on the implementation, especially the movement detection.
- Encryption is an integrated feature of IPv6 but is not mandatory in IPv6 nor in IPv4. Optional encryption and mandatory authentication features are defined between MN and HA in IPv6. Of course, the use of encryption features may eradicate a lot of possible weaknesses, especially eavesdropping related threats and may help in the prevention of masquerading related threats.
- Other features like IPv6 route optimisation or the use of the Home Address Option might provide opportunities for attackers. These features, even if they are not considered as very sensitive, must be taken into account when performing a detailled threat analysis for mobility facilities on IP.

Further information giving further details of the differences between IPv4 and IPv6 mobility can be found in James Solomon's 'Mobile IP: The Internet Unplugged' (Prentice Hall, 1998), Section 12.1.

3.3.2 Loss of confidentiality/Session stealing/Spoofing of the mobile node

These attacks can be performed on the mobile each time it is connected to a (hostile) foreign network. The other hosts of the visited network can capture every packet transmitted over the link media. Scenario examples: 1.2.1.2, 1.2.1.5, 1.2.1.8, 1.2.2.2, 1.2.2.5, 1.2.2.8, 1.2.3.2, 1.2.3.5, 1.2.3.8, 1.1.1.1, 1.3.3.1

3.3.3 Loss of confidentiality/Session stealing/Spoofing of the foreign-agent

These attacks can be performed by hostile mobile nodes connected to the foreign network. They can be achieved by any host masquerading as a mobile. Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2, 1.2.1.2, 1.2.1.5, 1.2.1.8, 1.2.2.2, 1.2.2.5, 1.2.2.8, 1.2.1.2, 1.2.1.5, 1.2.1.8, 1.3.3.1…

3.3.4 Loss of confidentiality/Session stealing/Spoofing of the home-agent

These attacks can be performed by malicious foreign hosts. This attack can be achieved by any host masquerading as the mobile. Scenario examples: 1.2.2.2, 1.2.2.5, 1.2.2.8, 1.2.1.2, 1.2.1.5, 1.2.1.8…

3.3.5 Loss of confidentiality/Session stealing/Spoofing of other hosts on the foreign network

All non-ciphered communication between the local hosts of the foreign network can be compromised by the visiting mobile.

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2…

3.3.6 Loss of security features provided by the home network

This situation occurs each time the mobile is no longer protected by its home network firewall.

Scenario examples: 1.2.3.2, 1.2.3.5, 1.2.3.8…

3.3.7 DoS/Flooding of the mobile node

Flooding of the mobile node with Mobile IP messages (binding ack, etc.) or any other type of messages.

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2, 1.2.1.2, 1.2.1.5, 1.2.1.8, 1.2.3.2, 1.2.3.5, 1.2.3.8…

3.3.8 DoS/Flooding of the home agent

Flooding of the home agent with Mobile IP messages (binding update, etc.) or any other type of messages.

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2, 1.2.1.2, 1.2.1.5, 1.2.1.8…

3.3.9 DoS/Flooding of the foreign agent (IPv4 environment)

Flooding of the foreign agent with Mobile IP messages (registration request, etc.) or any other type of messages.

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2, 1.2.1.2, 1.2.1.5, 1.2.1.8…

3.3.10 DoS/Flooding of the correspondent (IPv6 environment)

Flooding of the correspondent with Mobile IP messages (binding update, etc.) or any other type of messages.

 © 1999 EURESCOM Participants in Project P912-PF

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2, 1.2.1.2, 1.2.1.5, 1.2.1.8…

3.3.11 Tracking of mobile node

Loss of privacy. Unauthorised persons can get information about the mobile user's identity and movements. This problem may also arise with IPSec ESP if tunnel mode is not enabled.

Scenario examples: 1.1.1.1, 1.1.1.2, 1.1.2.2…

 © 1999 EURESCOM Participants in Project P912-PF

4 Risk assessment and evaluation of the likelihood of threats

4.1 Introduction to risk assessment

In this section, we provide a list of criteria to enable a risk evaluation of identified Mobile IP threats. Then we provide a list of potential attacks related to IP mobility. We provide technical criteria only, as other types of criteria are not easy to evaluate or define.

4.2 List of criteria

A list of 10 criteria have been defined for the risk analysis. These criteria are:

- Equipment required (price and availability)
- Knowledge required
- Time required (Time to prepare the attack, Time to perform the attack)
- Location required
- Time-window required (Number of periods of time, length of period of time)
- Number of possible targets
- Time to recover
- Difficulty of detecting an attack
- Difficulty of identifying the attacker
- Type of access required

4.3 Levels of risk

For each of these 10 criteria, levels of risk have been defined. These levels are:

- ***H*** Highest
- H High
- M Medium
- L Low
- *l* Lowest

A detailed description of these criteria, including descriptions of the levels of risks for each criterion, is provided in Appendix 3.

This symbolic notation is used in the risk assessment for the following list of threats.

4.4 Threat notation

This section provides a description of the threat notation used in the risk assessment exercise. Figure 4.1 defines the functional architecture to be investigated.

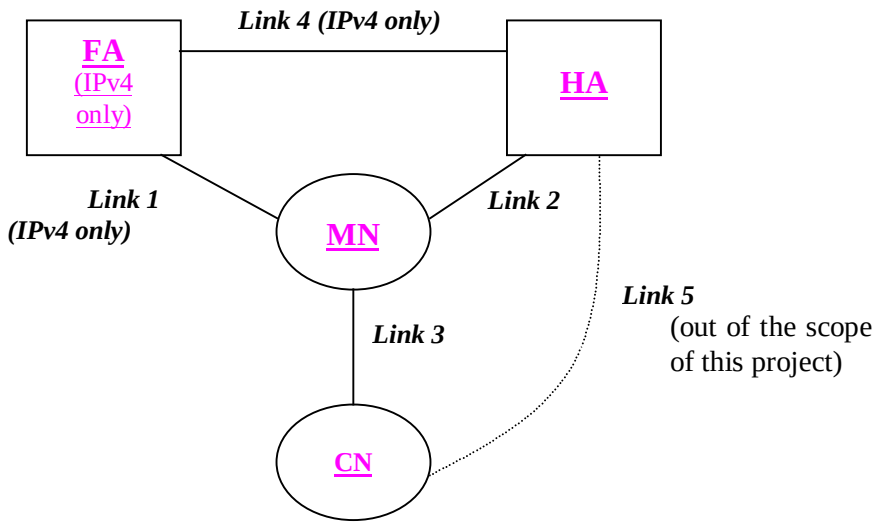


Figure 4.1 MobileIP nodes and linkages

Using this functional architecture a system for threat notation was developed and this is presented below:

- **C1** to **C10** denote the 10 risk criteria identified in section 4.2 above.
- **E1** to **E4** are Eavesdropping-related threats to links ***1, 2, 3*** and ***4*** (as identified in figure 4.1), respectively.
- **S1** to **S4** are Session Stealing-related threats to links ***1, 2, 3*** and ***4***, respectively.
- **SP-MN, SP-CN, SP-FA, SP-HA** are Spoofing-related threats to the MN, CN, FA and HA, respectively.
- **DF-MN, DF-CN, DF-FA, DF-HA** are Denial-of-Service and Flooding-related threats to the MN, CN, FA and HA, respectively.
- **T** is the threat related to Tracking of the mobile node.
- **LSF** is the threat related to the Loss of Security Features provided by the home network.

Using this threat notation and the risk criteria and classes identified above, risk assessments have been undertaken for both MobileIPv4 and MobileIPv6. The detailed results of this risk assessment exercise are presented as threat/risk matrices in Appendix 3.

 © 1999 EURESCOM Participants in Project P912-PF

5 Security requirements for mobility

5.1 Introduction

This chapter identifies the important security requirements for PNOs when introducing IP mobility. The requirements have mainly been identified as a result of the work presented hereabove in this document.

The focus of these requirements is on the PNOs that will be offering IP mobility services. There are different technologies that might be used to introduce IP mobility. In this project our focus is on MobileIP, although the requirements identified might be used as a more general basis for analysing internet mobility security.

5.2 Security requirements identification

When identifying the security requirements for secure internet mobility, there is a need to find a suitable classification for these requirements. This chapter will identify our chosen classification for these requirements.The main classes of security requirements are based on the specific security objectives that have already been identified.The identified classes are as follows:

1. Confidentiality
2. Integrity
3. Authentication
4. Availability
5. Authorised access
6. Accountability
7. Assurance

Within each of these classes we will specify the identified requirements in detail.

5.3 Security requirements

This chapter contains our identified security requirements. The requirements are divided into 7 classes, and are listed within sections 5.3.1 to 5.3.7.

5.3.1 Confidentiality

1. Data containing sensitive information about the users (such as profiles, identity, use of local resources, etc.) should be kept confidential from third parties while stored in the home or visited network.
2. Data exchanged between different PNO's containing sensitive data should be kept confidential from third parties while in transit.
3. Data containing user information that might lead to a breach of location privacy should be kept confidential from third parties. This includes binding updates, registration requests, etc.

4. Sensitive information stored on the mobile devices should be kept confidential from third parties. In the case of unauthorised access to the mobile client, its credentials should not be easily revealed which might permit later misuse.
5. User traffic should be confidentiality protected while in transit between different PNO's.
6. The PNO's should conform with legal requirements regarding lawful interception of user traffic. The PNO's should ensure that lawful interception is granted only if proper authorisation exists.
7. The user should be able to verify the status of the confidentiality protection mechanisms (radio interface only, end to end, etc.) in use, and be kept informed about changes in the status of confidentiality protection (with the possible exception of lawful interception).

5.3.2 Integrity

1. Information containing data about the users, in particular information related to accounting, billing and movement should be integrity protected while being exchanged between different PNO's.
2. Information stored in the home network and the visited network about the user, e.g. logs, should be integrity protected against unauthorised modification or deletion.
3. User traffic should be integrity protected while in transit between different PNO's.
4. The user should be able to verify the status of the integrity protection mechanisms, and should be informed about potential breaches of the integrity protection.
5. Sensitive information stored on the mobile devices should be integrity protected.
6. The integrity requirements listed should apply even if lawful interception is being performed.
7. The security modules in use should be tamper-proof in order to minimise the potential for malicious users to gain access to secret, security-critical data.

5.3.3 Authentication

1. The PNO's should be able to authenticate all information crossing different security domains.
2. If necessary, the visited network should authenticate visiting users trying to get access.
3. If necessary, the PNO should ensure that users trying to get access to internal services are authenticated.
4. The visiting nodes should be able to authenticate the visited network, in order to prevent 'fraudulent foreign networks'.
5. The key management system that will be used to support authentication mechanisms (as well as other security services) should be standardised in such a manner as to support a rapidly increasing number of users as well as offer the flexibility to add new services in a simple manner.

 © 1999 EURESCOM Participants in Project P912-PF

6. The authentication requirements listed within this section should apply even if lawful interception is being performed on a connection.
7. The visiting nodes should be able to verify the status of the authentication mechanisms in use, and stay informed about authentication failures.
8. The visited network and local services therein should be able to authenticate themselves to all visiting mobile nodes.
9. All network elements exchanging information within a security domain or across different security domains should authenticate each other as well as the information exchanged.

5.3.4 Availability

1. Both the home network and visited network should be able to protect themselves against (unauthorised) DoS conditions, either due to active attacks or 'unfortunate incidents'.
2. The visited network should ensure that legal users are given access to the services that they are authorised to access.
3. The home network should ensure that legal users are given access to the services that they are authorised to access.
4. Both the home network and visited network should ensure that their networks have sufficient resources to meet the demands of their users, and should ensure that their networks may be extended in the future to allow for new users, new services and increased traffic rates.
5. Logs should be available in compliance with laws and regulations applicable to each PNO.

5.3.5 Authorised access

1. The PNO's should ensure that all visiting users accessing mobility services are authorised to do so.
2. The PNO's should ensure that only authorised users are allowed access to "confidential information" that is stored locally, e.g. in logs.
3. The PNO's should ensure that only authorised users are allowed to modify or delete information stored about users or their use of services, movements etc.
4. The PNO's should ensure that only authorised users are allowed access to network management systems.
5. If necessary, the PNO should ensure that access to internal services is controlled.

5.3.6 Accountability

1. The PNO's should ensure sufficient logging of used services to be able to hold users unambiguously accountable for services used.
2. The PNO's should ensure sufficient logging of actions taken to be able to hold users unambiguously accountable for their actions, and to be able to trace misuse or attempted misuse.

3. All information stored about users should be stored in such a way that it adheres to the other requirements within this document.
4. The PNO's should ensure sufficient logging in order to adhere to external regulations and requirements.

5.3.7 Assurance

1. PNO's should ensure any security solution is capable of evaluation against PNO security policy and international security evaluation criteria.

 © 1999 EURESCOM Participants in Project P912-PF

6 Conclusions

This deliverable presents results from the first phase of project P912 based on the investigation of protocols for mobility management in both IPv6 and IPv4 and of security protocols (IPSec) required for mobility. These results are related to the following topics.

6.1 Identification of general security objectives for introduction of mobility IP services

General and specific security objective statements have been identified for PNOs and for users, specific security objectives (under the headings Confidentiality, Integrity, Authentication, Authenticity, Authorised access, Accountability, and Assurance) and management related security objectives (under the headings Key, Security Modules, Mobility information, and Rights and profiles management).

6.2 Threat analysis related to the addition of mobility facilities on Internet

The discussion within P912 has been based on a list of mobility scenarios giving a theoretical framework in which two basic network configurations identified for mobility analysis are defined: ‘static mobility’ and ‘dynamic mobility’.

Ninety seven scenarios have been investigated in detail within both IPv4 and IPv6 environments. Textual descriptions of the main categories of scenarios and graphical representations of scenarios using IPv4 and IPv6 are provided in the core text of this deliverable with a textual detailed threat analysis, while all scenarios are summarised in Appendix 1. The output of the scenario analysis is the following list of threat classes :

- Loss of confidentiality/Session stealing/Spoofing of the mobile node, the foreign-agent, the home-agent or the foreign network;
- DoS/Flooding of the mobile node, the home agent, the foreign agent (IPv4 environment) or the correspondent (IPv6 environment);
- Tracking of mobile node;
- Loss of security features provided by the home network.

