Multihoming in IPv6

Mobile Networks

Internship Report realized in WIDE Project

Master of Network Computer Engineering

September 2003

Julien Charbon

Under the supervision of Thierry Ernst, Keio University, Japan and
Thomas Noël, Louis Pasteur, University, Strasbourg, France.

Multihoming in IPv6 Mobile Networks

by Julien Charbon

Published Tuesday 26 September

Objectives

This document reports the author's activities during his master degree internship in the WIDE's Nautilus team in Japan.

The aims of this internship are:

- To evaluate the current NEMO IETF specification's ability ti support multihoming.
- To study the State-of-The-Art of multihoming in computer network, especially the multihoming under Network Mobility (NEMO).
- To test a NEMO implementation, then validate the concept and measure the benefits of multihoming.
- To report results and observations to the NEMO IETF working group.
- To administrate of the team network.

In a larger view, this internship is a chance to demonstrate skills and knowledge in an international collaboration project to improve the standardization and deployement of network protocols.

Acknowledgements

I want to thank each people who make this project possible:

Dr. Thierry Ernst. My supervisor in this internship for his self-denial to create this collaboration, for resolving with patience the numerous difficulties in the management this kind of project, and all his technicals and engineering precious advices to permit me to achive my task in the best conditions.

Pr. Jun Murai. For his welcome to his Laboratory, and his essential support to this international collaboration project.

Dr. Thomas Noël. The director of Network Computer Science DESS in Strasbourg, for his agreement and advices.

Koshiro Mitsuya. My main partner in this internship for his work, his kindness and his effort to explain me the Japaneses behavior.

WIDE Project. I thank the WIDE Project for its open view on international partnership.

Louis Pasteur University. I thank my origin University, and especially the "International Relationship" departement and the Network Computer Science DESS administration for their work to manage all the necessary documents and approvals needed for this experience.

Keio University. I thank the Keio University and the administration of Jun Murai Laboratory for resolving the several practical issues find by a foreigner in Japan.

Table of Contents

Chapter 1. Introduction

This internship took place in the WIDE Project's [WIDE-Web] Nautilus Working Group. In this chapter we briefly present the study area, the working group environment and we overview the goals of the internship.

1. Ubiquitous Internet

As focused in [Nautilus-Presentation] the next generation of computer network and devices would be:

o Always on the Internet: From anywhere, anytime: home, school, office, in the street, in transportation - Train, bus, car, *etc*....

o Heterogeneous: More and more medias provide a network access especially wireless access: 802.11, BlueTooth, GPRS, UMTS, Satellite, *etc*...

o Unified by IPv6: The next generation Internet Protocol version 6 should be the common protocol to exchange data on the global network.

o Mobile: The IP network would provide uninterrupted connection support for network nodes in motion.

To achieve this ubiquitous Internet in the real world many other mechanisms have to be provided to reach the deployment phase:

o Auto-configuration: To get a connection from all Access Points.

o Security & Authorization: To insure secure connection, and capabilities to Internet Service Providers to manage the customer connection.

o IPv4 to IPv6 transition: To get smooth transition and a compatibility between both devices: IPv4 & Ipv6.

o Quality of Service: To use efficiently each Internet connection

o Seamless mobility: To provide real-time services like Voice-over-IP, Videoconference without interruption in mobility cases.

Some of these mechanisms are already specified and implemented [IPv6, Auto-configuration, IPsec], some other are still in a research status or not yet completely specified [MIP6, NEMO, Seamless Mobility]. All of these technologies are studyed in the WIDE Project's working groups.

2. Nautilus Project Nautilus6

The aim of Nautilus is to achieve the ubiquitous Internet. To reach this goal this working group studies all related technologies:

- Host mobility with IPv6: Mobile IPv6.
- Network mobility: NEMO.
- Seamless Mobility: fast handover, FMIP and other.

- Security & Access Control, Radius, IPsec, and other.
- Multihoming: site-multihoming, multi-interface, etc...
- Services & Applications: Develop the applications to demonstrate these technologies.

Network mobility and multihoming being the two major parts of this internship.

3. Goals and Tasks

Multihoming & Network Mobility. The first goal was to study, define and identify the "multihoming" concept [Section 1.2, “Multihomibg in Fixed Networks”].

Evaluation, Testing & Report:

- Describe NEMO tests under identified multihomed cases.
- Test the Nautilus implementation and benchmark the results and compare with non-multihomed cases.
- Report the results to the NEMO IETF working group.

Chapter 2. Multihoming and Network Mobility Overview

This chapter introduces the concepts of Network Mobility, multihoming and explains in which cases and for which reasons a mobile network should be multihomed.

1. General Principles

This section describes the domains of studies of Network Mobility and multihoming.

1.1. Network Mobility

The goal of the network mobility study is to describe the operations of the Internet for supporting mobile networks.

Definition

> A mobile network is an entire network, moving as a unit, which dynamically changes its point of attachment to the Internet and thus its reachability in the topology. The mobile network is connected to the global Internet via one or more mobile(s) router(s) [NEMO-Terminology].

Network Mobility is a key feature to realize the ubiquitous Internet for in motion network nodes. A typical example of a mobile network is a vehicle connected to the Internet via multiple wireless medium, as investigated in the InternetCar project [InternetCar-Web].

As said in [InternetCar], other cases of mobile networks include PANs (small networks attached to people and composed of Internet appliances like PDAs, mobile phones, digital cameras, etc.), networks of sensors deployed in vehicles (aircrafts, boats, buses, trains), and access networks deployed in public transportation (taxis, trains, aircrafts, trucks and personal cars) to provide Internet access to devices carried by their passengers (laptop, camera, mobile phone, and even PANs).

Thus, the nodes inside the mobile network include micro devices such as sensors, wearable devices on passengers, and system controlling units such as engines. It is a waste of network and device resources to run a host mobility protocol such as Mobile IPv6 [MIPv6] on all the devices mentioned above, therefore it is reasonable to aggregate mobility support to a single router in each automobile. Devices include tiny sensors that are incapable of supporting extended protocol stacks other than IPv6.

To ensure continuous connectivity to the Internet, at anytime, any place, the mobile network is best connected via several interfaces, several access technologies and to distinct access networks, which is referred to as multihoming. Distinct interfaces should indeed be active simultaneously. As a result, the system must thus be able to deal with both horizontal handovers - between different point of attachments using the same communication medium - and vertical handovers - between different communication medium - and must cope with failures. As a wide coverage cannot be ensured by a single Internet Service Provider (ISP), handovers may need to be performed between distinct administrative domains and thus topologically distant parts of the Internet (Global Mobility). For instance, this either may occur when a vehicle crosses country boundaries, or when access is offered by different ISPs.

