MIF Problem Requirements and Scenarios
draft-williams-mif-problem-scenarios-00.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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 January 7, 2010.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document provides the problem statement requirements and scenarios for MIF. These requirements and use case scenarios are intended to define an approach to solving common problems presented
in MIF. These MIF requirements and scenarios are based around the common and prevalent problem of adaptation of a host to attach to multiple networks simultaneously. Such a host not only has to make decisions about selection of service parameters but also how to deal with issues relating to contradictory configuration objects. These MIF scenarios are intended to be part of a set of such scenarios that together define the purpose, scope and requirements for proposed and realized capabilities.

1. Introduction

Currently most of the network hosts (such as mobile phones, note PCs, etc) are equipped with multiple interfaces physically or virtually. The interfaces may connect with same or different network domains. Such scenarios result in connectivity issues as configuration information may be local to the interface or global to the node. Various issues arise when multiple configuration parameters are global to the node are received on the many interfaces the multihomed host has.

When a host has multiple network connections, problems arise within the network stack. Such hosts receive configuration parameters from multiple sources, such as from any set of default routers, DHCP servers, and manual configurations. Questions of how are conflicting parameters for host or interface configuration reconciled with each other, or, if not reconcilable, which parameters have precedence? Hosts with multiple interfaces are more likely to be confronted with this issue, but the issue may also come up for hosts with a single interface.

It is important therefore to detail the various scenarios cases to provide a framework for understanding the implications on problem statement requirements for defining the appropriate behavior of an IPv4 or IPv6 stack and what protocols would be to manage these cases. Below these scenarios are enumerated. They will help in understanding better the requirements and implications for solutions to these requirements.

2. Problem Statement Requirements

The MIF problem statement requirements are enumerated as:

2.1. General Requirements

- R0 - MIF must work with both IPv4 and IPv6 addresses. Any of these combinations of addresses must be supported. For example,
one network connection may be IPv4 and another IPv6.

- R1 - MIF must support one or more network interfaces which can be physical, logical or virtual.

- R2 - Network configuration parameters may come from different administrative domains. MIF must be able to handle network connection services that may be administered by different organizations. In some deployments, the network services may not be administered by the same organization or people, such as in a community wireless environment. This poses challenges for the host to have consistency of data offered by network connection services.

- R3 - MIF solution must be compatible with existing IPv4, IPv6 architecture and protocols.

- R4 - MIF does not require to support IP mobility management protocols (e.g. MIPv6, MIPv4) and is not part of the problem scope.

- R5 - MIF must support the ability of communication to happen simultaneously or independently over multiple network connections.

2.2. Requirements on merging of IP layer autoconfiguration

- R6 - MIF must be capable of collecting the global/local configuration objects from different interfaces.

- R7 - MIF must support specific policies to merge the configuration objects when they are conflicting.

- R8 - MIF must provide the way to users/network to exchange the policies for merging of configurations.

- R9 - MIF node must provide the way to update the configurations.

2.3. Split DNS

- R10 - MIF must be able to get DNS services from different networks.

- R11 - MIF must be configured with policies for DNS service access.

- R12 - MIF must provide the way to users/network to change the policies for DNS access.
3. Scenarios for Multi-interfaced Hosts

The MIF work is looking at a multi-homed host whereby it receives node configuration information from each of its access networks. This section enumerates scenarios of multi-homed hosts so that analysis can be made to the problem goals of the IETF work.

Combinations of the above - configurations with both multiple network interfaces and multiple IP addresses assigned to some or all of these interfaces - are also possible.

3.1. Sets of services are the same

Here the host has two or more unlimited Internet Connections. The sets of services for these connections are the same.

A and B are Internet connections both having the same set of services.

```
(     A, B      )
(               )
\___________/
          /           \
         /             \
        (               )
        /           /\          \
       (               )          \
      /     _____________/          \
     (               )              \
    /           /               /        \
   (               )               /        \
  /               /     _____________/      \
 (               )                     \
 /______/
```

Case I: Same set of services

Figure 1

3.2. Set of services are different

Next on the list of complexity is the scenario case a host has multiple Internet connections but the set of services for these are different. Here the host for example may have a physical and/or logical VPN connection to different private networks and services. Another example is connecting a host to 2 logically separate but physically connected networks. In this case a host has one Internet connection and one VPN connection through which only private network and services can be reached.
In the diagram A and B are the Internet Connections of a host each having a different set of services associated with them.

```
        ___         ___
       /   \       /   \            
      (    )     (    )      Case II: Different set of services
         \      /          Figure 2
        \______/         

3.3. Set of services are partially overlapping

Here the multi-connected host networking services are partially overlapping.

Connection A and B having overlapping services.