6.3 Identification and evaluation of risks for each threats

A risk assessment has been performed for each threat in both IPv4 and IPv6 environments on the basis of criteria defined within the project (price and availability of devices required, know how / time / location / time-window / type of access required, number of possible targets, time to recover and difficulty to detect an attack and to identify the attacker). This risk assessment is presented by means of appropriate matrices combining risk assessment and threats in various situations.

6.4 Identification of security requirements for mobility

Based on the above results, seven classes of security requirements (confidentiality, integrity, authentication, availability, authorised access, accountability and assurance related classes) have been investigated.

Results from the first phase are intended as input for the second phase of Project 912, where the main work assignments will be on investigation of security measures against selected threats, on definition of security services and guidelines and for improvement of security policy for PNOs. This will be presented within the final deliverable "Security guidelines for introduction of mobility facilities to the Internet" to be delivered at the end of this project.

 © 1999 EURESCOM Participants in Project P912-PF

7 References

7.1 IPSEC

Internet-Drafts

- Policy Framework for IP Security, draft-ietf-ipsec-policy-framework-00.txt, February 1999

Request For Comments

- Security Architecture for the Internet Protocol (RFC 2401) , November 1998
- IP Security Document Roadmap (RFC 2411), November 1998
- IP Authentication Header (RFC 2402), November 1998
- IP Encapsulating Security Payload (ESP) (RFC 2406), November 1998

7.2 IP Routing for Wireless / Mobile Hosts (Mobile IP)

Internet-Drafts

- Mobility Support in IPv6, draft-ietf-mobileip-ipv6-07.txt, November 1998
- Firewall Support for Mobile IP, draft-montenegro-firewall-sup-03.txt, January 1998
- IP Mobility Support version 2, draft-ietf-mobileip-v2-00.txt, November 1997
- Use of IPSec in Mobile IP, draft-ietf-mobileip-ipsec-use-00.txt, November 1997
- IP Mobility Architecture Framework, draft-ietf-mobileip-ipm-arch-00.txt, September 1998

Request For Comments

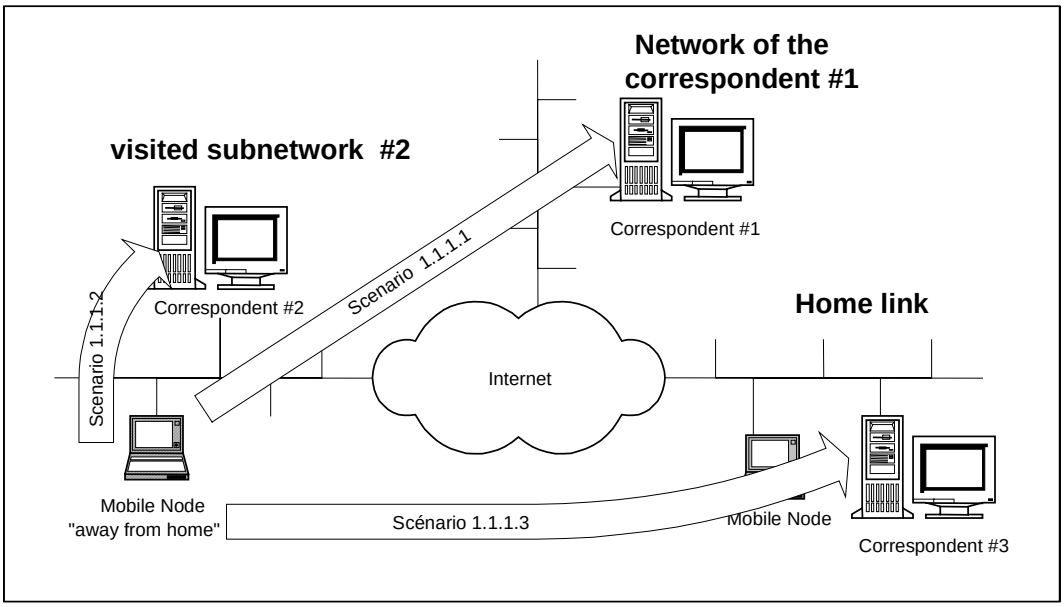
- IP Mobility Support (RFC 2002), October 1996
- Reverse Tunneling for Mobile IP (RFC 2344), May 1998

 © 1999 EURESCOM Participants in Project P912-PF

Appendix 1 - Detailed list of mobility scenarios

A1.1 Static mobility scenarios

A1.1.1 The mobile node is on a foreign network and wants to reach a correspondent



Scenario 1.1.1.1 : The correspondent is on a foreign network.

The mobile node has moved from its home network to a visited network and tries to contact a correspondent on a third network. This is the basic mobility scenario.

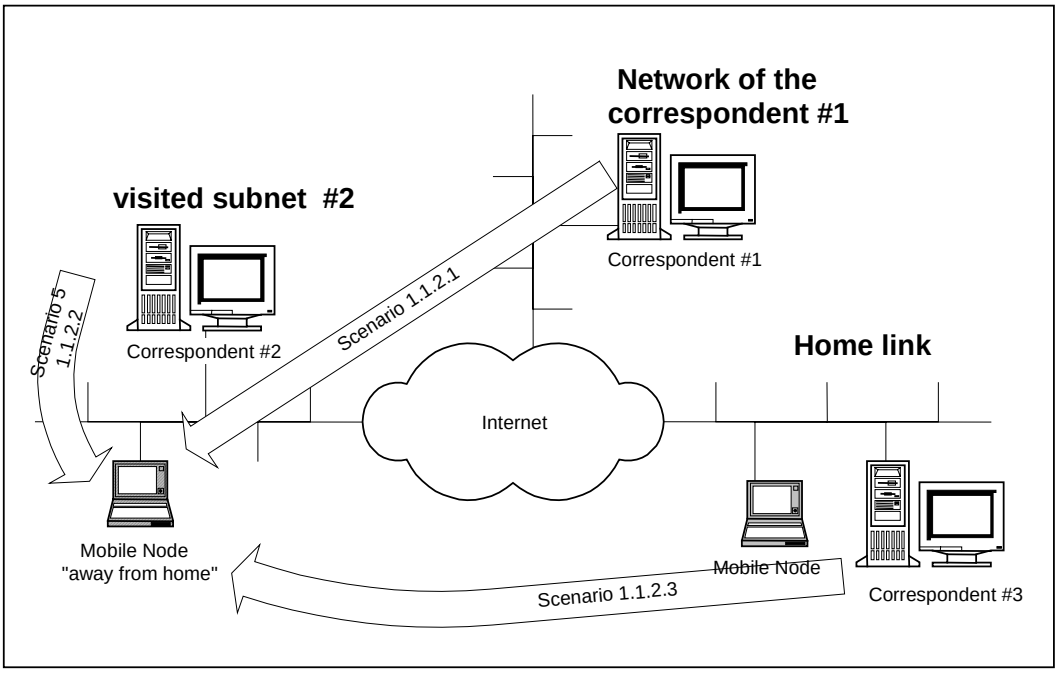
Scenario 1.1.1.2 : The correspondent is on the same network as the mobile node.

The mobile node has moved from its home network to a visited network and tries to contact a correspondent on the same network. Some security problems may arise from the management of the mobility since the machines should communicate directly (without an intervening firewall).

Scenario 1.1.1.3 : The correspondent is on the mobile's home link.

The mobile and the correspondent may exchange confidential data as if they were on the same link although they might cross a hostile network.

A1.1.2 The mobile node is on a foreign network and a correspondent wants to reach it



These scenarios are slightly different from the previous ones since the originator of the communication is the correspondent.

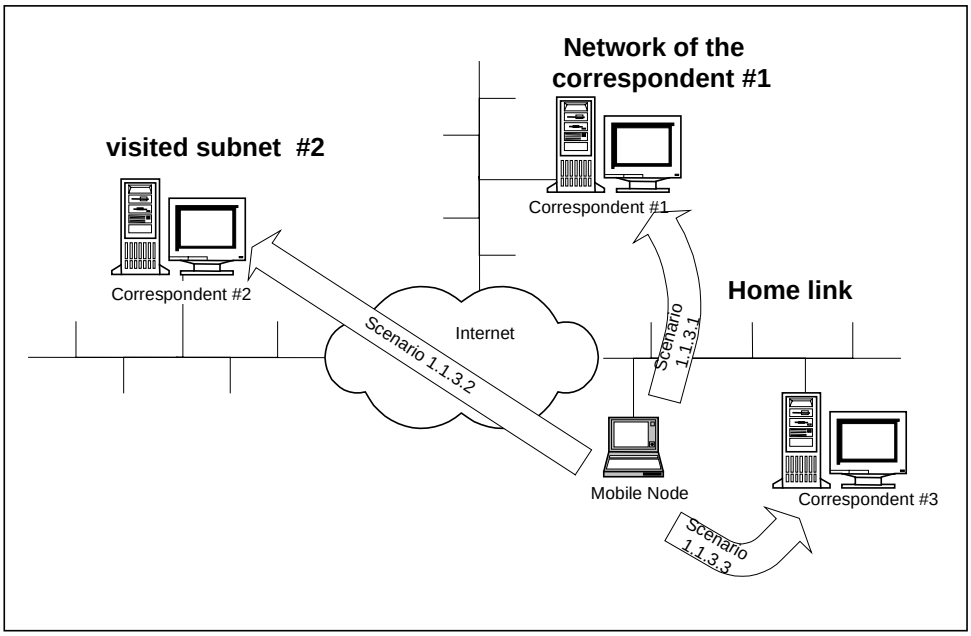
Scenario 1.1.2.1: The correspondent is on a foreign network.

Scenario 1.1.2.2: The correspondent is on the network on which the mobile is.

Scenario 1.1.2.3: The correspondent is on the mobile's home link.

 © 1999 EURESCOM Participants in Project P912-PF

A1.1.3 The mobile node is on its home link and wants to reach a correspondent



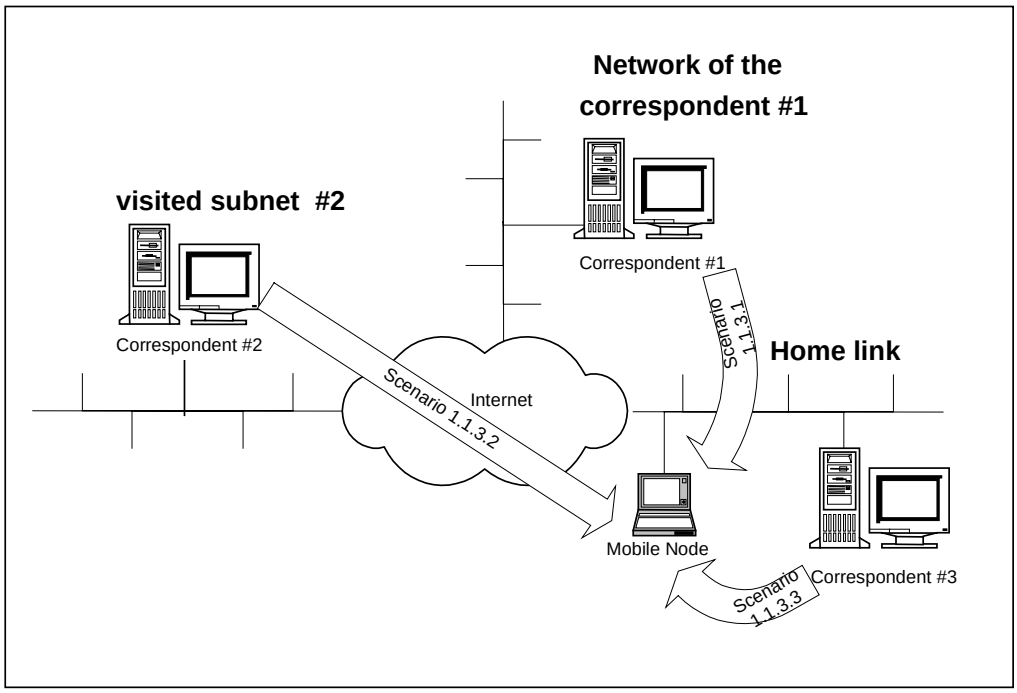
This is not really a situation of mobility, but all the components, albeit not moving, implement the mobility facilities. As a result, an outside node could masquerade as a mobile and use mobility facility weaknesses.

Scenario 1.1.3.1: The correspondent is on a foreign network that the mobile has not already visited.

Scenario 1.1.3.2: The correspondent is on a foreign network that the mobile has already visited.

Scenario 1.1.3.3: The correspondent is on the mobile's home link.

A1.1.4 The mobile node is on its home link and a correspondent wants to reach it



Scenario 1.1.4.1: The correspondent is on a foreign network that the mobile has not already visited.

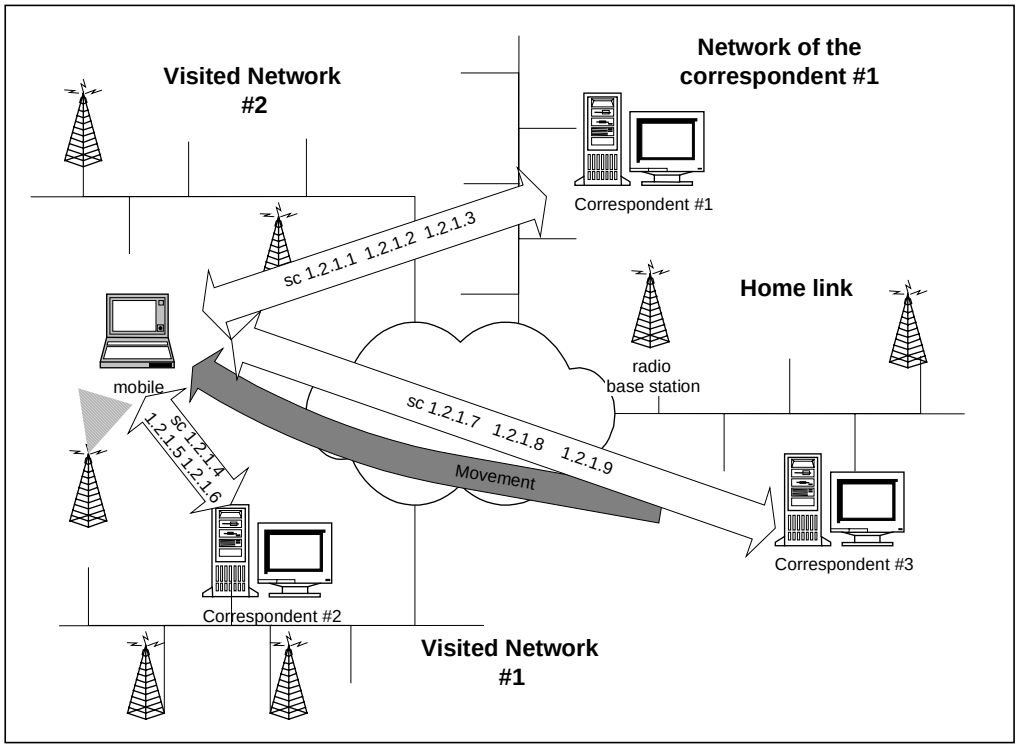
Scenario 1.1.4.2: The correspondent is on a foreign network that the mobile has already visited.