The latter is effective to keep communication costs low from a user's point of view. Having multiple point of attachment is also effective to avoid disruption of service when either a particular technology is not available in the geographic area or when one is experiencing some sort of failure. For instance, one can use 802.11b near parking lots or when traffic jams occur, and the mobile phone in areas with typically low traffic density.

Moreover when several similar Internet connection are available at the same time - and like the multihomed fixed networks - the network traffic can be share between them to optimize the available bandwidth utilization. If the connection have different characteristics - of bandwidth, latency, costs - the traffic can be distributed according some policy rules. This improvement is important for mobile networks otherwise there would be just one bi-directional tunnel between the mobile network and its Home Agent to reach the Internet [Section 1.1.1.2, “NEMO Basic Support”], which is a obvious bottleneck for the traffic. By creating several bi-directionnal tunnels, and use it efficiently at the time, this limitation can be avoided.

1.1.1. Network Mobility at the IETF

The IETF Working Group NEtwork Mobility (NEMO) is standarzing a solution to manage the network mobility. The NEMO WG specifies a unique solution for *Network Mobility Basic Support*; *i.e.* allow all nodes in the mobile network to be reachable via permanent IP addresses, as well as maintain ongoing sessions as the mobile network changes it(s) point(s) of attachment to the Internet. The WG is not yet working on routing optimizations between the mobile network nodes and their correspondants.

1.1.1.1. NEMO Terminology

According on [Mobility-Terminology]

Mobile Network. An entire network, moving as a unit, which dynamically changes its point of attachment to the Internet and thus its reachability in the topology. The mobile network is composed by one or more IP-subnets and is connected to the global Internet via one or more Mobile Routers (MR). The internal configuration of the mobile network is assumed to be relatively stable with respect to the MR.

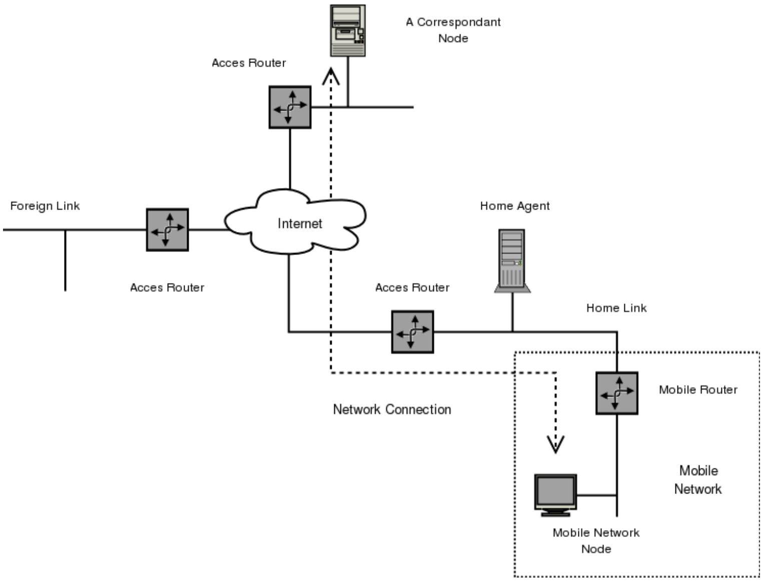
Mobile Router. A router capable of changing its point of attachment to the network, moving from one link to another link. The MR is capable of forwarding packets between two or more interfaces, and possibly running a dynamic routing protocol modifying the state by which to do packet forwarding.

Mobile Network Node (MNN). Any node (host or router) located within a mobile network, either permanently or temporarily. A Mobile Network Node may either be a mobile node or a fixed node.

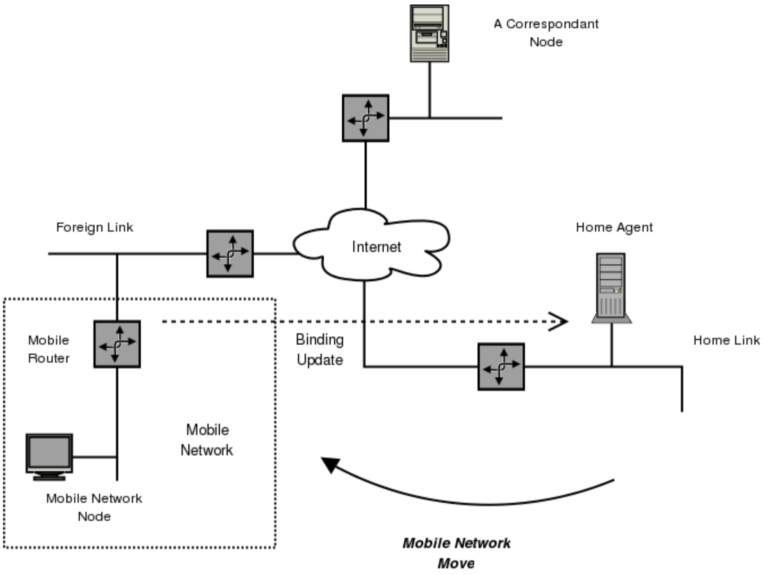
Access Router (AR). An Access Network Router residing on the edge of an Access Network and connected to one or more Access Points. The Access Points may be of different technology. An Access Router offers IP connectivity to Mobile Nodes, acting as a default router to the Mobile Nodes it is currently serving. The Access Router may include intelligence beyond a simple forwarding service offered by ordinary IP routers.

