Analysis of Multihoming in Mobile IPv6
draft-ietf-monami6-mipv6-analysis-05

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on November 4, 2008.

Abstract

Mobile IPv6 as specified in RFC 3775 allows a mobile node to maintain its IPv6 communications while moving between subnets. This document investigates configurations where a mobile node running Mobile IPv6 is multihomed. The use of multiple addresses is foreseen to provide ubiquitous, permanent and fault-tolerant access to the Internet,
particularly on mobile nodes which are more prone to failure or sudden lack of connectivity. However, Mobile IPv6 currently lacks support for such multihomed nodes. The purpose of this document is to detail all the issues arising through the operation of Mobile IPv6 on multihomed mobile nodes.

Table of Contents

1. Introduction ........................................ 3
2. Terminology ........................................ 4
3. Goals and Node Capabilities ......................... 6
4. Taxonomy ........................................... 8
5. Analysis of Multihoming Configurations ............. 9
   5.1. (1,1): 1 HoA, 1 CoA .......................... 9
   5.2. (n,1): n HoAs, 1 CoA .......................... 11
   5.3. (1,n): 1 HoA, n CoAs .......................... 13
   5.4. (n,n): n HoAs, n CoAs .......................... 14
   5.5. (n,0): n HoAs, no CoAs ........................ 16
6. Multihoming Issues ................................ 16
   6.1. General IPv6-related Issues ..................... 16
      6.1.1. Failure Detection .......................... 16
      6.1.2. Path Exploration ............................ 17
      6.1.3. Path Selection .............................. 18
      6.1.4. Rehoming .................................... 19
      6.1.5. Ingress Filtering ........................... 20
   6.2. MIPv6-specific Issues ........................... 21
      6.2.1. Binding Multiple CoAs to a given HoA ....... 21
      6.2.2. Simultaneous Location in Home and Foreign Networks ... 21
      6.2.3. HA Synchronization .......................... 22
   6.3. Considerations for MIPv6 Implementation ......... 22
      6.3.1. Using one HoA as a CoA ..................... 22
      6.3.2. Binding a new CoA to the Right HoA ........... 23
      6.3.3. Binding HoA to interface .................... 23
   6.4. Summary ........................................ 24
7. Conclusion .......................................... 25
8. IANA Considerations ................................ 25
9. Security Considerations ............................. 25
10. Contributors ........................................ 25
11. Acknowledgments ................................... 26
12. References ......................................... 26
   12.1. Normative References .......................... 26
   12.2. Informative References ......................... 26
Appendix A. Why a MN may want to redirect flows ........ 28
Authors’ Addresses .................................... 29
Intellectual Property and Copyright Statements ......... 31
1. Introduction

With the emergence of performant wireless technologies, nodes are highly mobile and can change their point of attachment to the Internet at any time, even during active network connections. To support such mobility in IPv6, Mobile IPv6 ([RFC 3775] and [RFC 3776]) allows mobile nodes to maintain ongoing sessions while changing their points of attachment to the Internet.

Additionally, as explained in [3], ubiquitous, permanent, fault-tolerant and heterogeneous access to the Internet is required. For doing so, mobile nodes which are prone to failure or sudden lack of connectivity may be equipped with multiple interfaces. They may also be connected to multihomed networks. In such a situation, mobile nodes would be allocated multiple addresses and are said to be multihomed. These addresses would be assigned to a single interface or to multiple interfaces. However, the current specification of Mobile IPv6 lacks support for using multiple addresses simultaneously.

Individual solutions have been proposed to extend Mobile IPv6 in such a way but all issues have not been addressed and not even discussed in some document.

This study aims at fulfilling this gap and has two goals. The first goal is to determine the capabilities required for providing ubiquitous, permanent, fault-tolerant and heterogeneous access to the Internet to multihomed mobile nodes operating Mobile IPv6. The second goal is to define the issues arising when we attempt to fulfill these requirements. The definition of solutions addressing these issues is out of scope of this document.

To understand the foundation of this study, readers should familiarize themselves with the companion document [3] which outlines the motivations, the goals and the benefits of multihoming for both fixed and mobile nodes (i.e. generic IPv6 nodes). Real-life scenarios as illustrated in that document are the base motivations for the present study. The reader should also has basic understanding of the operation of the Mobile IPv6 protocol specified in [RFC3775].

The document is organized as follows: in Section 2, we introduce the terminology related to multihoming and used in this document. In Section 3 we recall and refine the design goals behind multihoming and we discuss what are the required capabilities on the mobile nodes to fully meet these design goals. Then we propose in Section 4 a taxonomy to classify the different cases where mobile nodes are multihomed. Thereafter the taxonomy is used in Section 5 to describe
a number of multihomed configurations specific to Mobile IPv6. For each case, we show the resulting addressing configuration (number of Home Addresses, and the number of Care-of Addresses). Each configuration is illustrated with example diagrams and the means to meet the requirements are outlined. Finally we discuss in Section 6 all issues related to a multihomed mobile node and we identify what is missing in order to reach the goals outlined in [3]. These issues are classified into IPv6 issues, Mobile IPv6-specific issues, and advices to implementers.

2. Terminology

The terms used in the present document are defined in RFC3753 [4], RFC3775 [1] and [3].

In this document we are using the following terms and abbreviations:

- **MIPv6**
  The Mobile IPv6 protocol specified in RFC3775 [1]

- **Mobile Node (MN)**
  a Mobile Node operating Mobile IPv6

- **HA**
  a Mobile IPv6 Home Agent

- **HoA**
  a Mobile IPv6 Home Address

- **CoA**
  a Mobile IPv6 Care-of Address

- **Multihomed Mobile Node**

  In the companion document [3], a node is said to be multihomed when it has multiple IPv6 addresses, either because multiple prefixes are advertised on the link(s) the node is attached to, or because the node has multiple interfaces (see the entire definition). For a mobile node operating Mobile IPv6, this may translate into the following definition:

  A mobile node is said multihomed when it has either i) multiple
addresses which are used as source addresses or ii) multiple tunnels to transmit packets, or both.