Scenario 1.1.4.3: The correspondent is on the mobile's home link.

 © 1999 EURESCOM Participants in Project P912-PF

A1.2 Dynamic mobility scenarios

A1.2.1 The mobile moves from its home network to a foreign network



Scenario 1.2.1.1: The mobile and correspondent#1 are communicating with each other, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.2: The mobile starts a communication with correspondent #1, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.3: Correspondent#1 starts a communication with the mobile, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.4: The mobile and correspondent#2 are communicating with each other, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.5: The mobile starts a communication with correspondent #2, then the mobile moves from its home network to a foreign network.

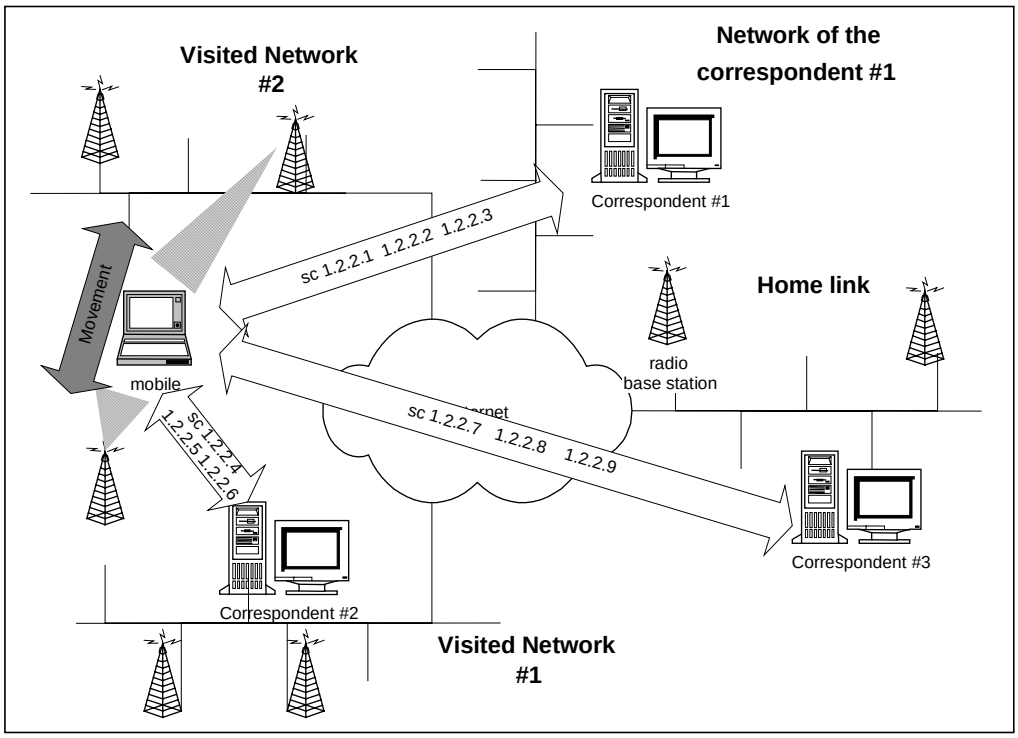
Scenario 1.2.1.6: Correspondent#2 starts a communication with the mobile, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.7: The mobile and correspondent#3 are communicating with each other, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.8: The mobile starts a communication with correspondent #3, then the mobile moves from its home network to a foreign network.

Scenario 1.2.1.9: Correspondent #3 starts a communication with the mobile, then the mobile moves from its home network to a foreign network.

A1.2.2 The mobile moves from a foreign network to another foreign network



Scenario 1.2.2.1: The mobile is on a foreign network. The mobile and correspondent#1 are communicating with each other, then the mobile moves to another foreign network.

Scenario 1.2.2.2: The mobile is on a foreign network. The mobile starts a communication with correspondent #1, then the mobile moves to another foreign network.

Scenario 1.2.2.3: The mobile is on a foreign network. Correspondent#1 starts a communication with the mobile, then the mobile moves to another foreign network.

Scenario 1.2.2.4: The mobile is on a foreign network. The mobile and correspondent#2 are communicating with each other, then the mobile moves to another foreign network..

Scenario 1.2.2.5: The mobile is on a foreign network. The mobile starts a communication with correspondent #2, then the mobile moves to another foreign network.

Scenario 1.2.2.6: The mobile is on a foreign network. Correspondent #2 starts a communication with the mobile, then the mobile moves to another foreign network.

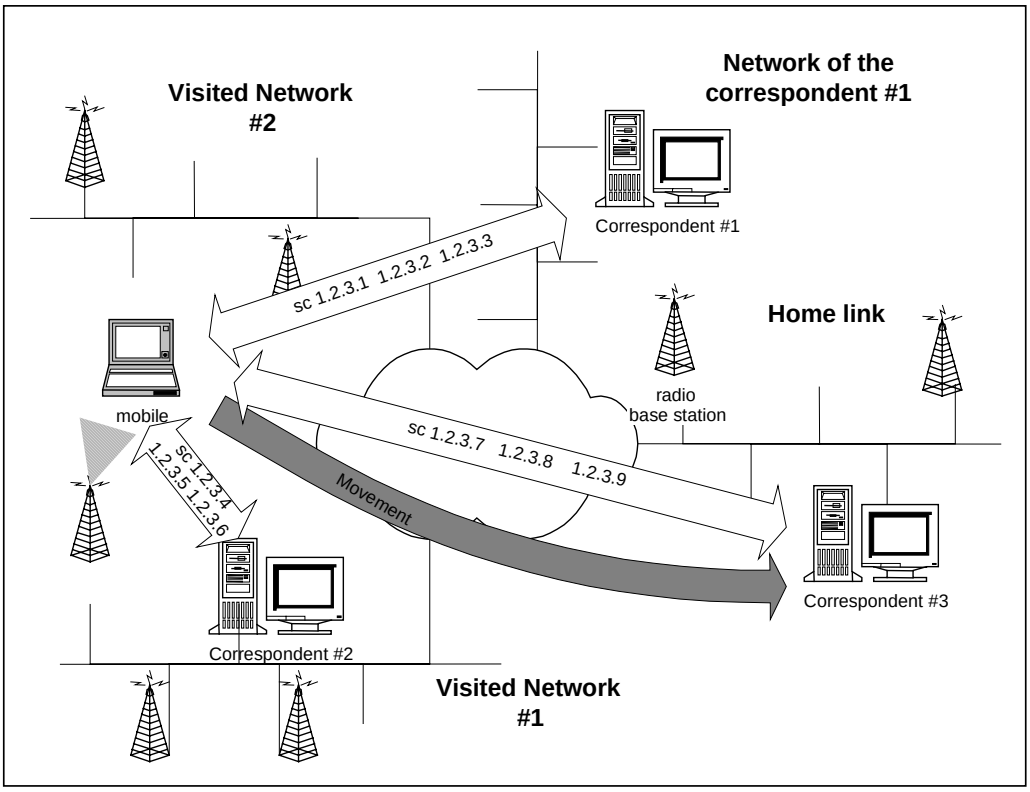
Scenario 1.2.2.7: The mobile is on a foreign network. The mobile and the correspondent#3 are communicating with each other then the mobile moves to another foreign subnetwork.

Scenario 1.2.2.8: The mobile is on a foreign network. The mobile starts a communication with correspondent #3, then the mobile moves to another foreign network.

Scenario 1.2.2.9: The mobile is on a foreign network. Correspondent#3 starts a communication with the mobile, then the mobile moves to another foreign network.

 © 1999 EURESCOM Participants in Project P912-PF

A1.2.3 The mobile moves from a foreign network to its home network



Scenario 1.2.3.1: The mobile is on a foreign network. The mobile and correspondent#1 are communicating with each other, then the mobile moves to its home network.

Scenario 1.2.3.2: The mobile is on a foreign network. The mobile starts a communication with correspondent #1, then the mobile moves to its home network.

Scenario 1.2.3.3: The mobile is on a foreign network. Correspondent#1 starts a communication with the mobile, then the mobile moves to its home network

Scenario 1.2.3.4: The mobile is on a foreign network. The mobile and correspondent#2 are communicating with each other, then the mobile moves to its home network.

Scenario 1.2.3.5: The mobile is on a foreign network. The mobile starts a communication with correspondent #2, then the mobile moves to its home network.

Scenario 1.2.3.6: The mobile is on a foreign network. Correspondent#2 starts a communication with the mobile, then the mobile moves to its home network

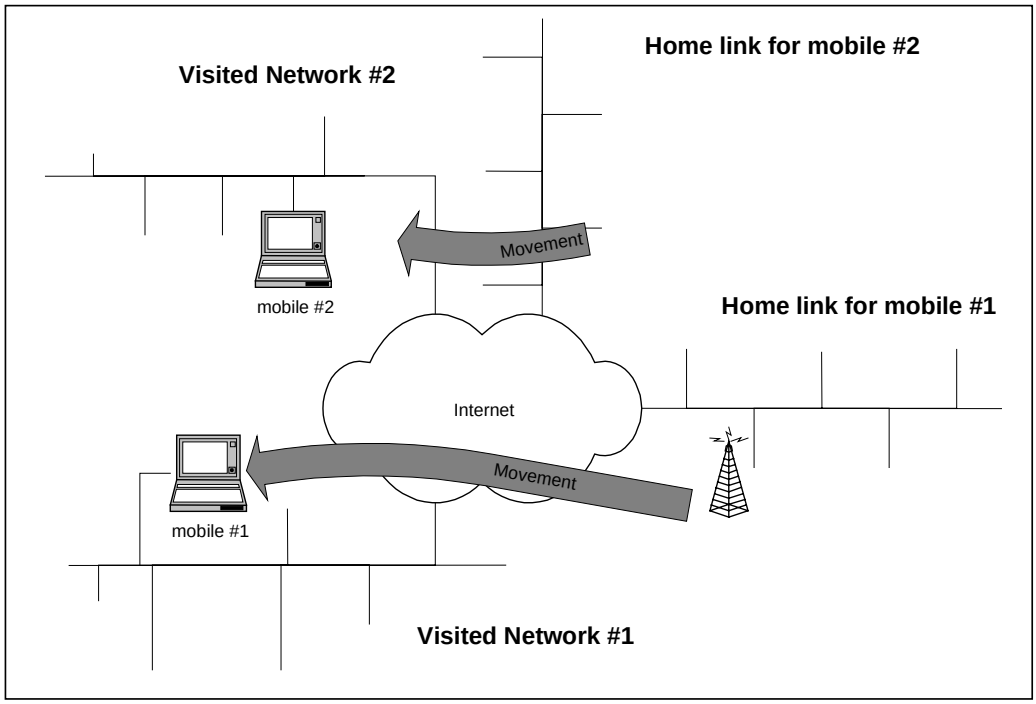
Scenario 1.2.3.7: The mobile is on a foreign network. The mobile and correspondent#3 are communicating with each other, then the mobile moves to its home network.

Scenario 1.2.3.8: The mobile is on a foreign network. The mobile starts a communication with correspondent #3, then the mobile moves to its home network.

Scenario 1.2.3.9: The mobile is on a foreign network. Correspondent#3 starts a communication with the mobile, then the mobile moves to its home network.

A1.3 Communication between two mobiles of different home networks

A1.3.1 static/static



Scenario 1.3.1.1: Both mobiles are on the same foreign network. One of them tries to connect to the other one

Scenario 1.3.1.2: Both mobiles are on different foreign networks. One of them tries to connect to the other one.

Scenario 1.3.1.3: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on a visited network. Mobile#1 tries to connect to Mobile#2.

Scenario 1.3.1.4: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on a visited network. Mobile#2 tries to connect to Mobile#1.

Scenario 1.3.1.5: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on Mobile#1 home network. Mobile#1 tries to connect to Mobile#2.

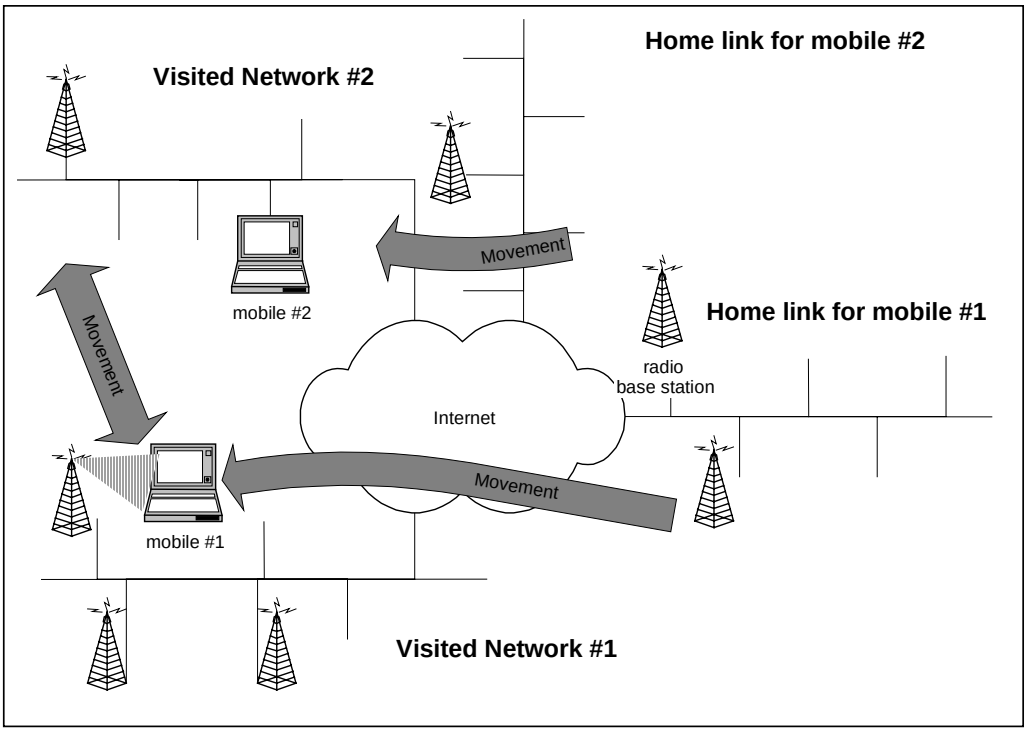
Scenario 1.3.1.6: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on Mobile#1 home network. Mobile#2 tries to connect to Mobile#1.