1.1.1.2. NEMO Basic Support

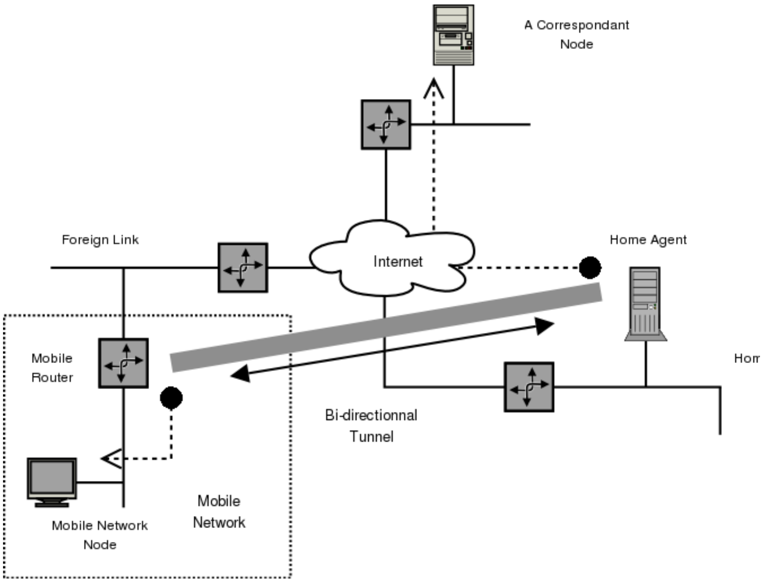
The NEMO WG will use a protocol based on Mobile IPv6 [MIPv6] and the use of a bi-directionnal tunnel [NEMO-Requirements]. The next figures illustrate the concept of this solution:



1. The mobile network is on his *Home Link* and a network session between a Correspondent Node; and a Mobile Network Node inside the mobile network is established.



2. The mobile network changes this point of attachment to the Internet, then the Mobile Router send a *Binding Update* message to his *Home Agent* to provide him his new reachable address [*i.e.* his *Care-of Address*].



3. A bi-directional tunnel is established between the mobile router and its *Home Agent*. All the traffic exchanged between the Mobile Network Node and the Correspondent Node; transit through this tunnel. The previous connection between them is preserved.

1.1.1.3. Major Problems

- Management of the routing table at the *Home Agent* and at the mobile router with the bi-directionnal tunnel, and with all the routing protocols that run inside [NEMO-MRHA].

- Security threats.

- Management of nested mobile networks - *i.e.* a mobile network inside an other mobile network - [NEMO-Nested].

- How to support multihoming [NEMO-Multihoming]. It is important for the future deployment of the mobile network. Indeed in numerous scenarios mobile networks will be multihomed with some interfaces which provided different connexion types like 802.11 for bandwidth, UMTS for a larger cover, and finally GSM or maybe a satellite connection for keeping connectivity while away from a HotSpot.

1.2. Multihomibg in Fixed Networks

Multihoming cases has no formal definition and cover many scenarios. We can see three cases: the first is with a single network interface, which has been assigned multiple IP addresses, and the second is multiple network interfaces on a same network node [Multihoming-IPv6]. We add a third case at a higher scale *Site Multihoming*: when "a network site has more than one connection to the public Internet" [Multi6-Charter].

1.2.1. Goals & Issues

Multihoming can provide numerous services [Multihoming-Requirements] :

- **Redundancy/Fault-tolerance.** When an address is not reachable anymore or when a link goes down or a router fails, the reachability to the Internet can be provided from the others addresses, links or routers. The continuity of the connectivity should be transparent for the application layer.

- **Load Sharing.** The multi-homed host/site should be able to distribute upstream and downstream traffic between his interfaces/border routers.

- **Traffic Policy.** The multi-homed host/site should be able to define some policies to manage the network traffic for reasons of costs, traffic requirements, users preferences, social policy, *etc*...

But, depending on the service offer, there are many problems to solve :

- **Routing scalability.** Multihoming heavily increases the size of the routing table. Actually it is a problem mainly for routers located in the backbone of the Internet. These routers have no default route [*a.k.a.* Default Free Zone - DFZ] and must know every route for all top-providers. It is one of the most important points because it is essential to other benefits [Analyze-BGP] [Multihoming-Requirements].

- **Transport-Layer Transparency.** Change of address/link/router after a multihoming decision should be transparency for transport-layer session. Otherwise the benefits of the Redundancy / Fault-Tolerance is lost.

- **DNS Issues.** It is a host issue: how to deal with multiple address for a single host?

- **Packet Filtering / Ingress Filtering.** In general a provider filter his customer's traffic and permits only transit to the Internet for packets with addresses provided to customers.

- **Address selection.** To offer load-sharing and policy behavior the network node must make a source and destination address selection, for each packet or stream of packets.

For these cases, NEMO Basic Support is a solution for providing mobility support to an entire network. As we will see in the next section the multihoming supportcan improve the reliability of the mobile network. We detailed this in [IEICE].

1.3. Multihomed Mobile Network Taxonomy

According to [NEMO-Terminology] a mobile network is multihomed in the following situation:

Multihomed Mobile Network

- a MR has multiple egress interfaces on the same link, or

- a MR has multiple egress interfaces on distinct link, or

- there are more than one MR in the mobile network

We need a taxonomy to classify each essential case of multihomed mobile network according to several discriminant parameters. We have designed such taxonomy in collaboration with Mr Chan-Wah from Panasonic Singapore Laboratories. This has beed reported in an Internet-Draft [NEMO-Multihoming].

1.3.1. Classification

There are various configurations of a multi-homed mobile network, depending on how many mobile routers are present, how many egress interfaces and home addresses the mobile routers have, how many subnet prefixes are advertised to the mobile network nodes, etc. Here, we identify three key parameters differentiating different multihomed configurations. With these parameters, we can refer to each configuration by the 3-tuple (w,x,y), where 'w', 'x', 'y' are defined as follows:

- 'w' indicates the number of MRs. This differentiates the case of single mobile router (with multiple egress interfaces or multiple home addresses) versus the case of multiple mobile routers, where:

  w = 1 Implies that a mobile network has only a single mobile router. In this case, the mobile router either has multiple egress interfaces or multiple home addresses bound to a single egress interface.

  w = N Implies a mobile network has more than one mobile router advertising an egress route.

- 'x' indicates the number of HAs. This differentiates the case of a single home agent for the mobile network versus the case of multiple home agents for the mobile network, where:

  x = 1 Implies that a single home agent is assigned to manage binding updates of the mobile network.

  x = N Implies that more than one home agents (possibly in different administrative domains) manage the binding updates of the mobile network.

- 'y' indicates the number of mobile network prefix. This differentiates the case of single mobile network prefix versus multiple mobile network prefixes that is/are advertised to the mobile network node, where

  y = 1 Implies that a single subnet prefix is advertised to the mobile network nodes.