A mobile node may have multiple tunnels in the following cases:

* When it has multiple home addresses, that is if multiple prefixes are available on the home link or if it has multiple interfaces named on (presumably) distinct home links.

* When it has multiple care-of addresses, that is if multiple prefixes are available on the foreign link or if it has multiple interfaces attached to (presumably) distinct foreign links.

* When the home agent has multiple addresses.

o A valid address

An address that is topologically correct (it is configured from the prefix available on the link the interface is attached to) and routable.

o Simultaneously using multiple addresses

A mobile node is using multiple addresses simultaneously when an incoming packet with the destination address set to any of these addresses reaches the mobile node, or when any of these addresses can be used by the mobile node as the source address of outcoming packets.

o Simultaneously using multiple interfaces

A mobile node is using multiple interfaces simultaneously when it can transmit IP packets over any of these interfaces.

o Bidirectional Tunnel (BT) Mode

Mobile IPv6 Bidirectional tunnel between the mobile node and its home agent.

o Route Optimization (RO) Mode

Mobile IPv6 Route optimization between the mobile node and its correspondent node.
3. Goals and Node Capabilities

In this section, we determine what are the capabilities required on the mobile nodes in order to benefit from multihoming configurations, as indicated in [3] where a number of goals/benefits are listed: ubiquitous access, flow redirection, reliability, load sharing, interface switching, preference settings, and aggregate bandwidth. These do somewhat overlap, i.e., they are not totally independent. Reaching one of them may imply reaching another one as well. For this reason, the following non-overlapping goals could be extracted:

1. Reliability
2. Load Sharing
3. Flow Distribution

From now on, this document will focus on these three non-overlapping goals, as in this section to determine capabilities. We will determine later in Section 5 which capabilities are already fulfilled by Mobile IPv6 and what issues still remain.

Basically, Internet connectivity is guaranteed for a mobile node as long as at least one path is maintained between the mobile node and the fixed Internet. This path can be divided into two portions: the path between the mobile node and its home agent(s) and the path between the home agent(s) and the correspondent node. If route optimization is in place between the mobile node and the correspondent node, an additional path between the mobile node and the correspondent node must be guaranteed. In essence, the benefit of multihoming is to allow all or parts of these paths to have multiple alternatives, so as to achieve reliability, load sharing and/or flow distribution. In some cases, it may be necessary to divert packets from a (perhaps failed) path to an alternative (perhaps newly established) path (e.g. for matters of reliability, preferences), or to split traffic between multiple paths (e.g. for load sharing, flow distribution). The use of an alternative path must be transparent at layers above layer 3 if broken sessions and the establishment of new transport sessions has to be avoided.

In order to meet some of the goals (particularly flow distribution and load sharing), multiple paths must be maintained simultaneously between the mobile node and its correspondent node.

This translates into the following capabilities:

1. A mechanism should be available to quickly activate a backup interface and redirect traffic when an interface fails (e.g.,
loss of connection).

2. A mechanism should be available to quickly redirect flows from one address to another when it is needed. Some of the triggers of flow redirection are given in Appendix A.

3. A mobile node allocated with multiple valid addresses must be able to use them simultaneously.

4. A mobile node equipped with multiple interfaces (attached to distinct foreign links or distinct home links, or a combination of both) must be able to use them simultaneously.

5. A mobile node should be able to distribute its traffic load among its valid global addresses.

6. If multiple home agents are available to manage bindings for a given home address, the mobile node should be able to use them simultaneously or to switch between them.

One has to consider whether these goals can be achieved with transparency or without transparency. Transparency is achieved when switching between interfaces-addresses does not cause the disruption of ongoing sessions. To achieve transparency, a necessary (may or may not be sufficient) condition is for the end-point addresses at the transport/application layer to remain unchanged. This is in view of the large amount of Internet traffic currently carried by TCP, which unlike SCTP, cannot handle multiple end-point address pairs.

Each of the aforementioned goals can be achieved independently. We define here which of the above capabilities are needed for each goal:

1. Reliability: 1, 2, 3, 6

2. Load Sharing: 3, 6

3. Flow Distribution: 2, 3, 4, 5, 6
4. Taxonomy

In order to examine the issues preventing a mobile node to meet the requirements listed in Section 3 we use in the present document the following taxonomy \((x,y)\) where:

- \(x\) = number of Home Addresses (HoAs)
- \(y\) = number of Care-of Addresses (CoAs)

A value of ‘1’ implies there is a single instance of the parameter, whereas a value of ‘n’ indicates that there are multiple instances of the parameter. A value of ‘0’ implies that there is no instance of this parameter. A value ‘*’ indicates that the number can be ‘0’, ‘1’ or ‘n’.