Scenario 1.3.1.7: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on its own home network. Mobile#1 tries to connect to Mobile#2.

Scenario 1.3.1.8: Mobile #1 is visiting Mobile#2 home network while Mobile#2 is on its own home network. Mobile#2 tries to connect to Mobile#1.

 © 1999 EURESCOM Participants in Project P912-PF

A1.3.2 dynamic/static



All these scenarios take place during a communication between the mobiles

Scenario 1.3.2.1: Mobile#1 moves from its home network to a foreign network. Mobile#2 is on another network.

Scenario 1.3.2.2: Mobile#1 moves from its home network to a foreign network. Mobile#2 is on the same visited network.

Scenario 1.3.2.3: Mobile#1 moves from its home network to a foreign network. Mobile#2 is on Moible#1 home network.

Scenario 7.2.4: Mobile#1 moves from its home network to a foreign network. Mobile#2 is on its own home network

Scenario 1.3.2.5: Mobile#1 moves from a foreign network to another foreign network. Mobile#2 is on another network.

Scenario 1.3.2.6: Mobile#1 moves from a foreign network (visited net #1) to another foreign network (visited net #2). Mobile#2 is on visited network #1.

Scenario 1.3.2.7: Mobile#1 moves from a foreign network (visited net #1) to another foreign network (visited net #2). Mobile#2 is on visited network #2.

Scenario 1.3.2.8: Mobile#1 moves from a foreign network to another foreign network. Mobile#2 is on Mobile#1 home network.

Scenario 1.3.2.9: Mobile#1 moves from a foreign network to another foreign network. Mobile#2 is on its own home network.

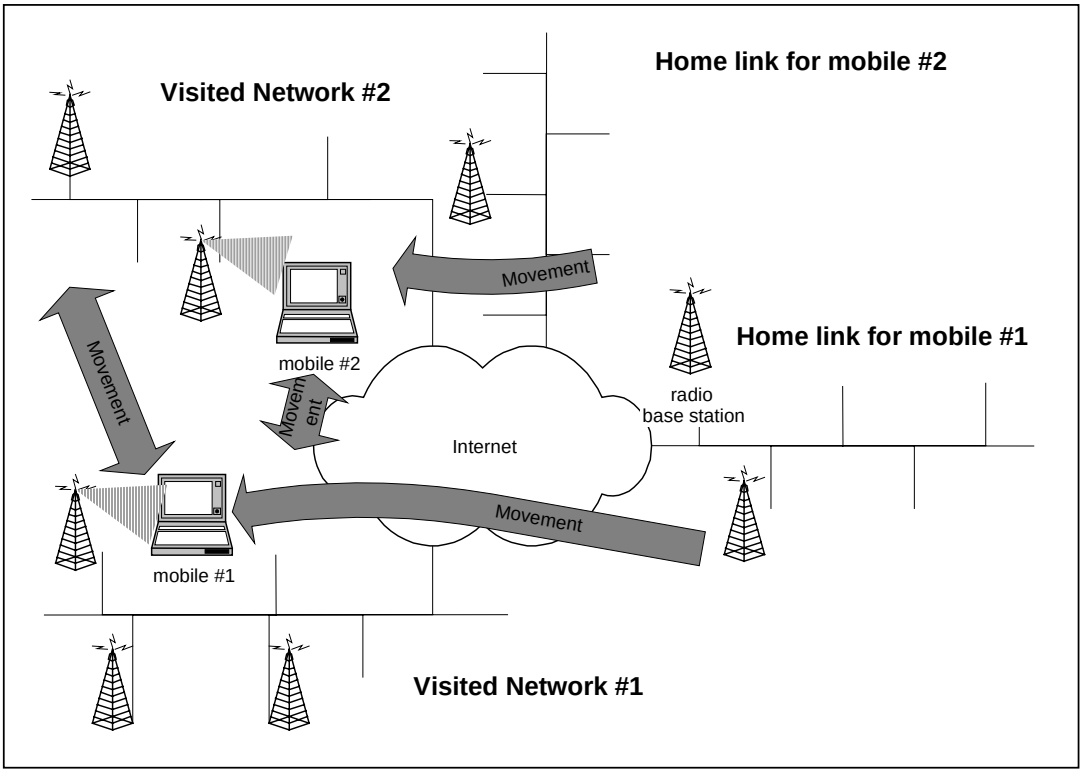
Scenario 1.3.2.10: Mobile#1 moves from a foreign network to its home network. Mobile#2 is on another network.

Scenario 1.3.2.11: Mobile#1 moves from a foreign network (visited net #1) to its home network. Mobile#2 is on visited network #1.

Scenario 1.3.2.12: Mobile#1 moves from a foreign network to its home network. Mobile#2 is on Mobile#1 home network.

Scenario 1.3.2.13: Mobile#1 moves from a foreign network to its home network. Mobile#2 is on its own home network.

A1.3.3 dynamic/dynamic



All these scenarios take place during a communication between the mobiles

Scenario 1.3.3.1: Mobile#1 and Mobile#2 move from their home networks to two different foreign networks.

Scenario 1.3.3.2: Mobile#1 and Mobile#2 move from their home networks to the same foreign networks.

Scenario 1.3.3.3: Mobile#1 moves from its home network to a foreign network while Mobile#2 moves from a foreign network to another foreign network.

Scenario 1.3.3.4: Mobile#1 moves from its home network to a foreign network (visited network #1) while Mobile#2 moves from a foreign network to visited network #1

Scenario 1.3.3.5: Mobile#1 moves from its home network to a foreign network (visited network #1) while Mobile#2 moves from visited network #1 to a foreign network.

Scenario 1.3.3.6: Mobile#1 moves from its home network to a foreign network (visited network #1) while Mobile#2 moves from visited network #1 to its home network.

Scenario 1.3.3.7: Mobile#1 moves from its home network to a foreign network (visited network #1) while Mobile#2 moves from visited network #1 to Mobile#1 home network.

 © 1999 EURESCOM Participants in Project P912-PF

Scenario 1.3.3.8: Both Mobile#1 and mobile#2 move from a foreign network (visited network #1) to another foreign network (visited network #2).

Scenario 1.3.3.9: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #2 to visited network #1.

Scenario 1.3.3.10: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #1 to its home network.

Scenario 1.3.3.11: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #2 to its home network.

Scenario 1.3.3.12: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #1 to Mobile#1 home network.

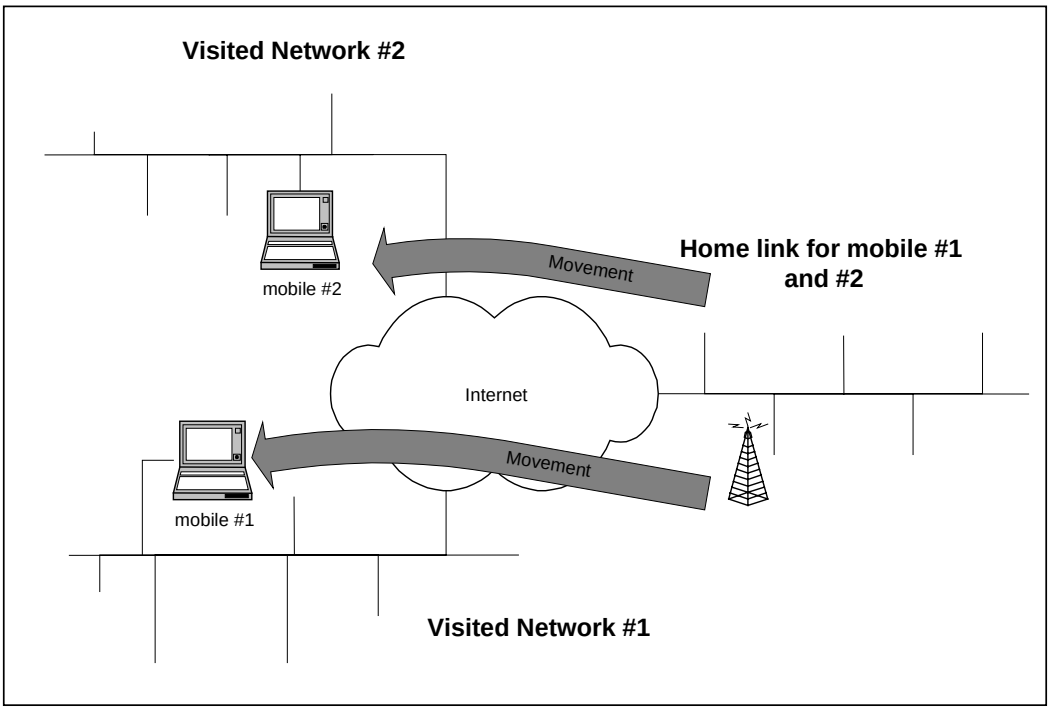
Scenario 1.3.3.13: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #2 to Mobile#1 home network.

Scenario 1.3.3.14: Both Mobile#1 and mobile#2 move from a foreign network (visited network #1) to Mobile#1 home network.

Scenario 1.3.3.15: Both Mobile#1 and mobile#2 move from a foreign network (visited network #1) to Mobile#2 home network.

A1.4 Communication between two mobiles of the same home network

A1.4.1 static/static

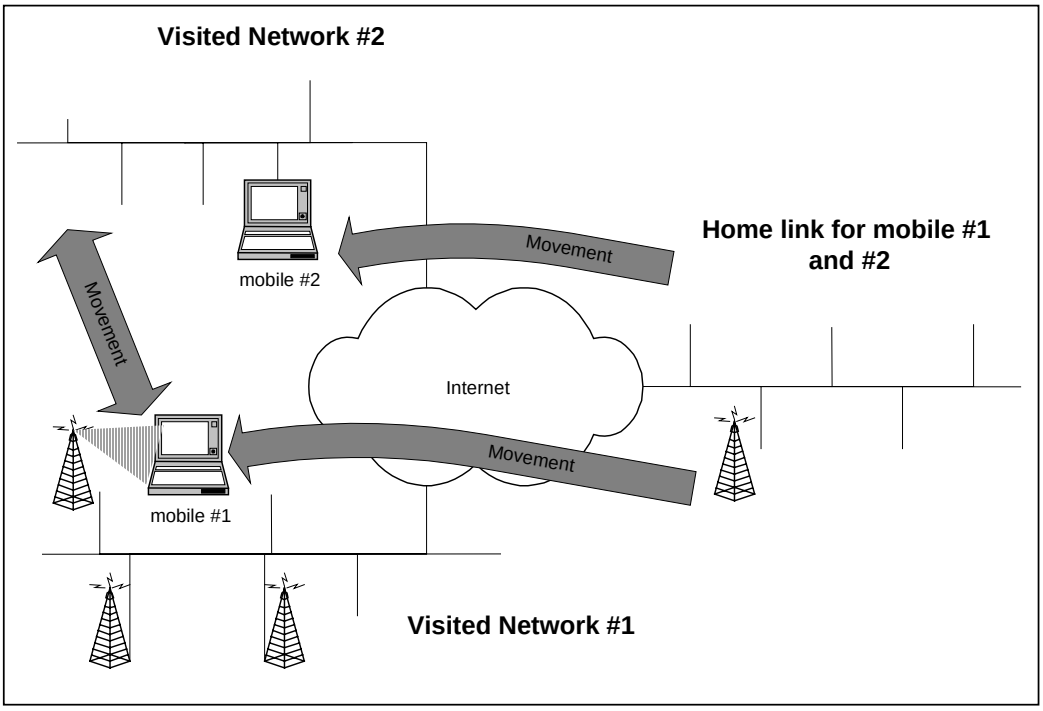


Scenario 1.4.1.1: Both mobiles are on the same foreign network.

Scenario 1.4.1.2: Both mobiles are on different foreign networks.

Scenario 1.4.1.3: Mobile #1 is visiting a foreign network while Mobile#2 is on its home network.

A1.4.2 dynamic/static



Scenario 1.4.2.1: Mobile#1 moves from its home network to a foreign network while Mobile#2 is on another network.

Scenario 1.4.2.2: Mobile#1 moves from its home network to a foreign network while Mobile#2 is on the same visited network.

Scenario 1.4.2.3: Mobile#1 moves from its home network to a foreign network while Mobile#2 is on Moible#1 home network.

Scenario 1.4.2.4: Mobile#1 moves from its home network to a foreign network while Mobile#2 is on its own home network.

Scenario 1.4.2.5: Mobile#1 moves from a foreign network to another foreign network while Mobile#2 is on another network.

Scenario 1.4.2.6: Mobile#1 moves from a foreign network (visited net #1) to another foreign network (visited net #2) while Mobile#2 is on visited network #1.

Scenario 1.4.2.7: Mobile#1 moves from a foreign network (visited net #1) to another foreign network (visited net #2) while Mobile#2 is on visited network #2.

Scenario 1.4.2.8: Mobile#1 moves from a foreign network to another foreign network while Mobile#2 is on home network.