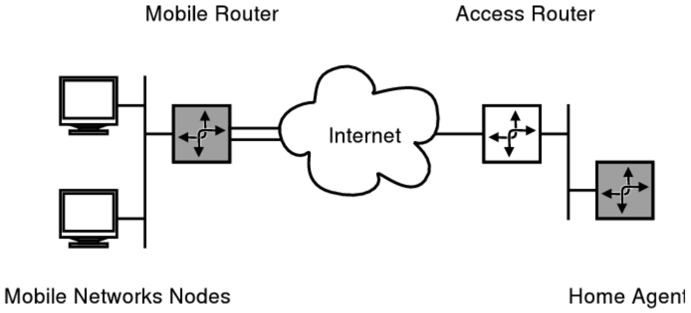
  y = N Implies that more than one subnet prefixes are advertised to the mobile network nodes.

It can be seen that the above three parameters are fairly orthogonal to one another. Thus different values of 'w', 'x' and 'y' give rise to different combinations of the 3-tuple (w,x,y). A total of 8 possible configurations can be identified.

1.3.2. Taxonomy examples

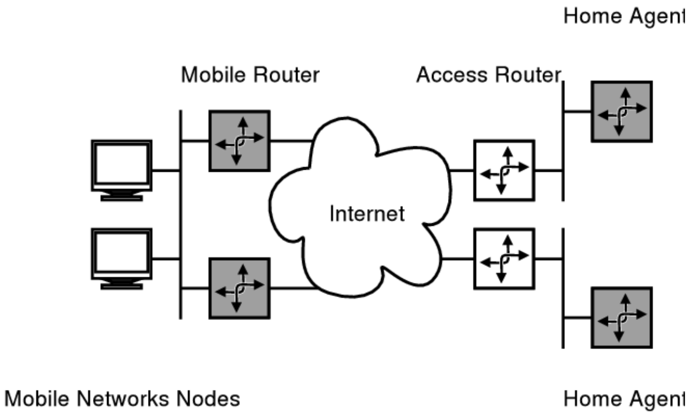
Few practical example to show application of this taxonomy:

Case 0,0,0: Single Mobile Router, Single Home Agent, Single Mobile Network Prefix.



This case is one of the most typical multihoming scenario. While on the move, each interface of the MR is associated with a CoA on their respective point of attachment. Multiple CoAs can thus simultaneously be chosen from to transmit the mobile network traffic.

Case 1,1,0: Multiple mobile routers, Multiple home agents, Single mobile network prefix. .



In this case each MR independently maintains its own bidirectional tunnel.

The other cases are illustrated in [NEMO-Multihoming][ICMU-2004].

2. Multihoming Support in NEMO Basic Support

One requirement for NEMO Basic Support is to not prevent the use of multihoming. We analyze the IETF NEMO Basic Support solution and we report the result in an Internet-Draft [NEMO-Evaluation] which describes and explains prerequisites to support multihoming. We study those prerequisites with respect to each case of a taxonomy proposed to the NEMO WG and we analyze how the IETF NEMO basic support solution fits with them. The analysis of each case listed in this taxonomy is broken into three parts, prerequisites, comments, and solution behaviors. The prerequisites are split in three categories: Prerequisites to support Redundancy, prerequisites to support Load-Sharing and prerequisites to support Policy.

A example of analysis on one case:

```
Case (1,1,1)

   Illustration of the case:


                         _____
         _    p      _  |     |
        |_|-| -_  |-|_|-|     |-|        _
         _  |-|_|=|     |_____| |  _  |-|_|
        |_|-|     |             |-|_|-|
                                      |

       MNNs    MR   AR  Internet  AR    HA


Prerequisites

   o Redundancy:

      If an interface/the link is broken, use the other: No additional
      prerequisites at NEMO level.  But for efficient support of this
      benefit the layer 2 have to send interface/link informations or
      orders to NEMO.  This redundancy is always transparent: Read
      "Fault-Tolerance and the MNNs" in (section 2.2).

      But this behavior is not sufficient with respect to the requirements:
```

- o Load-Sharing:

  For this class the solution MUST at least:

  1. Allow the use of several active bi-directional tunnels simultaneously between MR and HA.

  2. Allow the binding of multiple CoAs against the same Mobile Network Prefix.

  3. Provide a method to identify which CoA a Prefix-BU is meant to update. Read "CoA Identification" in (Section 2.2).

  In this case the MR and the HA MUST use the two bi-directional tunnels simultaneously.

  * Outbound Traffic: the MR distributes the traffic between its CoAs.

    There is no assumption on the distribution mechanism.

  * Inbound Traffic: the HA distributes the traffic between MR's CoAs.

    The distribution can be statically fixed or dynamic: a preference can be sent with each Prefix-BU to mark the preference of each CoA in the HA's Binding Cache.

- o Policy:

  * Outbound Traffic: this behavior depends on the NEMO implementation. There is no way to impose an algorithm.

  * Inbound Traffic: Provide a policy field or policy sub-option with each Prefix-BU to indicate a policy management for each CoA to the HA.

Etc...

And the main conclusion of this draft is:

In this IETF draft, we explore the level of Multi-homing support available in the NEMO Basic Support solution with respect to Multi-homing requirements, the main goal being:

> "Do not prevent Multi-homing configurations/benefits by the using of NEMO Basic Support."

This goal is mainly respected. However, based on our analysis, we propose some improvements.

- o Preference & Priority:

  This information permits to manage the sharing/the policy of the inbound traffic to the mobile network through several CoAs and/or several HAs.

  This information could be added to the Prefix-BU. The proposed solution should specify a field/an sub-option to permit some implementation to provide this benefit; or this feature should be specified in the next generation of NEMO protocol.

- o Multiple CoAs for the same MNP:

  The proposed solution doesn't have to specify anything for this. However a paragraph on this purpose can be helpful for implementation's developers.

The problem of multihoming in network mobility covers many specifications and network domains, which makes the ideas about this subject interesting but difficult to fix. We hope that this document can trigger further discussions on the multihoming aspect of NEMO basic solution.

Chapter 3. State of the Art in Multihoming

As we saw in [Section 1.2, “Multihomibg in Fixed Networks”] the multihoming cover numerous cases. Now with IPv6, it's either possible to repeat the same mistakes as IPv4 or try to them. I'll focus on the latter, as the adoption of IPv6 gives a possibility to start from good basis.

1. Transport Solutions

A TCP connection is always established between two end-points, using one IP address for each, even if the nodes would have multiple addresses. If the network connectivity using the addresses between the end-points is lost, the connection would be rendered unusable for the duration of the loss, or it would time out and be terminated in the event the loss lasts long enough.

Stream Control Transmission Protocol (SCTP) [SCTP] is a new, reliable connection-oriented protocol. The main differences from TCP are that it is possible to accept non-ordered delivery of packets in a stream, and that every SCTP association can have multiple end-points.