An illustration of this taxonomy is given in Figure 1.

\[
\begin{align*}
\text{Mobile Node} & \\
\text{HoA1} & \text{HoA2} & \ldots & \text{HoAn} & \rightarrow \text{Permanent Address (x)} \\
\uparrow & \downarrow & \uparrow & \downarrow & \\
\text{CoA1} & \text{CoA2} & \text{CoA3} & \ldots & \text{CoAn} & \rightarrow \text{Temporary Address (y)} \\
\uparrow & \downarrow & \uparrow & \downarrow & \\
\text{Link1} & \text{Link2} & \text{Link3} & \ldots & \text{Linkn} & \rightarrow \text{IPv6 Link (n/a *)} \\
\uparrow & \downarrow & \uparrow & \downarrow & \\
\text{IF1} & \text{IF2} & \ldots & \text{IFn} & \rightarrow \text{Physical layer}
\end{align*}
\]

CoA1, CoA2, CoA3 are bound to HoA1 on IF1 and IF2
CoA3 is bound to HoA2 on IF2

* n/a because the number of IPv6 links is equal to number of CoAs (y)

Figure 1: Illustration of the Taxonomy

As the taxonomy suggests, the fact that a mobile node has several home addresses is independent from it having multiple interfaces. Having multiple interfaces does not imply that it has multiple home addresses and vice-versa. Similarly, the number of care-of addresses is independent from the number of home addresses and the number of interfaces. While a node would probably have at least one care-of address per interface, multiple prefixes available on a link may lead the node to configure several care-of addresses on that link.
The proposed taxonomy has two parameters because each of them has an influence on either the mobile node behavior / management, or the potential benefits the mobile node may obtain from such a configuration.

The configurations denoted by these parameters will have an impact on how multihoming is supported. Depending on the number of home and care-of addresses, different policies will be needed, such as "which care-of address has to be mapped to which home address", "all the care-of addresses must be mapped with all the home addresses", etc.

The readers should note that for Mobile IPv6, home address is used to identify a binding. Thus when a mobile node has multiple home addresses, it would imply the mobile node is using multiple Mobile IPv6 sessions, regardless of whether all the home addresses are handled by a single home agent.

5. Analysis of Multihoming Configurations

In this section, we detail all the possible multihoming configurations. We briefly discuss the current situation with Mobile IPv6 and we point to issues that will be further detailed in Section 6.1, Section 6.2 and Section 6.3.

As it is demonstrated below, we notice that:

- When the mobile nodes is equipped with multiple interfaces, reliability, load sharing and flow distribution can be achieved in all (*,*) cases.

- When a single interface is available, none of the goals can be achieved in the (1,1) case (the mobile node is not multihomed). In all the other cases, only reliability and load sharing can be achieved.

5.1. (1,1): 1 HoA, 1 CoA

A mobile node in this configuration with only a single network interface is not multihomed. This configuration is the common case of a mobile node is away from its home link: the node has one home address and one care-of address which is configured on the foreign link. None of the multihoming goals are achievable.

A mobile node in the same configuration but with several interfaces is multihomed and lead to a special situation where the mobile node is connected to both its home link and a foreign link. In order to use both interfaces simultaneously, the home address would be
directly used on the interface connected to the home link, and a care-of address configured on the other interface connected to a foreign link. There cannot be more than two active interfaces in the (1,1) case, otherwise the mobile node would either have (A) multiple interfaces on the home link, or (B) multiple interfaces on foreign links. For (A), there would be multiple home addresses. For (B) there would be multiple care-of addresses. These are indeed cases (n,*) (see Section 5.2, Section 5.4 and Section 5.5) and (*,n) (see Section 5.3 and Section 5.4), respectively.

We next analyze if Mobile IPv6 can be used to achieve the following multihoming benefits:

- Reliability

  What Mobile IPv6 can achieve

  Reliability is achievable, but in a limited manner. Although the mobile node cannot register its care-of address at its home agent and use its home link at the same time, it could register the care-of address with selected correspondent nodes (i.e. route optimization). In this case, the mobile node can enjoy a better reliability for communications sessions opened with these correspondent nodes. When the care-of address fails, the mobile node can either bind a new care-of address with its home address at the correspondent nodes, or remove the binding and directly get the packets via the home link.

  What is missing for Mobile IPv6

  The mobile node cannot register the care-of address configured on the foreign network with its home address and receive packets from the home agent via a tunnel to the care-of address at the same time it receives packet on the home address from the home link. In addition, if the mobile node looses its connection on the foreign link, flows that are started by using the care-of address as a source address must be re-initiated with another address (either the home address, or a new care-of address obtained on another foreign link). Fault recovery is thus only possible without transparency, and Mobile IPv6 features can only recover the failure of the home address. This issue is detailed in Section 6.2.2.

  Reliability could also be achieved through bi-casting since the mobile node has two addresses and should be able to request any correspondent node to duplicate traffic to both of them. However, Mobile IPv6 does not allow the mobile node to request bi-casting on the correspondent node (see Section 6.2.2).
Load Sharing, Flow Distribution

What Mobile IPv6 can achieve

The mobile node is able to use both interfaces at the same time, according to some preference settings on its side to decide which one to use for which application. Therefore load sharing and flow distribution can be achieved when sessions are initiated by the mobile node. When a correspondent node initiates a session with the mobile node, it would choose the destination address depending on the available information about the mobile node (e.g., DNS request). Presently there is no mechanism allowing the mobile node to indicate on which interface (i.e., address) a correspondent node may reach it. If only one address is known by the distant node, load sharing and flow distribution cannot be achieved. See in Section 6.1.3 where such path selection issues are discussed.

What is missing for Mobile IPv6

Although the mobile node is able to use both interfaces at the same time, there is no mechanism that allows the mobile node to indicate to which interface (i.e., address) a correspondent node send packets for a particular flow. Section 6.1.3 discusses such path selection issues.

5.2. (n,1): n HoAs, 1 CoA

A mobile node in this configuration is multihomed since it has several home addresses. This case may happen when a node gets access to the Internet through different home agents (possibly distinct operators), each offering a Mobile IPv6 service to the node. That way, the mobile node would have a home address per home agent. Alternatively, a single home network may be multihomed to the Internet, leading to the advertisement of multiple prefixes on the home link. The mobile node would thus have multiple home addresses on a single home link.