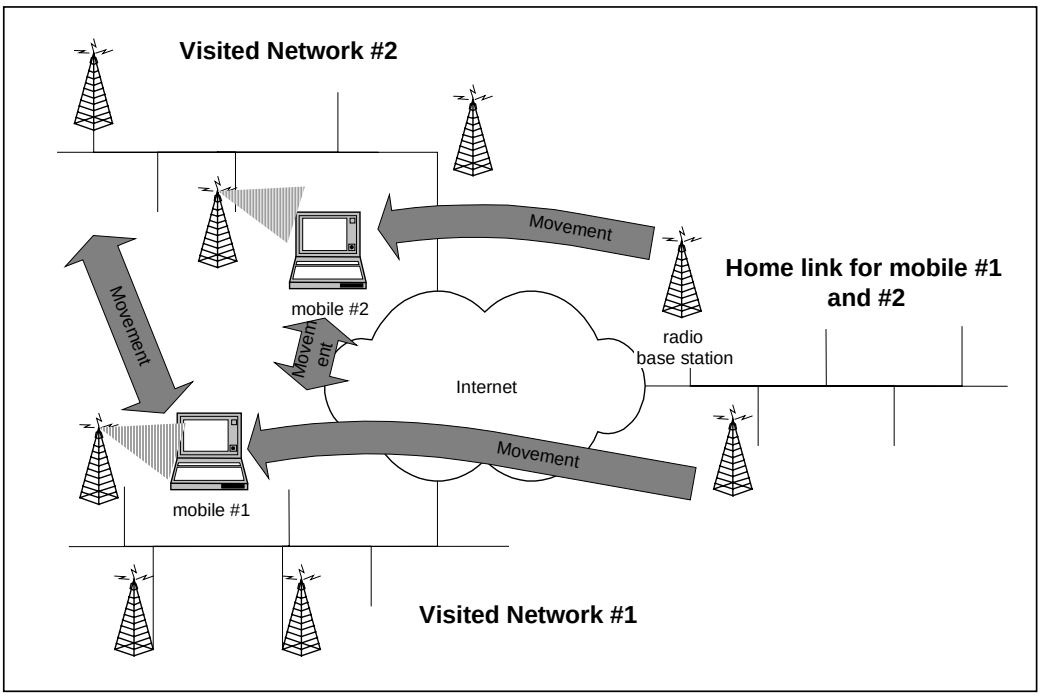
Scenario 1.4.2.9: Mobile#1 moves from a foreign network to its home network while Mobile#2 is on another network.

 © 1999 EURESCOM Participants in Project P912-PF

Scenario 1.4.2.10: Mobile#1 moves from a foreign network (visited net #1) to its home network while Mobile#2 is on visited network #1.

Scenario 1.4.2.11: Mobile#1 moves from a foreign network to home network while Mobile#2 is on home network.

A1.4.3 dynamic/dynamic



Scenario 1.4.3.1: Mobile#1 and Mobile#2 move from their home networks to two different foreign networks.

Scenario 1.4.3.2: Mobile#1 and Mobile#2 move from their home networks to the same foreign networks.

Scenario 1.4.3.3: Mobile#1 moves from home network to a foreign network while Mobile#2 moves from a foreign network to another foreign network.

Scenario 1.4.3.4: Mobile#1 moves from home network to a foreign network (visited network #1) while Mobile#2 moves from a foreign network to visited network #1.

Scenario 1.4.3.5: Mobile#1 moves from home network to a foreign network (visited network #1) while Mobile#2 moves from visited network #1 to a foreign network.

Scenario 1.4.3.6: Mobile#1 moves from home network to a foreign network (visited network #1) while Mobile#2 moves from visited network #1 to home network.

Scenario 1.4.3.7: Both Mobile#1 and Mobile#2 move from a foreign network (visited network #1) to another foreign network (visited network #2).

Scenario 1.4.3.8: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #2 to visited network #1.

Scenario 1.4.3.9: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #1 to home network.

Scenario 1.4.3.10: Mobile#1 moves from a foreign network (visited network #1) to another foreign network (visited network #2) while Mobile#2 moves from visited network #2 to its home network.

Scenario 1.4.3.11: Both Mobile#1 and mobile#2 move from a foreign network to home network.

 © 1999 EURESCOM Participants in Project P912-PF

Appendix 2: Detailed description of selected mobility scenarios and respective threat analysis

This appendix provides a more detailed description of dynamic mobility scenarios 1.2.2.2 and 1.2.3.2 identified in Appendix 1, and provides a threat analysis for each of these scenarios**.** These two scenarios have been selected for inclusion in this appendix because they were considered as the most representative mobility scenarios identified in Appendix 1. These scenarios are illustrated below in Figure A2.1.

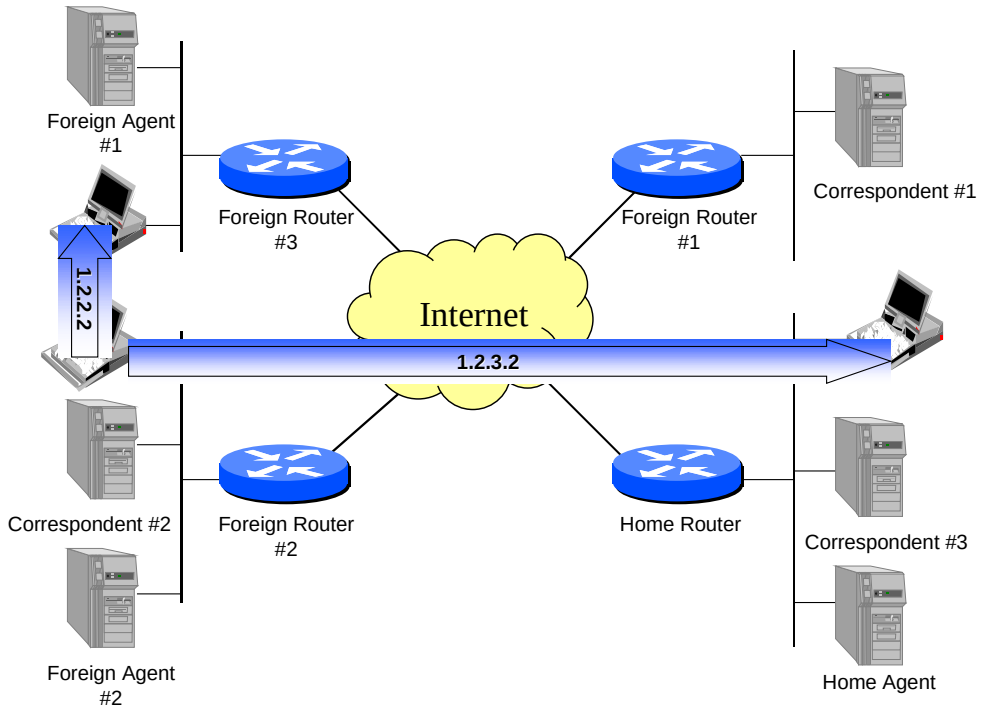


Figure A2.1 Mobility scenarios 1.2.2.2 and 1.2.3.2

This figure illustrates all of the entities in the scenario. The routers are assumed to include firewalls. In MobileIPv6, there are no foreign agents, which is reflected in the Message Sequence Chart (IPv6).

A.2.1 Scenario 1.2.2.2

A2.1.1 Description of the scenario

The mobile is on a foreign network. The mobile starts a communication with correspondent #1 (see Figure A1.2.2.2 in Appendix 1), then the mobile moves to another foreign network.

The scenario starts with the mobile connected to Visited Network #1, registered with its home agent and having a care-of address (either that of the foreign agent or a co-located one).

The mobile then starts communicating with correspondent #1 (on another foreign network), #2 (on the visited network to which the mobile is connected) or #3 (on the

mobile's home network). After that the mobile moves to another foreign network and communication continues.

The analysis assumes that both the visited networks and the home network are using Ethernet at the link-layer. For IPv4, it is also assumed that both foreign agent and router Ethernet addresses are already in the mobile node's ARP cache, that the home agent uses Gratuitous and Proxy ARP to intercept the packets destined for the mobile node and that the home router knows the home agent's Ethernet address. For IPv6, it is assumed that both foreign agent and router Ethernet addresses have been discovered using Neighbour Discovery, that the home agent uses Neighbour Discovery to intercept packets destined for the mobile node and that the home router knows the home agent's Ethernet address.

A2.1.2 IPv4 environment

In this scenario:

- the mobile node is registered (either with a co-located care-of-address, or via a foreign agent) on a foreign network;
- the mobile node starts sending packets to correspondent #1 (which is located on a foreign network not previously visited by the mobile node). These packets are routed directly (through the gateway on the foreign link);
- the mobile node detects that it has moved to another foreign network either using the ICMP Router Advertisement Lifetime field, or by observing a change in the Agent Advertisement network-prefix;
- the mobile node registers a new care-of-address with its home agent (either using a co-located care-of-address or the services of a foreign agent);
- the mobile node continues sending packets to correspondent #1. Sending the first packet may involve ARPing for the router's Ethernet address.

A2.1.3 IPv6 environment

In this scenario:

- the mobile node is registered (with a co-located care-of-address) on a foreign network;
- the mobile node starts sending packets to correspondent #1 (which is located on a foreign network not previously visited by the mobile node). These packets are routed directly (through the gateway on the foreign link);
- the mobile node detects that it has moved to another foreign network by comparing the network-prefixes contained in received Router Advertisements with its home address network-prefix and previouly received Router Advertisement network-prefixes;
- the mobile node obtains a new care-of-address using either stateful or stateless address autoconfiguration;
- the mobile node sends a binding update to its home agent (using the new co-located care-of-address);

 © 1999 EURESCOM Participants in Project P912-PF

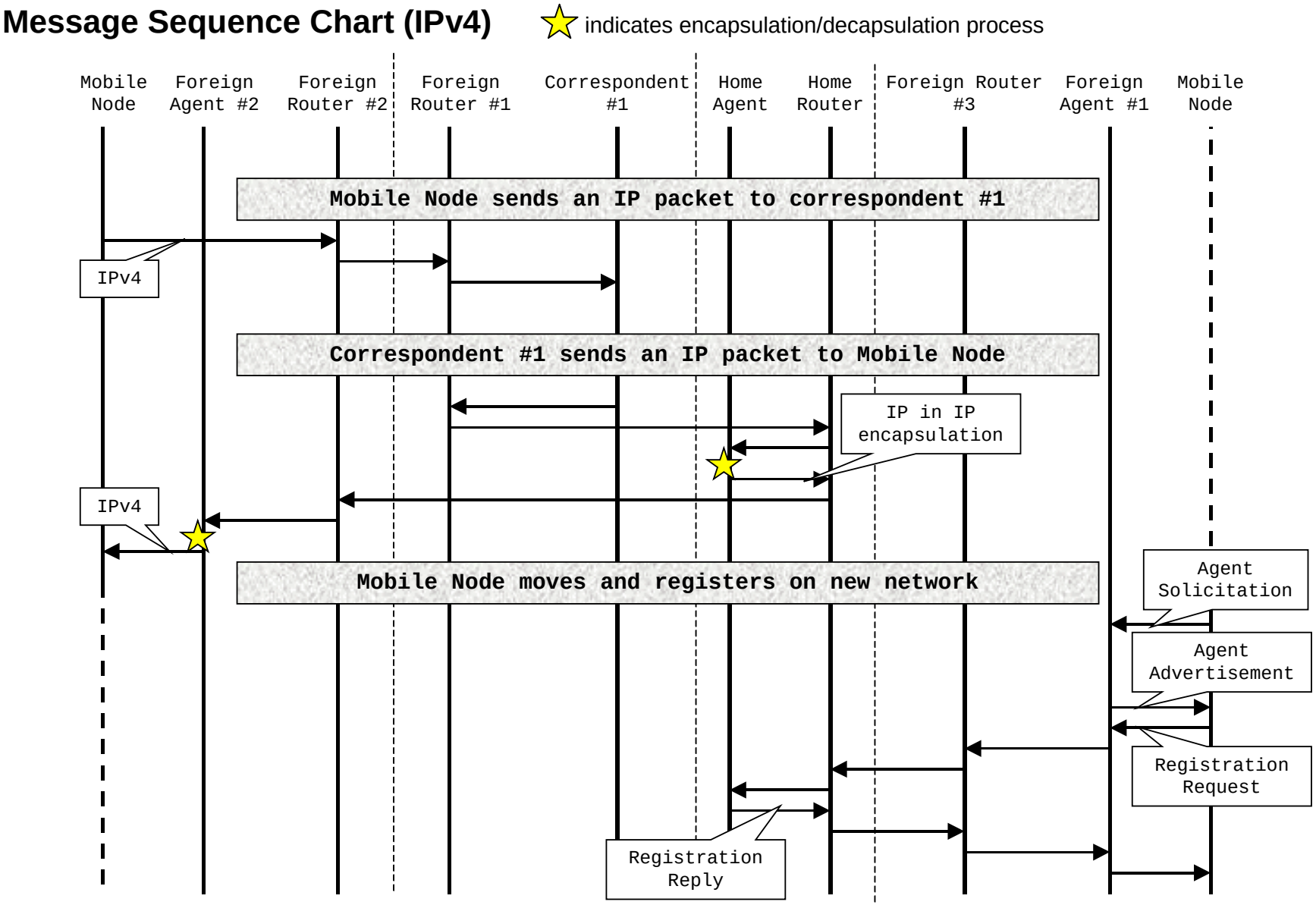
- the mobile node continues sending packets to correspondent #1. The mobile node can select any router on the foreign link from which it has received Router Advertisements.