When the connection is established, multiple addresses can be listed as end-points for the node. During the connection, each of these possible alternative paths are probed with "heartbeat" packets, to see that they're operational. So, if one network path fails, SCTP can switch to another end-to-end path, if set up, when it noticed the problem.

Transport solutions, such as TCP modifications and SCTP have a major problem: such modifications would have to be deployed everywhere so that they could be depended on, and all the connection-oriented. Maybe maybe even some connectionless protocols would have to solve the same problem multiple times.

Ignoring the initial issus to these proposals, several points can be underlined. The TCP modifications must be backward-compatible due to the huge installed base, to extent of classic TCP sessions.

In summary SCTP is likely to be deployed at least in a few relatively restricted environments, but not as a global solution; however, the application interface also has a TCP-like syntax, so changing the applications to use SCTP rather than TCP is a small effort.

Protocols such as SCTP are undoubtedly useful in certain specific applications but are unlikely to become popular in the global perspective.

2. Identifier and Locator Separation

IP addresses include two entirely separate functions: the address or the locator of the node (*i.e.* how to get there), and the identifier of the end-point (*i.e.* the name of the node). The semantics of IP address have been overloaded to include both.

The former is used to forward packets in routers, mostly, and the latter in the protocols like TCP and UDP to identify the end-points of connections or packets. It is understandable that these have been bundled in one: in simple nodes with only one stable address, these are the one and the same; indeed, this was the initial Internet architecture. However, when a node has multiple addresses with different network connectivity properties, this becomes an extremely challenging problem. The protocols in a node should be able to process packets belonging to a connection, regardless of how they reached the destination, and vice versa.

2.1. LIN6

In LIN6 [LIN6], the mapping function is basically done between an interface-ID derived from the "assumed-globally-unique" Ethernet MAC-address. It is not evident that this kind of mapping can be made reasonably secure or scalable, or that the particular approach to deriving globally unique identifiers would the best one.

In addition, LIN6 has patents or patent claims associated with it, making the approach difficult as a requirement for protocols providing multihoming.

2.2. HIP

Host Identity Payload and Protocol (HIP) [HIP] is a proposal to separate locators and identifiers. The proposal is to create a virtual Host Identity-layer between the Internet and transport layers. The idea is that all packets themselves contain the locator, as before, but the end-nodes use the addresses of the Host Identities at the transport layer. In consequence, the addresses used for packets can change freely without disrupting the sessions which are bound to Host Identities.

In HIP, the emphasis is on security from the start. However, one could say that security is also a weak point, if one would consider it being adopted globally. HIP uses a "rendezvous service" to map Host Identities to addresses. A problem is that the mapping must be secured using DNSSEC or a similar mechanism; otherwise there is no guarantee that the other endpoint's IP address that was returned from the rendezvous service really belongs to the party with the Host Identity.

Another issue with security, from a completely different point of view, is the use of encryption on all the traffic. It is typical that different entities like enterprises want to be able to monitor and set policies on the traffic, for example in firewalls. This is not possible with encryption; the policy-making process is either pushed to the end-nodes or one must use some kind of security gateways to act as a proxy for all the traffic.

Of course, the HIP protocol could probably be modified so that the end-nodes could also negotiate an unencrypted but authenticated association, depending on the wishes of the end-hosts, or use a proxied HIP to begin with. The experience and specification of HIP is still at an early stage.

2.3. Mobile IPv6

Mobile IPv6 [MIPv6] solves the problem of connections breaking when the IP address changes in the multihoming context. However, this does not really solve the problem as is, just shifts it around: an approach like this would require the Home Agents to be addressed and located in such a place in the network topology that they would not be affected by the outages. This is typically not the case. A Homeless Mobile IPv6 approach has been proposed but withdrawn by the authors; in this case, something like HIP is closer to the right solution.

The issue is that in order for the Correspondent Node to verify the Binding Update sent by a multihomed node the primary connectivity of which has failed, it must verify that the Care-of and Home Addresses are routed at the same node. However, in the case of multihoming-related network outage, by definition the previously used Care-of Address is no longer operational and the verification will not succeed. If a global Public Key Infrastructure was in place, it might be possible to authenticate the modified Binding Updates so that connections could survive; however, this does not seem to be realistic in the short term.

The proposal for the operation of the modified Binding Update has not been written out, so it is difficult to analyze whether sufficient security properties could be obtained without an explicit home agent.

2.4.

To summarize the locator/identifier mechanisms, LIN6 does not seem reasonable, standard Mobile IPv6 does not work, but a modified version could be explored, and HIP appears to be the most interesting architectural proposal in the long term.

Locator/identifier solutions build on having multiple addresses per node and solve the connection survivability problem.

3. Host-Centric IPv6 Multihoming

[TODO: Put the picture here]

The idea of this framework proposal [Host-Centric] is that sites connect to and obtain IP address prefixes from multiple ISPs, here A, B and C, D for sites X and Y, respectively. Each node has multiple addresses, and all addresses are configured in the DNS and other relevant registries and configuration databases.

In consequence, when Host X wishes to communicate with Host Y, it will typically perform a DNS lookup which gives two addresses. Host X will perform default address selection, which picks up the best source/destination address pair. This will be used throughout that particular communication with Host Y. The acknowledged problem with this model is that many ISPs nowadays perform ingress filtering; that is, they check that the source address of packets coming from their customer is one of those assigned to the customer. For example, ISP A would check that packets coming from Site X would be part of the prefix assigned to Site X by ISP A. With multiple addresses from difeerent providers, many packets would also include the source address from the prefix of ISP B; these packets would be discarded.

The host-centric IPv6 multihoming is a framework of all nodes having multiple addresses and the hosts being in control of many of the multihoming decisions. The most prominent issue with nodes using addresses from different providers is the correct source address selection. Disabling ingress filtering between the ISP and the site is not a realistic recommendation for the safety of the Internet. Using multiple addresses also requires additional solutions if connection survivability is desired.

The requirements for the mechanism to work are: 1. source nodes will be able to pick up a working source address, if not first, at least eventually, and 2. packets with the source address belonging to ISP X will be routed to the site-border router with an active interface to ISP X, and forwarded there.

The first requirement may not have to be solved if one can assume that connectivity to all the providers is always maintained, e.g. through a tunnel as described next. If this cannot be assumed, the information of the failure of one link must be propagated to the end nodes somehow. This can be done by e.g. routers using ICMP to suggest picking the different source address this could possibly even be propagated to the first hop routers, by distributing information to reject traffic by the use of special routes. A few other techniques might also be possible.