In either cases, the node would configure a single care-of address on the visited IPv6 subnet, and bind that single care-of address to all its home addresses. If the mobile node has multiple interfaces, only one interface is connected to a foreign network. The other interfaces are connected to their home links, or are inactive.

We next analyze if Mobile IPv6 can be used to achieve the following multihoming benefits:
o Reliability

What Mobile IPv6 can achieve

The care-of address may change when the mobile node has multiple interfaces and is disconnected from its home link (e.g. failure of the interface, or movement). In such a situation, Mobile IPv6 allows transparent redirection of flows using the old care-of address (i.e. the session was initiated using the home address) to another care-of address. For sessions directly opened via the care-of address, the loss of the address implies a re-initiation of the session.

What is missing for Mobile IPv6

If the home agent fails, the session using the failed home agent must be restarted since Mobile IPv6 does not provide any mechanism to hand-over transparently from a home agent to another one. Fault tolerance cannot be achieved in this case, since established communications cannot be preserved (unless mechanism such as [6] is used). See the corresponding discussion in Section 6.1.4 and Section 6.2.3.

If one of the home addresses of the mobile node fails, it means either that the corresponding home agent has failed (which is the case discussed above), or the home address is no longer routed to the home agent. In that latter case, sessions using that HoA would be terminated, since the home address cannot be changed transparently.

Reliability through bi-casting could also be achieved by registering two addresses with a single home address. However Mobile IPv6 does not provide any mechanism to associate more than one care-of address with one home address. Moreover, in this particular case, one home address should be used as a care-of address bound to the other home address. (see in Section 6.2.1 and Section 6.3.1).

o Load Sharing

What Mobile IPv6 can achieve

In bidirectional tunnel mode, load sharing only affects the path between the correspondent node and the home agent(s), and not the path between the mobile node and the home agent(s), as long as the care-of address does not change. In route optimization mode, the path between the mobile node and the correspondent node does not change if the care-of address does
not change. As an entry in the binding cache is identified by a home address, the mobile node can register the same care-of address with all home address, on any distant node.

What is missing for Mobile IPv6

A mechanism would be needed for the mobile node to select which home address should be used when a new communication flow is initiated. A similar mechanism is needed on the correspondent node side if it knows that multiple home addresses are assigned to the same mobile node. With such mechanisms, it would be possible to use multiple home addresses at the same time, and load sharing could be performed. However, it can be noted that load sharing on the path between the correspondent node and the home agent might not be the most bandwidth constraint part of the overall path from the correspondent node to the mobile node. Thus load sharing might not bring important benefits. See in Section 6.1.3 where such path selection issues are discussed. It is also possible that the mobile node register one home address as a care-of address for another home address (see in Section 6.3.1).

- Flow Distribution

What Mobile IPv6 can achieve

Flow distribution is achievable when the mobile node is attached to one foreign link via one of its interfaces and to the home link(s) via its other interface(s). In this case, the mobile node can spread flows over its interfaces. Note that if a correspondent node initiates a communication, the interface that it will use on the mobile node would depend on which mobile node’s address is advertised to the correspondent node.

5.3. (1,n): 1 HoA, n CoAs

A mobile node in this configuration is multihomed since it has several care-of addresses. This may occur when the mobile node has multiple interfaces connected to different links, or when the only interface is connected to a link where multiple IPv6 prefixes are advertised (i.e. the visited network is multihomed). Note that one of the interfaces of the mobile node may be connected to its home link.

We next analyze if Mobile IPv6 can be used to achieve the following multihoming benefits:
Internet-Draft       Analysis of Multihoming in MIPv6      May 2008

- What Mobile IPv6 can achieve

Reliability support is limited to recover from a failed care-of address. Fault recovery is achieved in Mobile IPv6 by associating an alternate care-of address to replace the failed one.

- What is missing for Mobile IPv6

Efficient mechanisms are needed to determine that a care-of address has failed (see Section 6.1.1), to check reachability (Section 6.1.2), to determine which care-of address should be used instead (Section 6.1.3) and to redirect flows to the new care-of address (Section 6.1.4).

- Load Sharing and Flow Distribution

What Mobile IPv6 can achieve

This configuration allows sharing of the load and setting of preferences among different paths between the home agent and the mobile node when bidirectional tunnel mode is used, and between the correspondent node and the mobile node when route optimized mode is used.

What is missing for Mobile IPv6

In order to achieve load sharing and flow distribution under this scenario, the mobile node would need to register several care-of addresses with its unique home addresses. However, the present specification of Mobile IPv6 only allows the mobile node to register a single care-of address per home address. This is discussed in Section 6.2.1. When a single home address is bounded to several care-of addresses at the same time, the mobile node, home agent, or correspondent node must be able to select the appropriate care-of address. This selection could be done based on user/application preferences (see Section 6.1.3).

5.4. (n,n): n HoAs, n CoAs

A mobile node in this configuration is multihomed since it has multiple addresses. This case can be viewed as a combination of the two cases described above: the mobile node has several home addresses, e.g. given by different operators (similar to case (n,1) in Section 5.2) and several care-of addresses, e.g. because the node
is receiving multiple IPv6 prefixes (similar to case (1,n) in Section 5.3).

We next analyze if Mobile IPv6 can be used to achieve the following multihoming benefits:

- **Reliability**

  **What Mobile IPv6 can achieve**

  If one care-of address becomes unreachable (similar to (1,n)), the mobile node can redirect flows to another care-of address by binding any of the other available care-of address to the corresponding home address. If the mobile node cannot use one of its home addresses anymore (similar to (n,1)), the mobile node will have to re-initiate all flows which were using the corresponding home address. Redirection between the addresses available for the mobile node will be different depending on the binding policies.