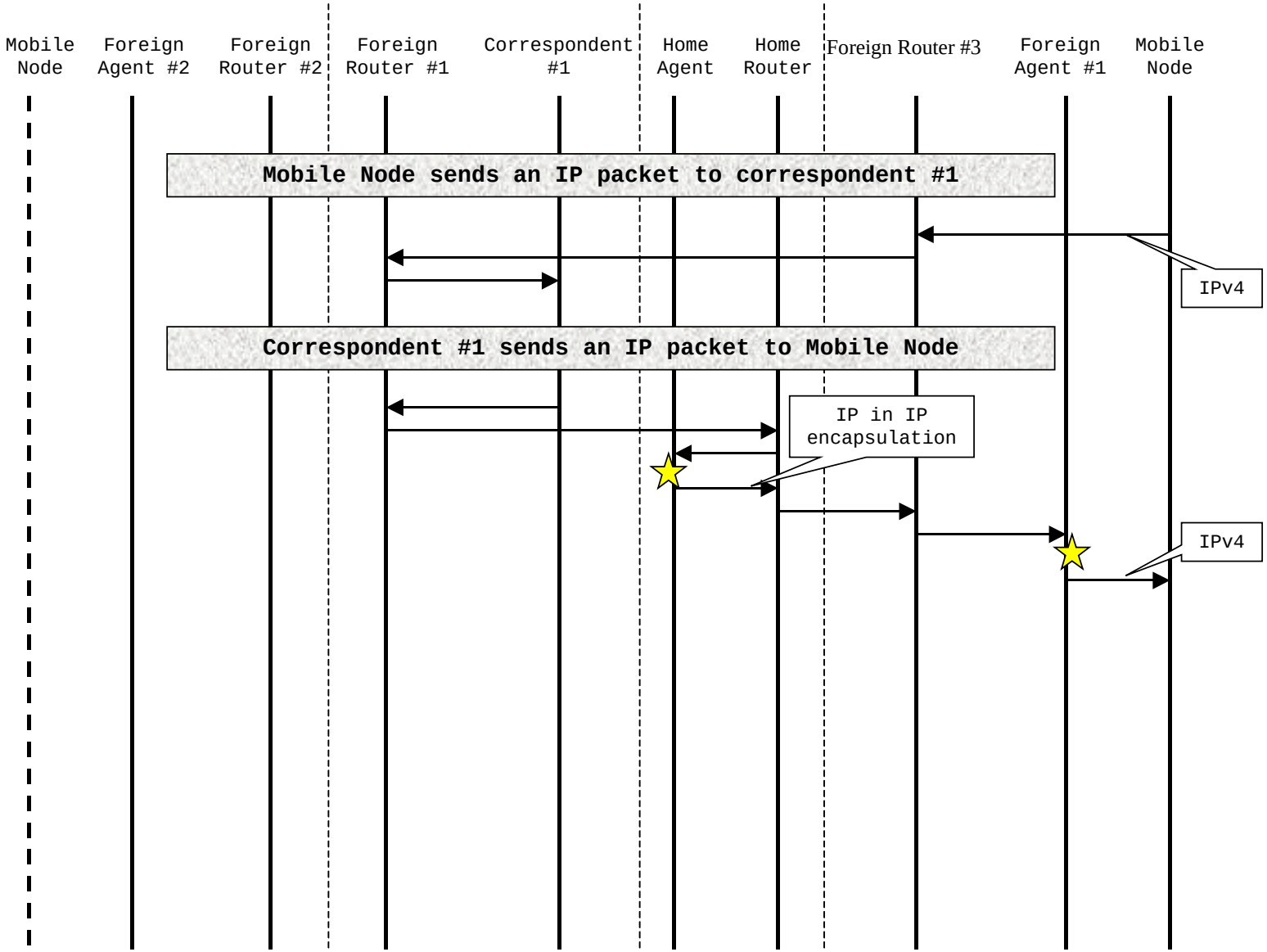
A2.1.4 Threat analysis

Threats to elements in this scenario include:

- Spoofing of mobile-node
- Spoofing of foreign-agent
- Loss of confidentiality of transmitted data packets
- Corruption of transmitted data packets
- Denial of service to mobile node
- Newly visited foreign network compromises the security of the mobile node
- Mobile node compromises the security of the visited network

A2.1.5 MSC for scenario 1.2.2.2

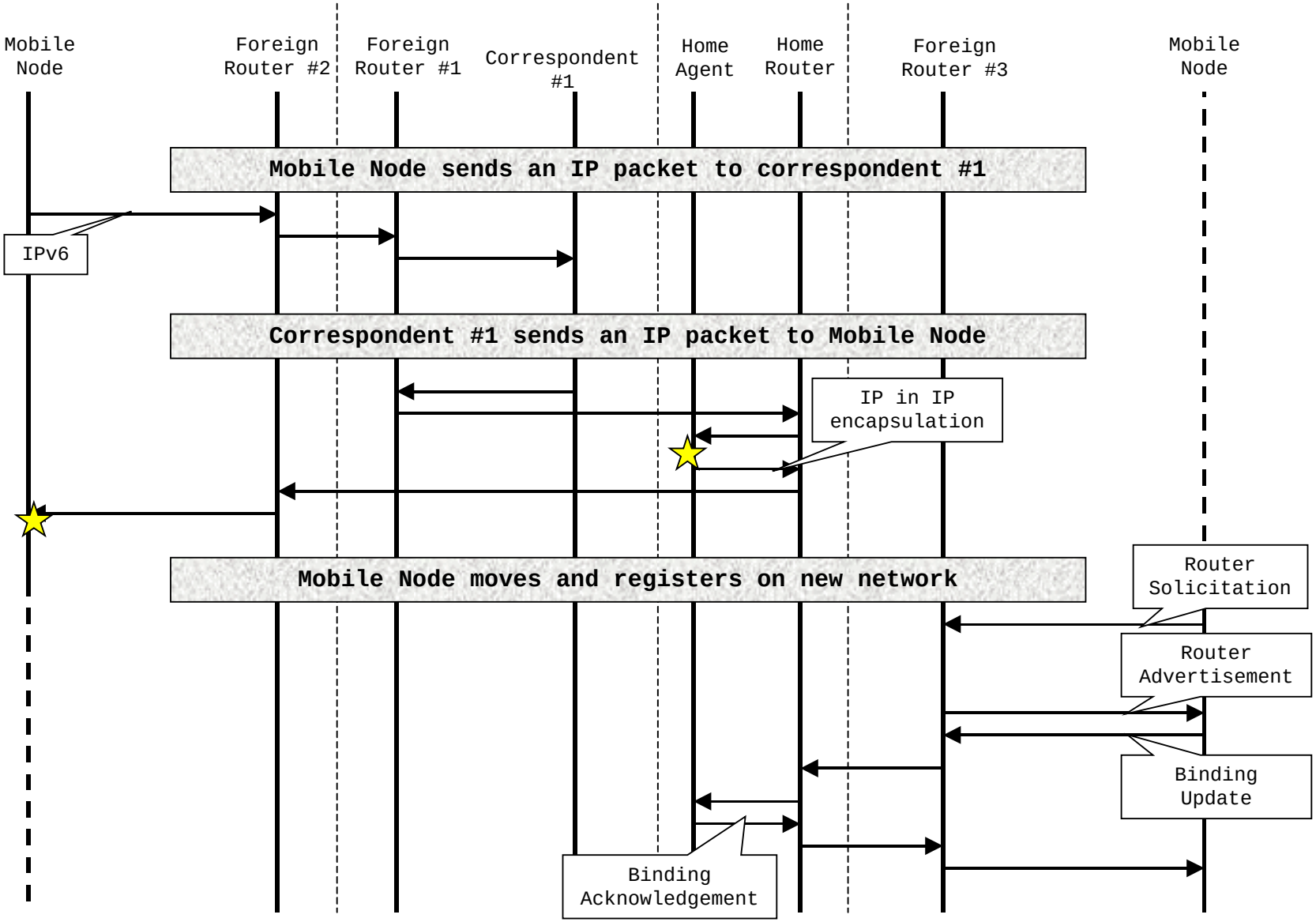


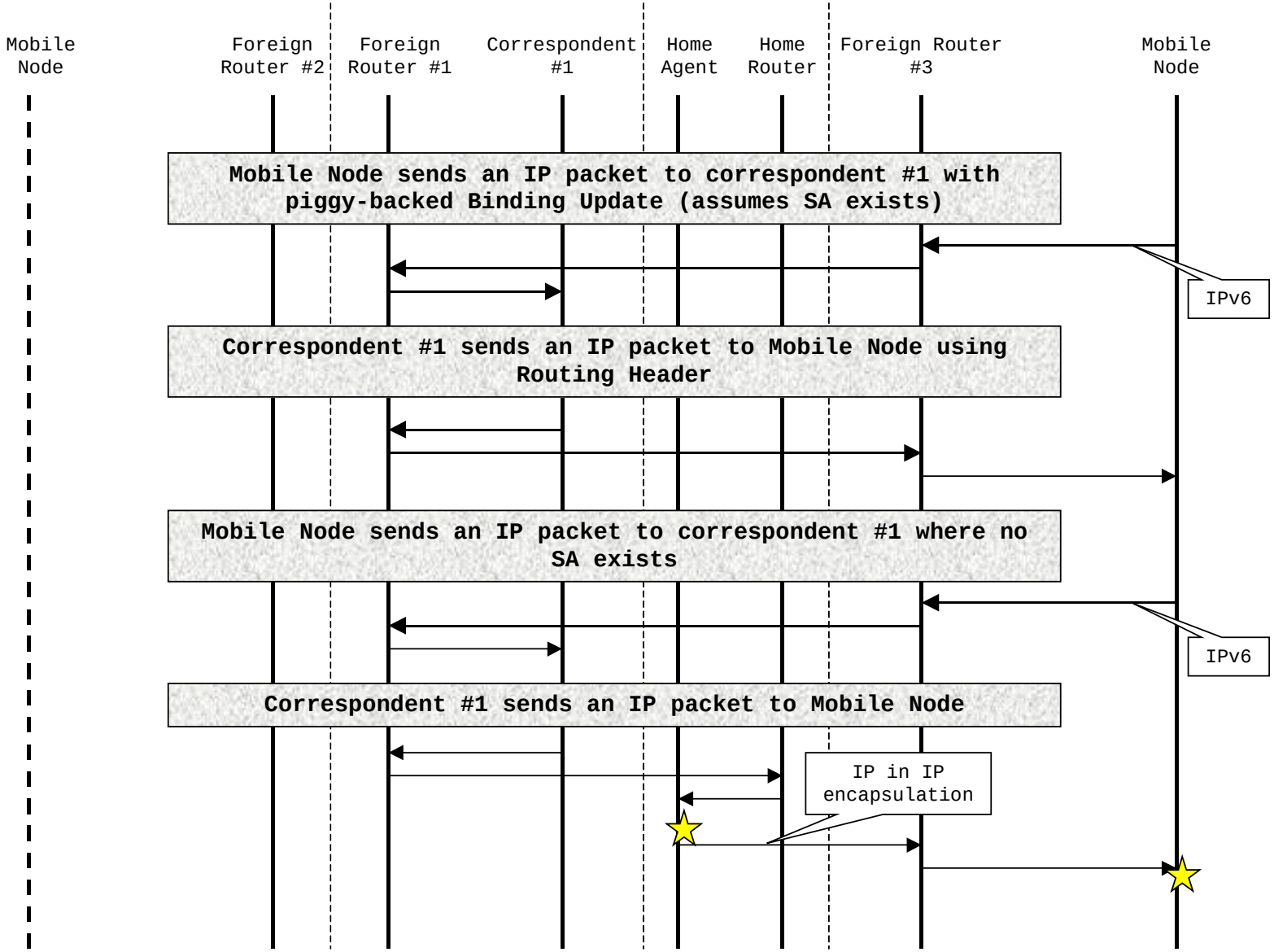


© 1999 EURESCOM Participants in Project P912-PF

Message Sequence Chart (IPv6)

indicates encapsulation/decapsulation process





 © 1999 EURESCOM Participants in Project P912-PF

A2.2 Scenario 1.2.3.2

A2.2.1 Description of the scenario

The mobile is on a foreign network. The mobile starts a communication with correspondent #1 (see Figure A1.2.3.2 in Appendix 1), then the mobile moves to its home network.

The scenario starts with the mobile connected to Visited Network #1, registered with its home agent and having a care-of address (either that of the foreign agent or a co-located one).

The mobile then starts communicating with correspondent #1 (on another foreign network), #2 (on the visited network to which the mobile is connected) or #3 (on the mobile's home network). After that the mobile moves to its home network and communication continues.

The analysis assumes that both the visited networks and the home network are using Ethernet at the link-layer. For IPv4, it is also assumed that both foreign agent and router Ethernet addresses are already in the mobile node's ARP cache, that the home agent uses Gratuitous and Proxy ARP to intercept the packets destined for the mobile node and that the home router knows the home agent's Ethernet address. For IPv6, it is assumed that both foreign agent and router Ethernet addresses have been discovered using Neighbour Discovery, that the home agent uses Neighbour Discovery to intercept packets destined for the mobile node and that the home router knows the home agent's Ethernet address.

A2.2.2 IPv4 environment

1 The mobile node is registered with the home agent with the foreign address (either a co-located one, or via the foreign agent).

2.1 The mobile sends packets to correspondent #1. These packets are routed directly (through the gateway on the foreign link).

2.2 Packets sent by correspondent #1 arrive at the home agent and are tunnelled to the mobile through the tunnel. They are de-tunnelled by either the mobile or the foreign agent. In the latter case they are delivered from the foreign agent to the mobile.

3 The mobile moves to the home network.

4.1 The mobile was powered off.

4.2 The mobile was not powered off. Move detection by lifetime expiry.

4.3 The mobile was not powered off. Move detection by network prefix.

5 The mobile re-configures its Ethernet interface to its home address and flushes the ARP cache. The mobile then issues a gratuitous ARP request. The routers, the home agent and the hosts on the link update their ARP cache.

6 The mobile may receive an ARP reply from the home agent. In this case the mobile probably issues an error message.

7 The mobile de-registers with its home agent. The home agent removes the mobile's care-off address from its binding list.

8 Packets to correspondent #1 are routed directly through the home link's router. Sending the first packet involves ARPing for the routers Ethernet address.

9 Packets from correspondent#1 are received via the router.

A2.2.3 IPv6 environment

1 The mobile node is registered with the home agent with a co-located care-of-address.

2.1 The mobile sends packets to correspondent #1. These packets are routed directly (through the gateway on the foreign link).

2.2 Packets sent by correspondent #1 arrive at the home agent and are tunnelled to the mobile through the tunnel. They are de-tunnelled by the mobile.

3.1 The mobile detects the tunnelling and sends a binding update to the correspondent.

3.2 The correspondent may acknowledge with a binding ack.

3.3 Packets sent by the correspondent to the mobile are routed directly to the mobile.

4 The mobile moves to the home network.

5 The mobile was not powered off. Move detection by network prefix.

6.1 The mobile reconfigures its Ethernet interface and (if move detection was not by receiving a router advertisement) issues a neighbour solicitation to find a router.