The second requirement can be solved by requiring the use of source-based routing in all routers of the site or at least the site exit routers but that would induce a possible extra hop(s) for the traffic, the use of routing header by the source nodes to the site exit routers or tunneling to the site exit routers. A special case is when only one ISP is in primary use; this can be achieved with a default route with a very good metric which is propagated through the site's rout- ing system which overrides all the other sites' routes everywhere in the site. The end-nodes will have to support source-based routing or have their default address selection policy database modified to pick the source address belonging to the primary site; either of these could be automated in e.g. route advertisement mes- sages. Then, no additional infrastructure to support the model would be needed.

Host-centric IPv6 multihoming in itself provides multiple addresses per node, but does not solve the connection survivability problem. There are some details to be worked out yet. Outbound, and inbound in particular, load-balancing may be difficult if the policy has to be set at the edges as decisions are made by end-hosts.

4. IPv6 Multihoming at Site Exit Routers

The model of IPv6 multihoming at site exit routers is presented in [Exit-Routers-IPv6]; it is based on a slightly on a similar technique specified earlier for IPv4 [Exit-Routers]. The idea is that the site connects to more than one ISP using multiple border routers, obtains IP address prefixes from each ISP, and deploys multiple addresses on every node, exactly as described with host-centric multihoming, above.

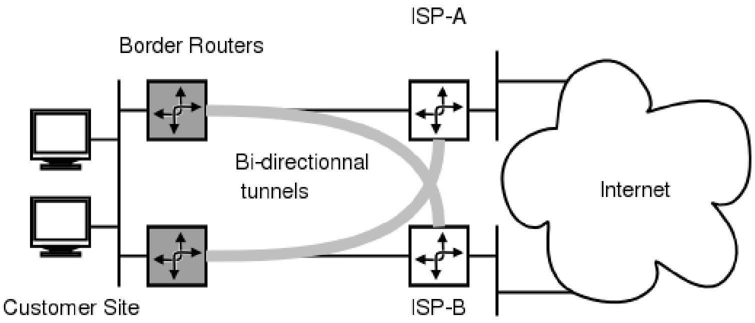


Illustration of IPv6 Multihoming at Site Exit Routers

This is very useful: in the normal case, if a link or router fails, connectivity to an ISP may be disturbed and connections using the addresses belonging to that ISP will break. Now, the connectivity is quickly restored and goes tunneled via a suboptimal path through the other ISP.

A concern specific to this model is that the Maximum Transmission Unit (MTU) of the physical links to both ISPs must be sufficiently large: over 1500 (MTU on Ethernet) bytes would be best. This is because tunneling will increase the packet size by at least 20 or 40 bytes, and the maximum sized packet that could originate in the site should still fit in the link even in the encapsulated format with extra bytes. If this is not possible, one will have to rely on Path MTU Discovery, which is suboptimal, or configure a lower MTU everywhere in the site.

Multihoming at site exit routers in itself provides multiple addresses per node, does not solve the connection survivability problem completely but reduce it dramati- cally so that it may not any longer be a problem. There are some details to be worked out yet. The sites should seriously consider link MTU's on connectivity they obtain. Outbound, and inbound in particular, load-balancing may be difficult if the policy has to be set at the edges as decisions are made by end-hosts.

5. Geographic Address Allocation

There are, and have been for a long time, a lot of proposals to allocate IP addresses in geographic fashion, making them independent of the network topology [GEO].

The fundamental, and acknowledged, problem with these is that the model, more or less, requires a neutral party like an Internet Exchange with redundant-enough upstream connectivity to do it, or a billing structure for the advertisement service from someone who does. This is typically a very problematic situation.

Geographic addressing may first sound like a good idea, but in practice it is a very challenging concept. Avoiding renumbering when changing operators and deploying a simple IP address plan without multiple addresses per node is what may seem desirable to many sites. However, tying the numbering to geography may not be as useful as one might hope. It is not uncommon for sites to move from one place to another, at least in the mid-long term like 4-7 years. Renumbering would seem inevitable then anyway. This is not really all that different from the lifetime of ISPs.

Another significant problem with topology-independent addressing is global routing. Who is willing to advertise the aggregate for a region, when not all sites in that region are your customers and pay you for transit service? The alternative is advertising more specific "geo-IP" addresses from different ISPs, but that only makes the idea of geographic aggregation and allocation useless. What would be needed is either end-sites, or their direct ISP, paying explicitly to a sufficient number of separate transit ISPs to advertise the regional aggregates: a billing structure with a granularity of an end-site.

For the model to work to the sufficient degree, a requirement also has to be that regional traffic can be routed regionally, without going through a long way through other providers as this would increase the number of more specifics in the routing table. This is quite problematic especially in the areas of lower Internet connectivity penetration: it is rather usual that the traffic is transported a long distance until it is spread out to the Internet.

Geographic address allocation provides a long-lived address per node, and thus con- nection survivability is not a problem. Typically only outbound load-balancing is possible. It does not seem to be an operationally or economically realistic approach.

6. Provider Independent Addressing Derived from AS Numbers

The model creates a IP address space (ASN-IP) [ASN] syntactically for every end-site that has an AS number that is, the majority of people who could be multihoming today. The approach is not the best one, as it would lead to a possible land-rush for AS numbers, and then in turn, AS number space would be exhausted, forcing the move to longer ones and a protocol change.

However, the proposed solution is considered significantly better than some alternatives, like using more specific routes. In this model, the routes are clearly controllable and distinguishable from the rest, and cannot lead to a mess of more specific routes nobody knows what they're for, as with IPv4 today. At the end of 2002, origin-only AS numbers currently being used were about 10000. This doesn't seem like too high a number to satisfy current multihoming needs.

ASN-IP allocation provides a stable address per node for existing AS number holders, and thus connection survivability is not a problem. Both outbound and inbound load-balancing are possible. The model might have some uncertainties regarding the applicability as a long-term policy. However, if such advertisements would come from specific, well-defined address blocks, this might be a usable approach.

7. Conclusion

As you can see there is no master solution to manage the multihoming configuration and provide all expected benefits. But many ideas and many differents way to deal with this particular state. A new RFC fix the goals for IPv6 Site-Multihoming Architectures, [Multi6-Goals], but is said that: "There may be more than one approach to multihoming, provided all approaches are orthogonal. Multiple solutions will incur a greater management overhead, however, and the adopted solutions should attempt to cover as many multihoming scenarios and goals as possible."