  **What is missing for Mobile IPv6**

  None specific to (n,n) configuration.

- **Load Sharing and Flow Distribution**

  **What Mobile IPv6 can achieve**

  Although Mobile IPv6 allows the mobile node to register only one care-of address per home address (see Section 6.2.1), it can register the same or different care-of addresses with multiple home addresses. If the mobile node chooses to bind the same care-of address to all its home addresses, we fall in the (n,1) case. In this case, load sharing can only be performed if route optimization is not used, on the CN-HA path, as a different home address may be used per correspondent node. If the mobile node chooses to bind a different care-of address for each home address, load sharing will be done along the whole path across the mobile node and its correspondent nodes. Preference settings may define which care-of address should be bound to which home address (see Section 6.1.3).

  In a very specific situation, one of the routable address of the mobile node (i.e., which can be directly used without tunneling to reach the mobile node) can be one of its home addresses. This home address would then be viewed as a care-of address bound to another home address (similar to (n,1)). Mobile IPv6 does not prevent this behavior, which allows to set
a certain preference on addresses usage. See Section 6.3.1 for the corresponding issue.

What is missing for Mobile IPv6

None specific to (n,n) configuration.

5.5. (n,0): n HoAs, no CoAs

This case happens when all the interfaces are connected to their respective home links. This situation is quite similar to a multihomed fixed node. The node would no longer be in the (n,0) configuration when one or more of the interfaces are attached to foreign links.

The mobile node may wish to use one or more home addresses to serve as the care-of address of another home address (see Section 6.3.1). In such situations, this scenario is reduced to a (1,1) or (1,n) configuration as described in Section 5.1 and Section 5.3, respectively. Analysis of which are already done in those section and is thus omitted.

6. Multihoming Issues

Existing protocols may not allow reaching the goals expressed in Section 3. For doing so, the issues discussed in this section must be addressed, and solved preferably by dynamic mechanisms. Note that some issues are pertaining to Mobile IPv6 solely, whereas other issues are not at all related to Mobile IPv6. However, such non MIPv6 issues must be solved in order to meet the goals outlined in Section 3.

In this section, we describe some of these issues in two main headings: general IPv6-related issues (Section 6.1), and issues that are specific to Mobile IPv6 (Section 6.2). Other concerns related to implementations of Mobile IPv6 are described in Section 6.3. Issues and their area of application are summarized in Section 6.4

6.1. General IPv6-related Issues

6.1.1. Failure Detection

It is expected for faults to occur more readily at the edge of the network (i.e. the mobile nodes), due to the use of wireless connections. Efficient fault detection mechanisms are necessary to recover in timely fashion. A failure in the path between two nodes can be located at many different places: the media of one of the node
is broken (i.e., loss of connectivity), the path between the mobile
node and the home agent is broken, the home link is disconnected from
the Internet, etc. The failure protection domain greatly varies. In
some configurations, the protection domain is limited to a portion of
the path.

So far, Mobile IPv6 only relies on the ability or the inability to
receive Router Advertisements within a stipulated period to detect
the availability or loss of media (local failure).

[7] is addressing such concerns through the use of layer 2 triggers
[8]. Movement detection might be extended to include other triggers
such as the loss of connectivity on one interface. Additional
mechanisms would be needed to detect a failure in the path between a
mobile node and its correspondent node(s), as well as between the
mobile node and its home agent(s), and between the home agent and
correspondent node(s).

6.1.2. Path Exploration

When the mobile node needs to re-home a communication to an
alternative path, a path exploration may take place. The path
exploration is a step that occurs after the failure detection, and
before the path selection. It consists of identifying a set of paths
that are known to provide bidirectional connectivity between the
mobile node and its home agent, and optionally between the mobile
node and its correspondent node. It may be noted that the step of
path exploration may be avoided by selecting a new path, and trying
to re-home the communications on this new path. If the re-
homing fails, a new path is selected until there is no alternate path, or
the re-homing signaling succeed.

Path exploration requires some signaling between pairs of addresses
to check reachability. An additional protocol may be needed to
perform this task.

In (1,*) the path exploration consists in checking reachability
between each care-of address and each home agent address. If RO mode
is used, the mobile node may also insure reachability between its
correspondent nodes’ address(es) and each care-of address.

In (n,*), the path exploration consists in checking reachability
between the home address that is used with the session that must be
re-homed and each care-of address (and optionally with the
correspondent nodes’ address(es)). In addition, the session may need
to be re-homed to a different home address. In this case, each path
between a pair (HoA, CoA) must to be validated.
In all these cases the path between the home agent and the correspondent node is not checked. A specific mechanism may be defined to check reachability between a home agent and a correspondent node.

6.1.3. Path Selection

When there exists multiple paths from and to the mobile node, the mobile node ends up choosing a source address, and possibly the interface that should be used. A correspondent node that wants to establish a communication with such a mobile node may end up by choosing a destination address for this mobile node.

- **Interface selection**

  When the mobile node has multiple available interfaces, the simultaneous or selective use of several interfaces would allow a mobile node to spread flows between its different interfaces.

  Each interface could be used differently according to some user and applications policies and preferences that would define which flow would be mapped to which interface and/or which flow should not be used over a given interface. How such preferences would be set on the mobile node is out of scope of Mobile IPv6 and might be implementation specific. On the other hand, if the mobile node wishes to influence how preferences are set on distant nodes (correspondent node or home agent), mechanisms such as those proposed in draft-soliman-flow-binding [9] could be used.

