INTERNET Draft
Expires: August 2002

Hesham Soliman,
Mattias Pettersson
Ericsson

MObile Networks (MONET) problem statement and scope
<draft-soliman-monet-statement-00.txt>

Status of this memo

Abstract

This draft illustrates some of the problems that need to be addressed in order to provide an optimal mobility management mechanism for mobile networks consisting of a mobile router and a number of IPv6 hosts. The reader shall refer to a separate document[TERMINOLOGY] for the terminology used in this draft, while a list of proposed requirements can be found in [REQUIREMENTS]

1. Introduction and motivation

The MObile Networks (MONET) problem stated in this document addresses a network consisting of a Mobile Router (MR) with a number of devices attached to it. Such network may change its attachment point within the Internet due to physical mobility or changes in the topology. The mechanisms required for handling such mobility are currently lacking or non-existent within the IETF standards.
Some of these required mechanisms are mentioned in this draft to illustrate the need for solutions.

Several mobility scenarios exist for mobile networks depending on the size of the mobile network and its administrative charcteristics. These scenarios are subdivided in this document. The commonalities and differences between them are addressed.

The solutions for most of the MONET issues below are affected by:

- The size of the mobile network.
- The administrative characteristics of such MONETs. Ie. Whether MNNs and MRs are administered/owned by the same entity. These characteristics will affect the types of issues that need to be solved and the level of trust that can be assumed.

The issues associated with each of the scenarios above are shown below. For each issue some consideration of the two influences above is mentioned.

2. Types of Mobile Networks

This chapter will discuss two different types of mobile networks by illustrating two categories: Monet IN The small (MINT) and (large MONET). The reason for making this distinction, is the belief that in most expected use cases such distinction would highlight the impacts on mobility management and access control. It should be noted that this is not to be interpreted as a desire to assume that certain uses should only be associated to the monet size. The distinction based on size is simply regarded as a starting point for understanding the problem space.

It should be noted that solving the mobility problem for MNNs within a monet, is not to part of the monet problem space. Other solutions (e.g. MANET) can address this topic. The aim of this work is to solve the mobility problem for the entire monet when considered as a single unit moving within the topology.

2.1 Mobile networks In The Small (MINTs)

A MINT can be described as a single mobile IP-subnet attached to the Internet via one of more MRs. A typical example for MINTs is a car or a Personal Area Network (PAN) with a few devices connected to the Internet via different access technologies and/or ISPs via one or more MR. Several issues need to be considered to allow for MINTsÆ scalable deployment. Some of these issues are listed below.

2.2 Large MONETs

A large MONET can be defined as a network with one or several subnets connected to the Internet via one or more MRs and providing access to VMNs. Examples of such networks are IP networks on trains or ships. In these networks, MRs and VMNs are typically administered by different entities.

3. Issues to be resolved

3.1 Addressing

The addressing mechanism required for MONETs needs to be carefully considered as it will affect some of the solutions for other issues associated with MONETs. For instance, allowing every MNN to acquire a topologically correct address would imply that the MNNs are aware of their movement within the topology, hence affecting the mechanism chosen for mobility management.
Several possibilities exist for address configuration for MRs and the MNNs attached to it:

- Stateful address autoconfiguration [DHCPv6]
- Stateless address autoconfiguration [Multi-link subnets] and [Automatic prefix delegation]
- IPv6 Router Renumbering

The first 2 mechanisms can be used to configure the MRs ONLY or the entire subnet with topologically correct addresses. Such choice will affect the mobility management solution. For instance changing an MNNs address would require updating the CN and the HA.

The choice of the addressing mechanism will need to be made based on the following factors:

- Scalability:
  Can the chosen mechanism support a large number of MINTs ? This may depend on the size of the æfixedÆ network to which a MINT is attached.

- Speed:
  How much time is required for address autoconfiguration to be completed ? Is it quick enough to support fast mobility ?

- Mobility Frequency

- Nested Mobility

- Impacts on the Mobility management model:
  Does the chosen mechanism support the requirements for a scalable and secure mobility management solution ?

- Multihoming:
  Each MR may be connected to multiple ISPs, each potentially providing different paths to the Internet. In addition, there may be multiple MRs in the MINT.

- MINT definition:
  How are nodes in the MINT defined to belong to the MINT? In case of a wired MINT, it is physically defined. But a wireless MINT can begin to interfere with other geographically close wireless nodes, thus losing the definition of the MINT. A secure layer 2 is not assumed in this document, however, a secure layer 2 would certainly simplify this problem.