Which is a clear summary of the current indecision inside the Multi6 IETF WG. Our preferred approach is to decide which qsolution is the best in which pratical case and argue for this one in the appropriate case. A global decision for extending a solution everywhere seems difficult without consesus, and the consensus can't happen with all these multihoming goals which don't discriminated a special solution. Anyway IPv6 deployement is already started and the time to choice between should be soon. A combination of several solution at once should be studied.

Chapter 4. Testing Multihoming Scenarios

1. Nautilus implementation

The Working Group has developed is own NEMO Basic Solution implementation based on the latest KAME kit.

The test serie is split in several step to parallelize the tasks implementing and testing.

1. Test the IPv6 KAME implementation behavior in the case of fixed network.

   Goal: Create a test template.

2. Test the behavior of a network connected to the Internet through a bi-directionnal tunnel.

   Goal: Create a serie of NEMO-related test.

3. Test the NEMO implementation in Multihoming case.

   Goal: Verify the multihoming support/benefits.

2. Test template

In order to describe efficiently the tests, we design a test template based on Tahi [TODO: Put link], and Connectathon [TODO: Put link].

The description of each test field is in Appendix B, *Test Template: Definition*.

2.1. Test example

Read the example test in Appendix C, *Test Example: Multihoming in Fixed Network*.

3. Reports

Report consist in comments and results discorver during the test.

3.1. Example

Read the report exemple in Appendix D, *Report Example: Multihoming in Fixed Network*

Chapter 5. Related Work

During this internship we make differents tasks like network installation, network administration, collaboration software management.

- Installation of Nautilus network: IPv6, IPv4, wired and wireless.
- Installation of Nautilus main server: jules.nautilus6.org with services like: SSH, Apache, CVS.
- Creation and maintenance of Nautilus Web site: http://www.nautilus6.org
- Documentation about Tests and Web site maintenance.

Chapter 6. Conclusion

This internship provide a chance to apply my skills and my knowledge in the aim to improve a next generation network protocol. Because this work has been accomplished inside a international team, it permit us to share our point of view in a same problematic.

Starting from the begining this project permit me to study two new domains in computer network: The multihoming and the Network Mobility. With this knowledge and collaboration in the IETF and with Keio University and WIDE people [master student, thesis student, professor, engineer], we create a taxonomy to identify each case of multihoming in NEMO.

Based on this taxonomy we evaluate the current NEMO Basic Support solution, and propose some improvements to the NEMO IETF WG. These drafts found an echo in the WG, and we get many feedbacks to customize them.

In parallel with these studies permit to design and use several pratical tests to show and demonstrate in real situation the support of multihoming by the Nautilus6 implementation.

Moreover, with the network administrative tasks, documentation writing and the collaborative tools management, most domain of competence of a engineer in research and development has been used.

The futur tasks of this work, are complete our tests and send reports to NEMO WG, and update our drafts to propose to NEMO WG a working group document on this topic. To finally specify in IETF's standard document the appropriate improvements for a full support of multihoming in Network Mobility.

Bibliography

Web Site

[WIDE-Web] *The WIDE Project*. URL [http://www.wide.ad.jp/] .

[Kame-Web] *The Kame Project*. WIDE Project. URL [http://www.kame.net/] .

[SOI-Web] *School Of Internet*. WIDE Project. URL [http://www.soi.wide.ad.jp/] .

[InternetCar-Web] *Internet Car*. WIDE Project. URL [http://www.sfc.wide.ad.jp/NACM/english/index.html] .

[Nautilus-Web] *Nautilus*. WIDE Project. URL [http://www.nautilus6.org] .

Internet White Papers

[Nautilus-Presentation] *Nautilus Presentation*. Nautilus. Presentation Url [http://www.nautilus6.org/doc/nautilus-widemeeting-0305/img0.html] .

[NEMO-Charter] *Network Mobility [Nemo] Charter*. I.E.T.F.. Charter Url [http://www.ietf.org/html.charters/nemo-charter.html] .

[Multi6-Charter] *Site Multihoming in IPv6 [Multi6] Charter*. I.E.T.F.. Charter Url [http://www.ietf.org/html.charters/multi6-charter.html] .

[MIPv6-Charter] *IP Routing for Wireless/Mobile Hosts [mobileip]*. I.E.T.F.. Charter Url [http://www.ietf.org/html.charters/mobileip-charter.html] .

[Analyze-BGP] *Analyzing the Internet's BGP Routing Table*. G. Huston. Document Url [Todo: It is not the official one] [http://macross.dynodns.net/idr/4-1-bgp.pdf] . January 2001.

IETF Internet Drafts and RFCs

[NEMO-Terminology] *Network Mobility Support Terminology*. Thierry Ernst and Hong-Yon Lach. I.E.T.F.. November, 2002. Draft Url [http://www.nal.motlabs.com/nemo/drafts/draft-ernst-nemo-terminology.txt] .

[HIP] *Host Identity Protocol*. R Moskowitz, P. Nikander, P. Jokela, and P. Nikander. I.E.T.F.. June 19, 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-moskowitz-hip-07.txt] .

[GEO] *Application and Use of the IPv6 Provider Independent Global Unicast Address Format* . T Hain. I.E.T.F.. August 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-hain-ipv6-pi-addr-use-05.txt] .

[ASN] *Multihoming Using IPv6 Addressing Derived from AS Numbers*. P Savola. I.E.T.F.. January 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-savola-multi6-asn-pi-00.txt] .

[Multi6-Goals] *Goals for IPv6 Site-Multihoming Architectures*. J. Abley, B. Black, and V. Gill. I.E.T.F.. August 2003. RFC Url [http://ietf.org/rfc/rfc3582.txt] .

[Host-Centric] *Host-Centric IPv6 Multihoming*. C. Huitema and P. Draves. I.E.T.F.. June 24, 2002. Draft Url [http://www.ispras.ru/~ipv6/docs/draft-huitema-multi6-hosts-01.txt] .

[LIN6] *LIN6: A Solution to Mobility and Multi-Homing in IPv6*. Fumio Teraoka, Masahiro Ishiyama, Mitsunobu Kunishi, and Atsushi Shionozaki. I.E.T.F.. 16 August 2001. Draft Url [http://www.lin6.net/draft/draft-teraoka-ipng-lin6-01.txt] .

[MIPv6] *Mobility Support in IPv6*. D. Johnson, C. Perkins, and J. Arkko. I.E.T.F.. June 30, 2003.