- **Home Address Selection**

  When multiple home addresses are available, the mobile node and its communicating peers (home agent and correspondent nodes) must be able to select the appropriate home address to be used for a particular packet or flow.

  This choice would be made at the time of a new communication flow set up. Usual IPv6 mechanisms for source and destination address selection, such as "Default Address Selection for IPv6" (RFC3484) [10] or DNS SRV Protocol (RFC2782) [11] could be used.

  However, in RFC3484 it is said that "if the eight rules fail to choose a single address, some unspecified tie-breaker should be used". Therefore more specific rules in addition to those described in RFC3484 may be defined for home address selection.
CoA Selection

When multiple care-of addresses are available, the mobile node and its communicating peers must be able to select the appropriate care-of address to be used for a particular packet or flow. The mobile node may use its internal policies to (i) distribute its flow, and (ii) distribute policies on distant nodes to allow them to select the preferred care-of address. Solutions like [12] or [13] may be used.

Another related aspect of path selection is the concern of ingress filtering. This is covered below in Section 6.1.5.

6.1.4. Rehoming

Re-homing takes place after an outage has been detected or an alternative path has been identified (see previous issues Section 6.1.1, Section 6.1.2 and Section 6.1.3), therefrom diverting existing sessions from one path to another. New transport sessions would have to be established over the alternate path if no mechanism is provided to redirect flow transparently at layers above layer 3. The need for re-homing or flow redirection is explained in Appendix A.

The different mechanisms that can be used to provide re-homing can be split into three categories, depending on the part of the path that needs to be changed.

The first category is the care-of address changes : it influences the path between the mobile node and its home agent, and the path between the mobile node and its correspondent node in RO mode. This may hold in case (n, n).

The second category is when the home address changes (: it influences the entire path. As the home address is the address shown to the higher layer (above layer 3), an additional mechanism is needed to manage this change. Solution with a shim layer (e.g., Shim6 [14]), or solution at the transport layer such as SCTP [5] may be useful.

The third category is when the home agent address changes. In this case, the bidirectional tunnel between the mobile node and its home agent as to be switched to the new address of the home agent. This can be managed transparently by Mobile IPv6 if the home address doesn’t change at the same time. Otherwise, sessions continuity is not ensured, as explained in the above paragraph.
6.1.5. Ingress Filtering

Ingress filtering mechanisms [15][16] may drop the outgoing packets when multiple bi-directional tunnels end up at different home agents. This could particularly occur if different prefixes are handled by different home agents. If a packet with a source address configured from a specific prefix is tunneled to a home agent that does not handle that specific prefix, the packet may be discarded either by the home agent or by a border router in the home network. The problem of ingress filtering however, is two-fold. It can occur in the access network as well as the home network.

Suppose the mobile node selects the interface (which would determine the care-of address) and the home network (which would determine the home address): the chosen care-of address may not be registered with the chosen home address. For instance, consider Figure 2 below. In the access network, the mobile node MN must use CoA=PA.MN when it sends packets through AR-A and it must use CoA=PB.MN when it sends a packet through AR-B. In the home network, it must use HoA=P1.MN when it tunnels the packet to home agent HA-1, and it must use HoA=P2.MN when it tunnels the packet to home agent HA-2. To avoid ingress filtering, the choice is thus limited to a of valid (HoA,CoA) pairs. This issue is related to Section 6.1.3 and greatly limits the way mobile node can benefit from its multihoming configuration (particularly in case of the home agent failure since flows cannot be diverted to the other home agent).

Should the mobile node be able to bind both care-of addresses PA.MN and PB.MN simultaneously to home addresses P1.MN and P2.MN respectively (see Section 6.2.1), it would be able to choose the (HoA,CoA) pair based on the access network it wishes to use for outgoing packets. It is, nonetheless, still limited to transmit all packets to a specific home agent for the selected (HoA,CoA) pair, i.e. ingress filtering at the home network remains unsolved.

Ingress filtering in the home network concerns only the (n,n) case.

Figure 2: MN connected to Multiple Access/Home Networks

Prefix: PA +--------+ +--------+ +--------+
HoA: P1.MN /-----| AR-A |----|          |----| HA-1 |
CoA: PA.MN / +--------+ |          | +--------+

| MN | Prefix: P1
+----+ Internet

Prefix: P1

HoA: P2.MN \ +--------+ | +--------+
CoA: PB.MN \-----| AR-B |----|----| HA-2 |

Prefix: PB +--------+ +--------+ +--------+

Figure 2: MN connected to Multiple Access/Home Networks

Should the mobile node be able to bind both care-of addresses PA.MN and PB.MN simultaneously to home addresses P1.MN and P2.MN respectively (see Section 6.2.1), it would be able to choose the (HoA,CoA) pair based on the access network it wishes to use for outgoing packets. It is, nonetheless, still limited to transmit all packets to a specific home agent for the selected (HoA,CoA) pair, i.e. ingress filtering at the home network remains unsolved.

Ingress filtering in the home network concerns only the (n,n) case.
since the choice of the home and care-of addresses is limited to a single (HoA, CoA) pair in other cases. In (n,n), the mobile node may be connected to multiple access networks or multiple home networks each practicing ingress filtering. To overcome this, mechanisms such as those provided by Shim6 (see RFC3582 [17] and [14]) may be used.

6.2. MIPv6-specific Issues

6.2.1. Binding Multiple CoAs to a given HoA

In the (1,n) cases, multiple care-of addresses would be available to the mobile node. In order to use them simultaneously, the mobile node must be able to bind and register multiple care-of addresses for a single home address with both the home agent and the correspondent nodes. The Mobile IPv6 specification is currently lacking such ability.