6.2 The router answers with a router advertisement.

7.1 The mobile may optionally start home agent discovery by sending a binding update to the home agent anycast address.

7.2 This is rejected, but the response contains the unicast addresses of the home agent(s).

8.1 The mobile sends a Binding Update to the Home Agent.

8.2 The Binding Update is Acked by the Home Agent.

9.1 The mobile sends a Binding Update to correspondent #1.

9.2 Correspondent #1 may Ack the Binding Update.

10.1 Packets sent from Mobile to Correspondent #1 are routed directly.

10.2 Packets sent from Correspondent #1 to the Mobile are routed directly.

A2.2.4 Threat Analysis

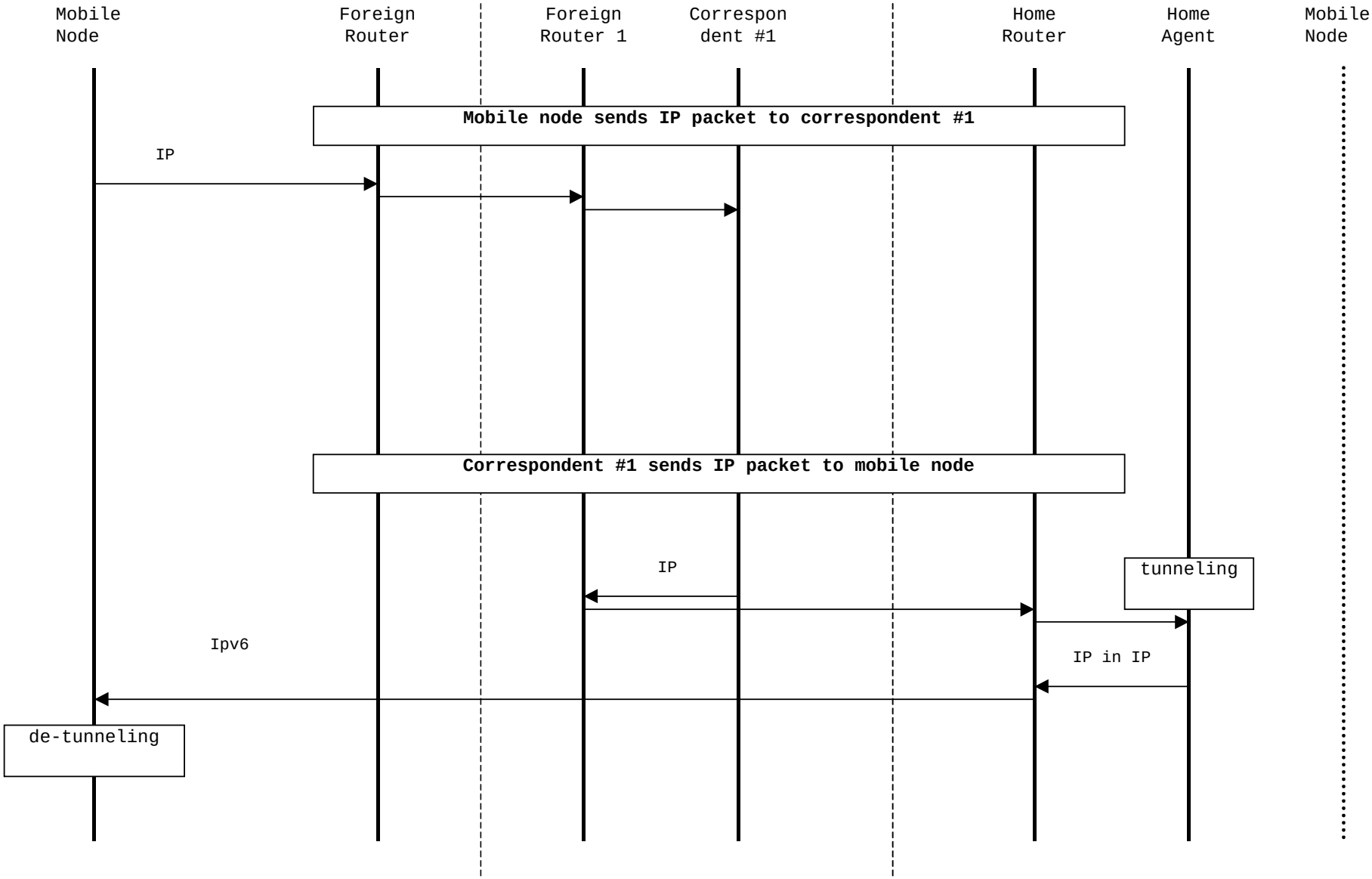
All usual IP-threats apply. Additionally:

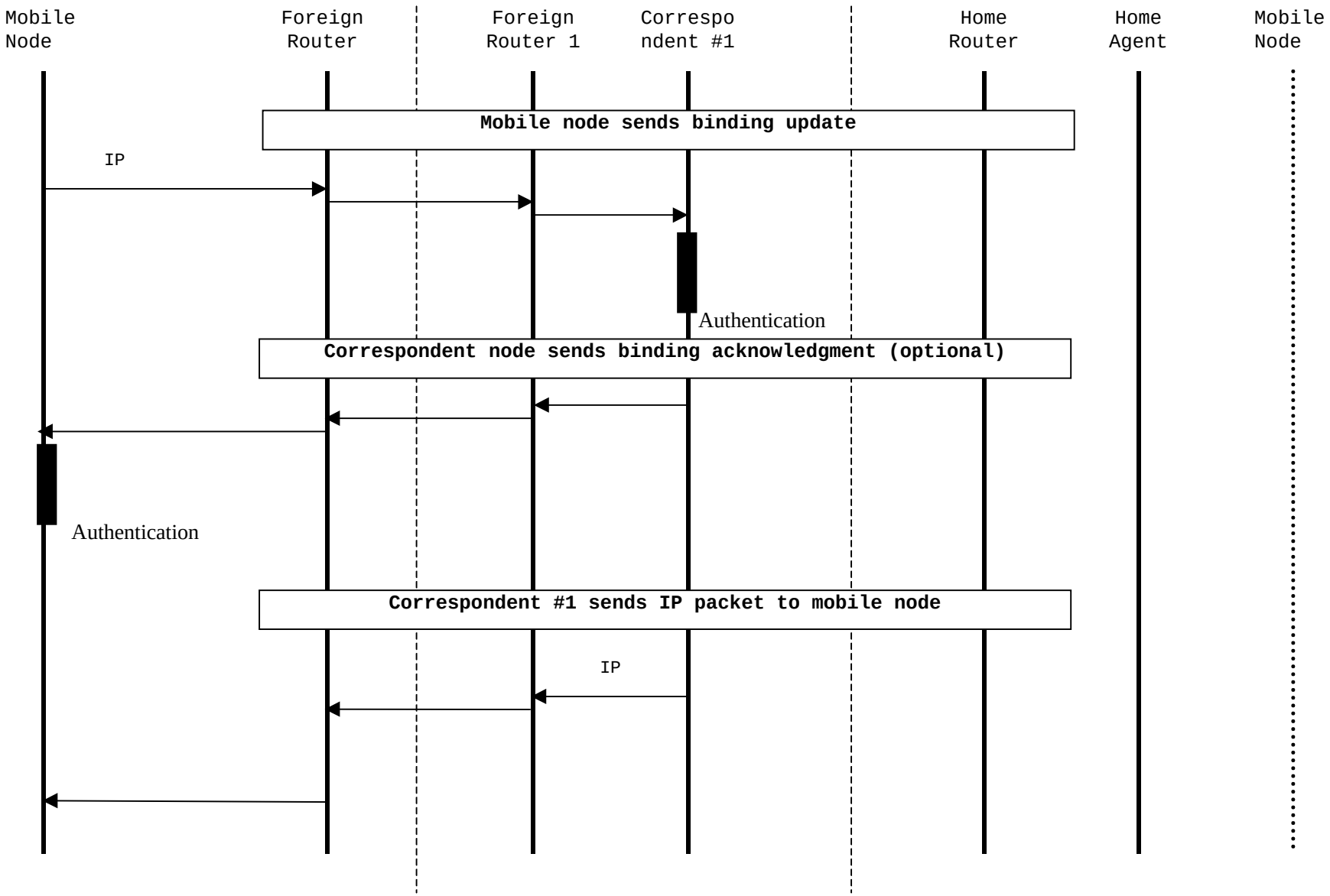
- Loss of confidentiality of packets. This is especially a problem with scenario 1.2.3.3, because correspondent #3 could falsely assume, that it is corresponding with a local node (which may be trusted more than nodes outside the home network). This assumption can also compromise higher level protocols.

 © 1999 EURESCOM Participants in Project P912-PF

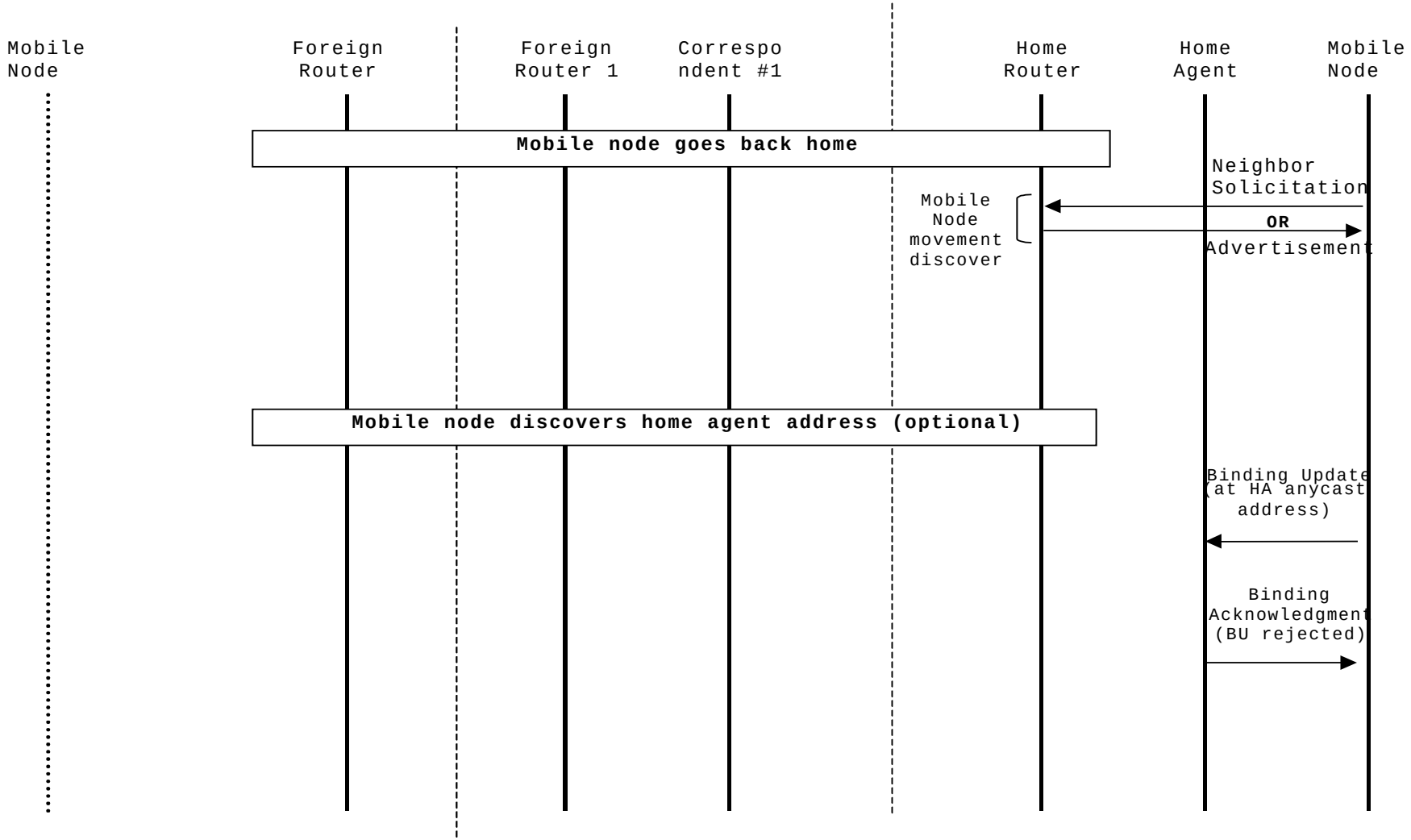
- Loss of security features provided by the home network. Usually networks are secured by a firewall. Because the mobile node is now physically outside the home network, it is more vulnerable to attacks which are otherwise prevented by the home firewall (especially denial of service attacks and spoofing).
- Session stealing on the foreign link.
- Denial of service of the mobile node.
- Denial of service of the home agent.