3.2 Mobility management

This document assumes a MIP-based mobility management solution for MONETs.
The current MIPv6 proposals provide limited levels of support for MONETs. Some solutions for the mobility scenarios are proposed in [HMIPv6] and [MONET]. However, some further investigation is needed to see whether these solutions are sufficient for the different MONET scenarios.
Specifically, issues related to route optimisation need to be investigated further. [HMIPv6], [MOBRTR] and [MONET] provide different approaches for mobility management. In [HMIPv6] MNNs connected to MRs are aware of the MRs mobility, hence route optimisation is performed by the MNNs. On the other hand, [MONET] provides an extension to MIPv6 to allow MRs to send a prefix scoped BU to re-direct traffic for the entire prefix on behalf of the MNNs. [MOBRTR] assumes a bi-directional tunnel between the mobile router and the HA, over which routing protocols are tunnelled.

In [HMIPv6], MNNs are aware of their mobility, while [MONET] and [MOBRTR] hide the networkÆs mobility from the MNNs.

The choice of the Mobility management mechanism will depend on the

following factors:

- The size of the network vs BW efficiency and speed of mobility:
  Hiding the networkÆs mobility from the MNNs can reduce MIP
  signalling (e.g. one BU from the MR to the HA instead of many).
  What tradeoffs are needed to decide whether route optimisation
  (additional signalling) should be used? How does the size of the
  network in a wireless environment affect this decision?
  How do we treat a large network on a fast train (frequent handovers
  for many MNNs) compared to a MINT (eg. a PAN)?

- Security and authorisation issues:
  BUs from MRs to CNs can cause some serious security threats for
  unauthorised MRs. Currently there is no specified solution for this
  problem.

- Routing Protocol Issues:

  Shall MR of a MINT run a routing protocol ? What is the impact on
  the routing protocol running in the visited network ?

  Which protocol shall we run within large MONETs, how it interact
  with routing protocols running in visited network

3.4 Access control and security

This chapter discusses the issues associated with access control within the Mobile Network. In this context, the spectrum of access control covers the MR û AR (fixed default router), MN û MR, and MN û MN relationships. Issues related to securing Neighbour Discovery may also be related.

3.4.1 Access control between AR and MR

The access network at the ISP/operator must allow the connection of not only a single device but also a network behind that device. The access network can perform ingress filtering, access control lists etc.

3.4.2 Access control between MR and VMNs in a large MONET

In the case of a large MONET providing Internet access for visiting nodes (VMNs) such as the train or ship case, this access will probably be controlled.
This problem is very similar to what UNAP is attempting to solve.

3.4.3 Access control between nodes in a MINT

Nodes in the MINT must trust each other. At least, MR must know who are the nodes that uses it as access router to the Internet. This is a question of who will pay for the packets.

4. Acknowledgement

Thanks to Thierry Ernst for his detailed comments. We would like to thank the monet æunofficial-BOFÆ members for their input on the monet mailing list which led to having a more concrete problem scope.

5. AuthorsÆ Addresses

Hesham Soliman and Mattias Pettersson
Ericsson Radio Systems AB.
Torshamnsgatan 23, Kista 16480,
Stockholm, Sweden.
E-mail: Hesham.Soliman@era.ericsson.se
E-mail: Mattias.Pettersson@era.ericsson.se

6. References

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[TERMINOLOGY] T. Ernst, "Network Mobility Support Terminology" draft-ernst-monet-terminology-00.txt

[REQUIREMENTS]T. Ernst, "Network Mobility Support Requirements" draft-ernst-monet-requirements-00.txt Work in progress.

[HMIPv6] H. Soliman, C. Castelluccia, K. ElMalki, L. Bellier, ôHierarchical MIPv6 mobility managementö. draft-ietf-mobileip-hmipv6-05.txt. Work in progress

[MONET] T. Ernst, L. Bellier, A. Olivereau, C. Castelluccia, H. Lach, "Mobile Networks Support in Mobile IPv6(Prefix Scope Binding Updates)" draft-ernst-mobileip-v6-network-02.txt, June 2001. Work in progress

[MOBRTR] T.J. Kniveton, J. J. Malinen, V. Devarapalli and C. E. Perkins, ôMobile router support in Mobile IPö draft-kniveton-mobrtr-00.txt. Work in progress.

This Internet-Draft expires in August 2002.