Although in the (n,n) cases, Mobile IPv6 allows the mobile node to have multiple (HoA,CoA) pairs, the upper layer’s choice of using a particular home address would mean that the mobile node is forced to use the corresponding care-of address. This constrains the mobile node from choosing the best (in terms of cost, bandwidth etc) access link for a particular flow, since care-of address is normally bound to a particular interface. If the mobile node can register all available care-of addresses with each home address, this would completely decouple the home address from the interface, and allow the mobile node to fully exploit its multihoming capabilities.

To counter this issue, a solution like [18] may be used. However, with simultaneous binding support, there exists a possibility that a malicious mobile node can successfully bind a number of victims’ addresses as valid care-of addresses for the mobile node with its home agent. This is further elaborated in [19]. In view of such risk, it might be advisable for home agent implementations to employ some form of care-of addresses verification before using the care-of addresses as a valid routing path to mobile node when accepting multiple care-of address registrations.

6.2.2. Simultaneous Location in Home and Foreign Networks

Rule 4 of RFC3484 (section 5) specifies that a home address should be preferred to a care-of address. While this rule allows the host to choose which address to use, it does not allow the mobile node to benefit from being multihomed in a situation where it may have one of its interfaces directly connected to a home link. That is, addresses from other interfaces cannot be registered as care-of addresses for the home address associated to the home link the mobile node is connected to. As a result, flows cannot be redirected transparently
from one care-of address to another and Mobile IPv6 features can only recover the failure of the home address.

In the case of (1,*) where one of the interface is connected to the home link, none of the other addresses can be used to achieve multihoming goals with the home agent.

This issue is currently being resolved by [18].

6.2.3. HA Synchronization

For a single home address obtained from a single home network, when a failure is affecting ongoing sessions on a given home agent (i.e. home agent has failed or is overloaded), solutions like [6] may be used to allowing existing sessions to be shifted from one home agent to another. However, in the (n,*) cases where home addresses may be obtained from different home agents on different home networks, such coordination is not currently available. To achieve a global home agent synchronization, it might be necessary to extend mechanisms such as proposed in [6], [20] and [21].

6.3. Considerations for MIPv6 Implementation

In addition to the issues described in Section 6.1 and Section 6.2, there are other concerns implementers should take into consideration so that their Mobile IPv6 implementations are more "friendly" to multihoming, particularly the use of multiple interfaces. These implementation-related considerations are described in the sub-sections below.

6.3.1. Using one HoA as a CoA

In (n,*) cases, the mobile node has multiple home addresses. A home address may be seen as a care-of address from the perspective of another home link of the same mobile node.

As an example, a mobile node has two home addresses (HoA1 and HoA2) on two distinct home links. The mobile node is connected to these two home links via two interfaces. When the mobile node loses its connectivity on its first interface and HoA1 is not reachable, it may want to register HoA2 as a care-of address for HoA1 in order to keep receiving packets intended to HoA1, via the second interface.

According to the definition of a care-of address, the current Mobile IPv6 specification does not prohibit to register a home address as the care-of address from the perspective of another home address.

In RFC3775 section 6.1.7 it is written: "Similarly, the Binding
Update MUST be silently discarded if the care-of address appears as a
home address in an existing Binding Cache entry, with its current
location creating a circular reference back to the home address
specified in the Binding Update (possibly through additional
entries).

In order to benefit from any multihoming configuration, a mobile node
must be able to register whatever address it owns with any of its
home address, as long as the above statement is observed.

6.3.2. Binding a new CoA to the Right HoA

In the \((n, *)\) cases, the mobile node has multiple home addresses.
When the mobile node moves and configures a new care-of address, the
newly obtained care-of address must be bound to a specific home
address. The current Mobile IPv6 specification doesn’t provide a
decision mechanism to determine to which home address this newly
acquired care-of address should be bound to.

With no such mechanism, the mobile node may be confused and may bind
this care-of address to a possibly wrong home address. The result
might be to bind the care-of address to the same home address the
previous care-of address was bound to or to another one, depending on
the implementation. It would indeed be better to specify the
behavior so that all implementations are compliant.

6.3.3. Binding HoA to interface

In \((n, *)\) cases, Mobile IPv6 does not provide any information on how
home addresses should be bound to a device, and particularly there is
no mechanism to bind home addresses to interfaces.

This may be troublesome, for example, when we consider a mobile node
configured with two home addresses and equipped with three
interfaces. When the mobile node is connected to a home link via one
interface, it will need to bind the corresponding home address to
this interface, even if the home address was initially assigned to
another one.

\[
\begin{array}{ccc}
\text{HoA1} & \text{HoA2} \\
\text{CoA1} & \text{CoA2} & \text{CoA3} \\
\text{Iface1} & \text{Iface2} & \text{Iface3} \\
\end{array}
\]

Figure 3: Illustration of the case \((2, 3)\)

Home address must always be assigned to an activated interface and if
the mobile node is connected to its home link, the corresponding home
address must be used on this interface. In some cases, the home address then would have to be re-assigned to another interface in case of connection loss or attachment to the home link.

6.4. Summary

The table below summarizes the cases where each issue applies.