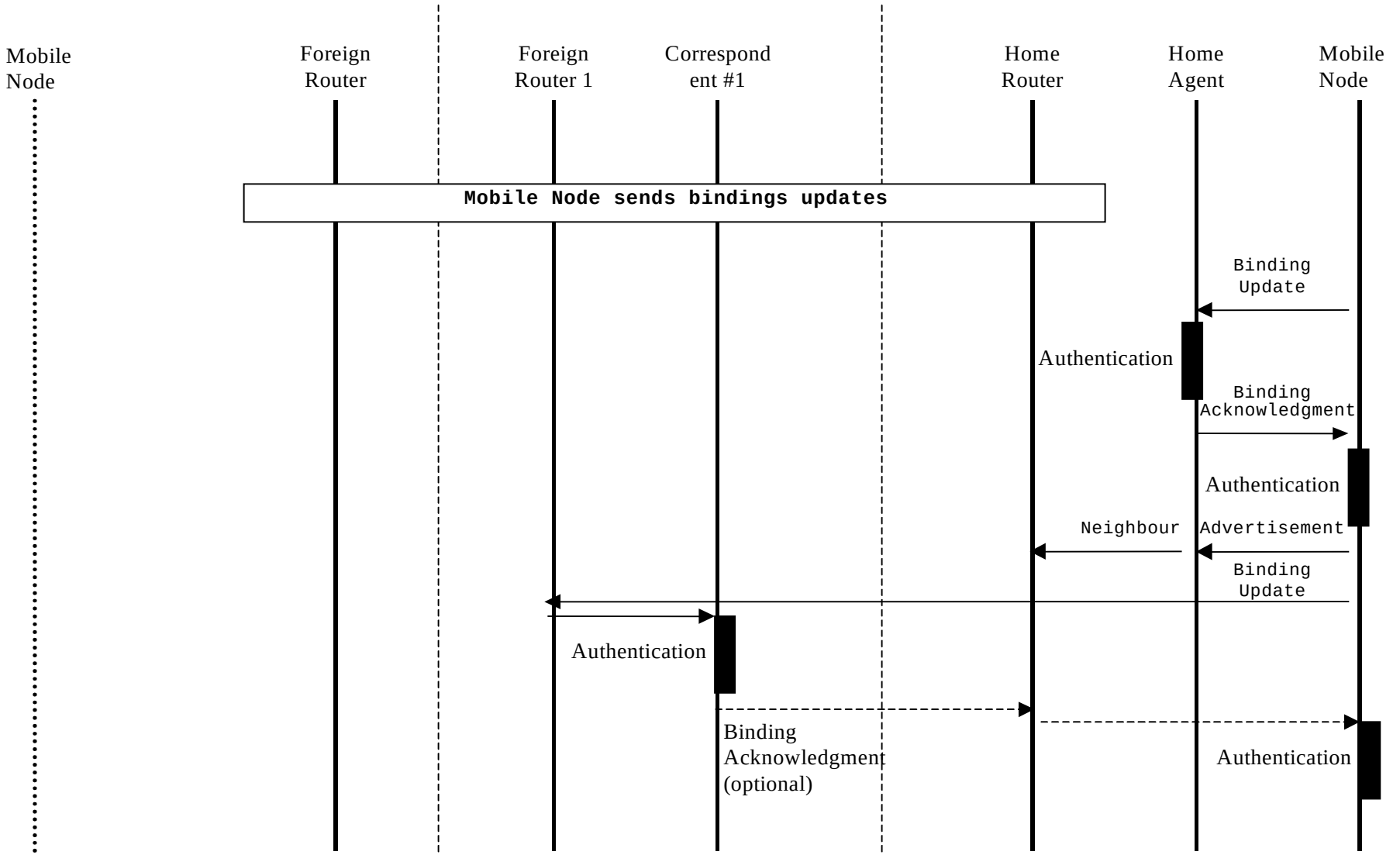
A2.2.5 MSC for scenario 1.2.3.2



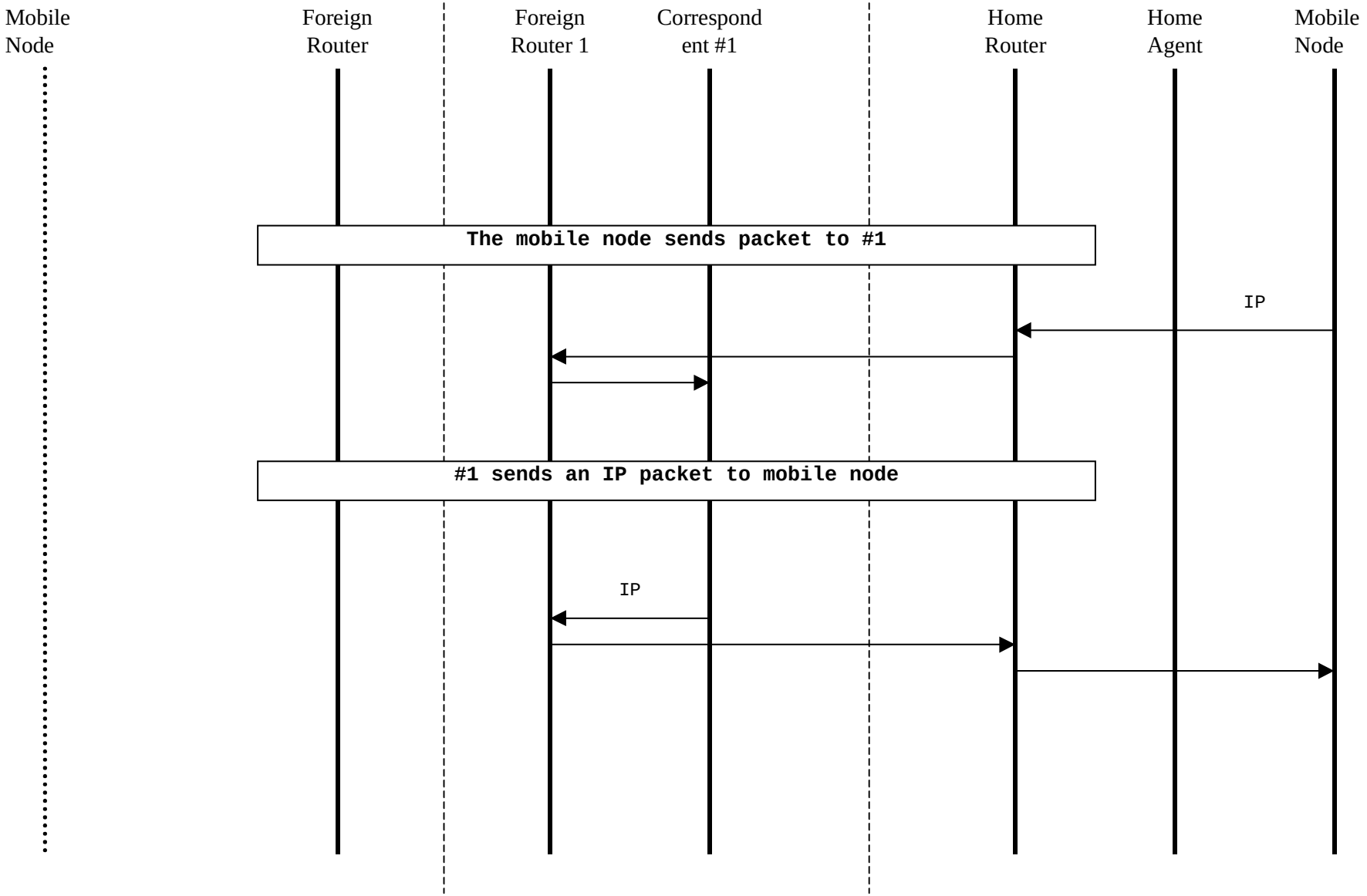


 © 1999 EURESCOM Participants in Project P912-PF


Mobile Node
Foreign Router
Foreign Router 1
Correspo ndent #1
Home Router
Home Agent
Mobile Node
Mobile node goes back home
Neighbor Solicitation
Mobile Node movement discover
OR
Advertisement
Mobile node discovers home agent address (optional)
Binding Update (at HA anycast address)
Binding Acknowledgment (BU rejected)



 © 1999 EURESCOM Participants in Project P912-PF


Mobile Node
Foreign Router
Foreign Router 1
Correspondent #1
Home Router
Home Agent
Mobile Node
The mobile node sends packet to #1
IP
#1 sends an IP packet to mobile node
IP

Appendix 3 - Risk Assessment Details

A3.1 Detailed description of risk assessment criteria

A3.1.1 Equipment required

Hardware and/or software needed to realise threats.

Price

How much money is needed to acquire the devices required to attack?

Highest : Free

High : < €10,000

Normal : €10,000 < €1,000,000

Low : > €1,000,000

Lowest : Unavailable at any price

Availability

How easy is it to acquire the devices?

Highest : Globally available

Medium : Restricted availability (e.g. Local availability, availability to specific or restricted social groups)

Low : Unavailability

A3.1.2 Knowledge required

Level of study needed to use the equipment or perform an attack.

Highest : No study required

Medium : Several years of study required

Low : Many years of study required

A3.1.3 Time required

How much time is required to carry out the attack?

Time to prepare the attack

Highest : Hours are required to prepare the attack

High : Days are required to prepare the attack

Medium : Weeks are required to prepare the attack

Low : Years are required to prepare the attack

Time to perform the attack

Highest : Seconds are required to perform the attack

High : Hours are required to perform the attack

 © 1999 EURESCOM Participants in Project P912-PF

Medium : Days are required to perform the attack

Low : Years are required to perform the attack

A3.1.4 Location required

Mobility facilities may create new locations from which to perform attacks.

High : Attack can be performed from anywhere

Medium : The attack can only be performed from specific locations

Low : The attack can only be performed from protected locations

A3.1.5 Time-window required

How many periods of time are there in one day/month/year in which to make a succesful attack, and how long are they?

Number of periods of time

High : Many periods per hour

Medium : A few periods per hour

Low : One period per day

Length of period of time

High : Length of period is one minute or more

Medium : Length of period is a few seconds

Low : Length of period is less than one second

A3.1.6 Number of possible targets

How many network nodes or services can be affected by an attack?

High : One attack can affect one or more services or a large number of network nodes

Medium : One attack can affect a small number of network nodes

Low : One attack has no critical consequences on services or network nodes

A3.1.7 Time to recover

What is the impact of the damage from a technical point of view? How much time is a system out of service as a result of the attack?

Highest : The system never recovers.

High : The system recovers after more than one day

Medium : The system recovers after more than one hour

Low : The system recovers after more than five minutes

Lowest : The system recovers after less than five minutes

A3.1.8 Difficulty of detecting an attack

How difficult is it to detect an attack?

High : Impossible to detect (e.g. eavesdropping)

Medium : Network monitoring has to be performed in order to detect an attack

Low : The attack provides modifications that are immediately obvious.

A3.1.9 Difficulty of identifying the attacker

How difficult is it to identify the attacker?

High : It is very complicated and it is necessary to use a lot of resources

Medium : Identification is possible using few resources

Low : Identification is possible using automatic tools

A3.1.10 Type of access required

What class of privileges/rights (user administrator, ordinary user, etc.) must the attacker have?

High : All public and anonymous users can perform the attack

Medium : Only users with identified rights can perform the attack

Low : Only privileged users can perform the attack

A3.2 Threat/Risk Matrices for Mobile IPv4 and Mobile IPv6

A3.2.1 Eavesdropping IPv4

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
E1	***H***	M	H	H	H	n/a[3]	*l*[4]	H[5]	H	H
E2	***H***	M	H	l	H[2]	n/a[3]	*l*[4]	H[5]	M	H
E3	***H***	M	H	H,l[1]	H[2]	n/a[3]	*l*[4]	H[5]	M	H
E4	***H***	M	H	H	H	n/a[3]	*l*[4]	H[5]	H	H

1. Depends on the location of the CN. In the worst case, the risk is the same as on a traditional Internet connection.
2. the risk is the same as on a traditional Internet connection.
3. eavesdropping is not related to a host but to a connection.
4. eavesdropping does not affect system functions.
5. intrusion detection is more difficult on a foreign network because of the lack of administration tools.

 © 1999 EURESCOM Participants in Project P912-PF

A3.2.2 Eavesdropping IPv6

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
E2	***H***	M	H	H	H[1]	n/a[2]	*l*[3]	H	H	H
E3	***H***	M	H	H	H[1]	n/a[2]	*l*[3]	H	H	H

1. the risk is the same as on a traditional Internet connection.
2. eavesdropping is not related to a host but to a connection.
3. eavesdropping does not affect system functions.

A3.2.3 Session Stealing IPv4

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
S1	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]
S2	l	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]
S3	H,***H***	M	***H***,***H***	M	H,H	H[2]	n/a[3]	L	H	H
S4	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]	n/a[4]

1. Because of the low risk for criterion C1, there is no sense to assign risks to the other criteria
2. This depends on the actual application. Worst case assumed.
3. This can be answered only with a concrete application in mind.
4. Taking over the communication between the given two entities does not give the intruder anything beyond eavsdropping.

It is assumed that reverse tunnelling is used because this makes session stealing easier.

A3.2.4 Session Stealing IPv6

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
S2	l	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]	n/a[1]
S3	H,***H***	M	***H***,***H***	M	H,H	H[2]	n/a[3]	L	H	H

This analysis does not differ from IPv4.

A3.2.5 DoS/Flooding IPv4

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
DF-MN	H, ***H***	M	***H, H***	H	H, H	L	*l*	M[1]	H/L[2]	H
DF-CN	H, ***H***	M	***H, H***	H	H, H	L	*l*	M[1]	H/L[2]	H
DF-FA	H, ***H***	M	***H, H***	H	H, H	M	M	M[1]	H/L[2]	H
DF-HA	H, ***H***	M	***H, H***	H	H, H	M	M	M[1]	H/L[2]	H

1. Most simple DoS or Flooding attacks are easily detectable, but other more sophisticated attackts might be harder to discover.
2. This will depend on the specific attack that has been used. Simple flooding attacks might be easy to trace, while more sophisticated attacks are more or less untraceable.

A3.2.6 DoS/Flooding IPv6

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
DF-MN	H, ***H***	M	***H, H***	H	H, H	L	*l*	M[1]	H/L[2]	H
DF-CN	H, ***H***	M	***H, H***	H	H, H	L	*l*	M[1]	H/L[2]	H
DF-FA	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
DF-HA	H, ***H***	M	***H, H***	H	H, H	M	M	M[1]	H/L[2]	H

This is the same as for the IPv4 environment, the only difference being that the Foreign Agent does not exist in IPv6.

1. Most simple DoS or Flooding attacks are easily detectable, but other more sophisticated attackts might be harder to discover.
2. This will depend on the specific attack that has been used. Simple flooding attacks might be easy to trace, while more sophisticated attacks are more or less untraceable.

A3.2.7 Spoofing IPv4

	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
SP-MN	*l*[1],L	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
SP-CN	H[2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
SP-FA	H[3],***H***	M	***H,H***	L	M,H	H	H	M	H	M
SP-HA	*l*[1],L	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

1. Due to the low risk for C1, this threat will not be treated further here.
2. This threat is not MobileIP specific and will not be treated further here.
3. This risk assumes that the Mobile-Foreign Authentication Extension is not used to secure this link. All other risk assessments for this threat assume a ‘worst-case’ scenario.

A3.2.8 Spoofing IPv6

Threat	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10
SP-MN	*l*[1],L	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
SP-CN	H[2]	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
SP-HA	*l*[1],L	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

1. Due to the low risk for C1, this threat will not be treated further here.

This threat is not MobileIP specific and will not be treated further here.

 © 1999 EURESCOM Participants in Project P912-PF