```

```
       ___         ___
      /   \       /   \              
     (    )     (    )    Case III: Partially overlapping set of services
        \      /                Figure 3
       \______/                  

3.4. Inclusion of a set of services

In this usage scenario services provided by one network the host connects to are completely included by the provision of another. For example, the host has one Internet connection and one VPN connection, while it can also access the Internet services through NATs and proxies provided in the VPN besides some private services.
3.5. Combination of services

A realistic scenario is the combination of the above mentioned scenarios. A multi-homed host has multiple network interfaces both physical and logical. If the host has all physical connections, the host may be connected to different networks through various ways, for instance, wired LAN, 802.11 LAN or a 3G cellular network. For the case that multiple interfaces on the same network, connection issues should be handled by lower-layer protocols, the MIF focuses on upper-layer routing and service reachability. If there is one logical connection the host may have logical connections built on its physical connection, this may be handled by some third-party tools. While the data forwarding process needs to be defined further such as in a BCP document.

4. Implication of usage scenarios on Multi-homed requirements

Analysis of these case scenarios will enable a more meaningful perspective on the requirement solution space. Requirement implications include:

- The host with multiple network interfaces must be able to handle configuration information that may be gathered from multiple sources.

- The host must be able handle per-node and per-interface settings. Per interface settings can be complex because a client node needs to know from which interface system settings came from. And it may not be apparent which setting should be used, if e.g. if the service setting is received on multiple interfaces, potentially over different protocols.

- The host must be able to handle network connection services that may be administered by different organizations. In some
deployments, the network services may not be administered by the same organization or people, such as in a community wireless environment. This poses problems for consistency of data offered by network connection services.

- Multi-interface fixed nodes may start, stop and dynamically change flows and connection status. The host must be able to handle these dynamic changes that may be both host wide as well as interface specific. In addition, the host must be able to handle protocol startup sequence that may result from such changes.

- Different requirements of different applications can result in a different preference of the interface (physical or logical) that should be used. Network connections should be placed in the best possible interface based on these requirements. A fixed node should not only be enabled to connect to different networks simultaneously but also based on policies be able to dynamically assign desired flows to the best interface.

5. Related IETF Works

5.1. Relationship with current internet hosts ([RFC1122])

[RFC1122] specified the requirements on the internet host softwares related to link layer, IP layer, and transport layer. MIF will not change the basic routing policies of outbound packets in [RFC1122]. As for multihoming support, if the datagram is sent in response to a received datagram, MIF will also select the source address for the response SHOULD be the specific-destination address of the request, which is the same as the definition of [RFC1122]. Otherwise, more rules will be provided by MIF besides the specified rules to select the source addresses. The rules of MIF are applicable for both strong and weak end systems (ES). In MIF, An application is not required to explicitly specify the source address for initiating a connection or a request.

5.2. Network Discovery and Selection Problem ([RFC5113])

[RFC5113] defines the ways to help users to select which network to connect to and how to authenticate with that network, when multiple access networks are available. Basically, it divides the problems of network discovery and selection into multiple sub-problems, including Discovery of Points of Attachment, Identity Selection, AAA Routing, Network Capabilities Discovery, etc. Some constraints on potential solutions are outlined, and the limitations of several solutions (including existing ones) are discussed as well. In [RFC5113], the routing of data packets, in the situation where
mechanisms more advanced than destination-based routing are thought to be necessary. But, it explicitly specified that payload routings not discussed further in [RFC5113]. MIF will have solution for this issue. MIF will rely on [RFC5113] for network discovery and selection. Before the MIF works for routing/configuration/split DNS, the network discovery and attachment must be finished beforehand by way of [RFC5113]. In this sense, MIF will not cover the network selection and discovery at all.

5.3. PMIPv6 & Monami6

As discussed in early section, the solutions of both multihoming support in MEXT and NetLMM need the support from Home Agent (HA) or Local Mobility Anchor (LMA). MIF will work on multiple interfaces solutions of generic simple IP model. Furthermore, from an IP perspective, there is only a single interface with PMIPv6 and any network changes happen within the network. However, some experiences in these working groups will be good references in MIF as well.

5.4. Default address selection (RFC3484)

[RFC3484] proposed default address selection and destination address for IPv6 could be a reference to MIF work. On-going work is being done with issues of default address selection in [I-D.chown-addr-select-considerations]

5.5. Site Multi-homing of IPv6 (SHIM6)

SHIM6 provides multi-homed site with a new sub-layer (shim) into the IP stack of end-system hosts, for the purposes of redundancy, load sharing, operational policy or cost. It will enable hosts on multi-homed sites to use a set of provider-assigned IP address prefixes and switch between them without upsetting transport protocols or applications. It’s different from MIF in the following two items:

- SHIM6 only schedules the interfaces for the purposes of redundancy, load sharing, etc.
- SHIM6 is more on switching the prefixes without the involvement of transport protocols or applications. SHIM6 assumes the configuration of multiple interfaces has been done beforehand. MIF will work on the reconciliation of these configuration objects.
6. Security Considerations

MIF must have the security capabilities to protect MIF node from any malicious attempts caused by security holes such as denial of service attacks. The MIF solution must not compromise the security architecture of the basic IPv4/IPv6 networks. MIF is required to provide an admission control mechanism to regulate any MIF events. MIF could rely on the security mechanism of each interface on MIF node. Mechanisms used by MIF to exchange policies MUST support security feature to protect this flow of information.

This document doesn’t intend to provide the MIF security analysis but one will be required.

7. IANA Considerations

This document makes no requests to IANA.

8. Informative References

[I-D.blanchet-mif-problem-statement]

[I-D.chown-addr-select-considerations]

[I-D.savolainen-6man-fqdn-based-if-selection]

[I-D.savolainen-mif-dns-server-selection]
Savolainen, T., "DNS Server Selection on Multi-Homed Hosts", draft-savolainen-mif-dns-server-selection-00 (work in progress), February 2009.


Authors’ Addresses

Carl Williams
ZTE
Consultant
Palo Alto
United States

Email: carl.williams@mcsr-labs.org

Jacni Qin
ZTE
Shanghai
China

Email: jacniq@gmail.com

Williams & Qin Expires January 7, 2010