<table>
<thead>
<tr>
<th></th>
<th># of HoAs:</th>
<th>1</th>
<th>1</th>
<th>n</th>
<th>n</th>
<th>n</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td># of CoAs:</td>
<td>1</td>
<td>n</td>
<td>0</td>
<td>1</td>
<td>n</td>
</tr>
<tr>
<td>General IPv6 Issues</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Failure Detection</td>
<td>o</td>
<td>o</td>
<td>?</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Path Exploration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Path Selection</td>
<td></td>
<td>o</td>
<td>?</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Flow Redirection</td>
<td>o</td>
<td>o</td>
<td>?</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Ingress Filtering</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Binding Multiple CoAs to a given HoA</td>
<td></td>
<td></td>
<td>o</td>
<td>?</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Simultaneous Location in Home and Foreign Networks</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HA Synchronization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implementation-Related Concerns</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Using one HoA as a CoA</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Binding a new CoA to the Right HoA</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>Binding HoA to Interface(s)</td>
<td>o</td>
<td>o</td>
<td>?</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

Figure 4: Summary of Issues and Categorization
7. Conclusion

In this document, we have demonstrated issues arising for multihomed mobile nodes operating Mobile IPv6. We have seen that mechanisms are needed:

- to redirect flows from a failed path to a new path,
- to decide which path should better be taken when multiple paths are available,
- to register multiple care-of addresses,
- to exchange policies between the mobile node and the home agent.

Even if Mobile IPv6 can be used as a mechanism to manage multihomed mobile nodes, triggers of flow redirection between interfaces/addresses are not adapted to the multihoming status of the node. Also, we have shown that in some configurations Mobile IPv6 is ambiguous in the definitions of CoA/HoA and in the mappings between home addresses, care-of addresses and network interfaces. Finally, we have also raised issues not directly related to Mobile IPv6, but solutions for these issues are needed for mobile nodes to fully take advantage of their multihomed configuration.

8. IANA Considerations

This is an informational document and as such does not require any IANA action.

9. Security Considerations

This is an informational document where the multihoming configurations under the operation of Mobile IPv6 are analyzed. Security considerations of these multihoming configurations, should they be different from those that concern Mobile IPv6, must be considered by forthcoming solutions. For instance, Section 6.2.1 described a potential threat that should be considered when developing a proposed solution for multiple care-of addresses registration.

10. Contributors

The following people have contributed ideas, text and comments to earlier versions of this document: Eun Kyoung Paik from Seoul.
11. Acknowledgments

The authors would like to thank all the people who have sent comments so far, particularly Marcelo Bagnulo, Romain Kuntz, Tobias Kufner, Henrik Levkowetz, George Tsirtsis for their in-depth comments and raising new issues.

12. References

12.1. Normative References


12.2. Informative References


Appendix A. Why a MN may want to redirect flows

When a mobile node is multihomed, an addresses selection mechanism is needed to distribute flows over interfaces. As policies may change over time, as well as the available addresses/interfaces, flow redirection mechanisms are needed. While the selection policy is out of scope of this document, the following reasons may trigger the mobile node to redirect flow from one address to another:

- **Failure detection:** the path between the mobile node and its correspondent node(s) is broken. The failure can occur at different places onto this path; The failure can be local on the mobile node, where the interface used on the mobile node is disconnected from the network (e.g., a wireless interface which comes out of range from its point of attachment). Alternatively, the failure can be on the path between the mobile node and one of its home agent. Yet another alternative is that the failure can be on the path between the home agent and the correspondent node. If route optimization is used, it can also be a failure between the mobile node and its correspondent node(s).

- **New address:** a new address on the mobile node may become available, e.g. when the mobile node connects to the network with a new interface. The mobile node may decide that this new interface is most suitable for its current flows that are using another interface.

- **Uninterrupted horizontal handover in mobility:** if the mobile node is mobile, it may have to change its point of attachment. When a mobile node performs a horizontal handover, the handover latency (the time during which the mobile node can not send nor receive packets) can be long and the flows exchanged on the interface can be interrupted. If the mobile node wants to minimize such perturbation, it can redirect some or all the flows on another available interface. This redirection can be done prior to the handover if L2 triggering is considered [8].

- **Change in the network capabilities:** the mobile node can observe a degradation of service on one of its interface, or conversely an improvement of capacity on an interface. The mobile node may then
decide to redirect some or all flows on another interface that it considers most suitable for the target flows.

- Initiation of a new flow: a new flow is initiated between the mobile node and a correspondent node. According to internal policies, the mobile node may want to redirect this flow on a most suitable interface.

Authors’ Addresses

Nicolas Montavont
Institut Telecom - Telecom Bretagne
2, rue de la chataigneraie
Cesson Sevigne  35576
France

Phone: (+33) 2 99 12 70 23
Email: nicolas.montavont@telecom-bretagne.eu
URI: http://www.rennes.enst-bretagne.fr/~montavont/

Ryuji Wakikawa
Toyota ITC / Keio University
6-6-20 Akasaka, Minato-ku
Tokyo 107-0052
Japan

Phone: +81-3-5561-8276
Fax: +81-3-5561-8292
Email: ryuji@jp.toyota-itc.com

Thierry Ernst
INRIA
INRIA Rocquencourt
Domaine de Voluceau B.P. 105
Le Chesnay,   78153
France

Phone: +33-1-39-63-59-30
Fax: +33-1-39-63-54-91
Email: thierry.ernst@inria.fr
URI: http://www.nautilus6.org/~thierry
Chan-Wah Ng
Panasonic Singapore Laboratories Pte Ltd
Blk 1022 Tai Seng Ave #06-3530
Tai Seng Industrial Estate
Singapore  534415
Singapore

Phone: +65 65505420
Email: chanwah.ng@sg.panasonic.com

Koojana Kuladinithi
University of Bremen
ComNets-ikom, University of Bremen.
Otto-Hahn-Allee NW 1
Bremen, Bremen  28359
Germany

Phone: +49-421-218-8264
Fax:  +49-421-218-3601
Email: koo@comnets.uni-bremen.de
URI:  http://www.comnets.uni-bremen.de/~koo/
Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.