Draft Url [http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-24.txt] .

[Mobility-Terminology] *Mobility Related Terminology*. J. Manner and M. Kojo. I.E.T.F.. April, 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-ietf-seamoby-mobility-terminology-03.txt] .

[NEMO-Requirements] *Network Mobility Support Requirements*. Thierry Ernst. I.E.T.F.. February, 2003. Draft Url [http://www.nal.motlabs.com/nemo/drafts/draft-ernst-nemo-requirements.txt] .

[NEMO-MRHA] *Issues in Designing Mobile IPv6 Network Mobility with the MR-HA Bidirectional Tunnel [MRHA]*. A. Petrescu, M. Catalina-Gallego, C. Janneteau, H.-Y. Lach, and A. Olivereau. I.E.T.F.. March, 2003. Draft Url [http://www.nal.motlabs.com/nemo/drafts/draft-petrescu-nemo-mrha-02.txt].

[NEMO-AAA] *Usage Scenario and Requirements for AAA in Network Mobility Support*. C. W. Ng and T. Tanaka. I.E.T.F.. October, 2002. Draft Url [http://www.nal.motlabs.com/nemo/drafts/draft-ng-nemo-aaa-use.txt].

[NEMO-Multihoming] *Multihoming Issues in Bi-Directional Tunneling*. C. W. Ng and J. Charbon. I.E.T.F.. May, 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-ng-nemo-multihoming-issues-01.txt].

[NEMO-Evaluation] *valuating Multi-homing Support in NEMO Basic Solution*. J. Charbon and C. W. Ng. I.E.T.F.. July, 2003. Draft Url [http://www.ietf.org/internet-drafts/draft-charbon-nemo-multihoming-evaluation-00.txt] .

[NEMO-Nested] *IPv6 Reverse Routing Header and its application to Mobile Networks*. P. Thubert and M. Molteni. I.E.T.F.. October 11, 2002. Draft Url [http://www.nal.motlabs.com/nemo/drafts/draft-thubert-nemo-reverse-routing-header.txt] .

[Multihoming-Requirements] *RFC-3582 - Goals for IPv6 Site-Multihoming Architectures*. J. Abley, B. Black, and V. Gill. I.E.T.F.. August 2003. RFC Url [http://ietf.org/rfc/rfc3582.txt] .

[SCTP] *RFC-3309 - Stream Control Transmission Protocol (SCTP) Checksum Change*. J. Stone, R. Stewart, and D. Otis. I.E.T.F.. September 2002. RFC Url [http://ietf.org/rfc/rfc3309.txt] .

[Exit-Routers-IPv6] *RFC-3178 - IPv6 Multihoming Support at Site Exit Routers*. J. Hagino and H. Snyder. I.E.T.F.. October 2001. RFC Url [http://ietf.org/rfc/rfc3178.txt] .

[Exit-Routers] *RFC-2260 - Scalable Support for Multi-homed Multi-provider Connectivity*. T. Bates and Y. Rekhter. I.E.T.F.. January 1998. RFC Url [http://ietf.org/rfc/rfc2260.txt] .

Papers

[InternetCar] *Connecting Automobiles to the Internet*. T. Ernst and K. Uehara. WIDE Project & Keio University. November, 2002. ITST: 3rd International Workshop on ITS Telecommunications . Seoul, South Korea.

[ICMU-2004] *Multihoming in Network Mobility*. T. Ernst and J. Charbon. WIDE Project, Keio University & Louis Pasteur University. Paper in revision. *Submitted to*: ICMU 2004: First International Conference on Mobile Computing and Ubiquitous Networking. . Yokosuka, Japan.

[IEICE] *Enhanced Mobile Network Protocol for its Robustness and Policy Based Routing.* . R. Wakikawa, S. Koshiba, T. Ernst, J. Charbon, K. Uehara, and J. Murai. WIDE Project, Keio University & Louis Pasteur University. Paper in revision. *Submitted to* IEICE: Institute of Electronics, Information & Communication Engineers. . Yokosuka, Japan.

Thesis

[Multihoming-IPv6] *Multihoming with Internet Protocol Version 6*. Troels Walsted Hansen. I

Tromsø University - Norway. December 21, 2001. Thesis Url [http://www.vermicelli.pasta.cs.uit.no/ipv6/students/troels/html/thesis/thesis.html] .

[NEMO-IPv6] *Network Mobility Support in IPv6*. Thierry Ernst. University Joseph Fourier - France. October 29, 2001. Thesis Url [http://www.inria.fr/rrrt/tu-0714.html].

Appendix A. Presentation ot the Environment

1. The WIDE Project

"The aim of the WIDE Project, launched in 1988, is to establish a Widely Integrated Distributed Environment [WIDE]: a new computer environment based on operating systems and communications technology, designed to benefit the human race on a broad scale", the WIDE web site said.

The research area of the WIDE Project covers many computer study areas, including computer networks, operating systems, distributed processing, fault-tolerant system technology, security technology, multimedia information processing, groupware, computer education, etc...

The WIDE Project include several Working Groups as different as Kame [Kame-Web] (Free implementation of IPv6, MIP6 and IPsec on BSD), School of Internet [SOI-Web] (Education based on Internet), InternetCar [InternetCar-Web] (Connecting cars to the Internet), and Nautilus [Nautilus-Web].

2. Jun Murai Laboratory - Keio University

The aim of Jun Murai Laboratory - located in the Shonan Fujisawa Campus of Keio University - is supporting the research studying of Keio university students.

This support is is achieved by providing computer equipement and fund needed to some research project. With the goal to demonstrate as much as possible in real world the quality of the project.

Appendix B. Test Template: Definition

Author's Firstname Author's Surname

Publishing date

Abstract

Abstract of goals of this test series.

1. Title of first test

Purpose

The main purpose of the test.

Summary

A summary of expected events and behaviors.

References

References to RFCs and Internet-Drafts with citation of appropriate sections.

Resource Requirement

Description of all resources needed for this test.

Last Updates

All modifications since the previous versions.

Initial State

Description of initial state before the first step in Test Procedure.

Test Procedure

Description step by step of events.

Final State

Description of expected final state.

Observable Variable

Description of interesting result and variables measurements.

See also

Reference to other related tests.

Appendix C. Test Example: Multihoming in Fixed Network

Julien Charbon
Koshiro Mitsuya
Manabu Tsukada

August 4th, 2003

Abstract

The main purpose of these tests is study the multihoming support in IPv6 for fixed network in case of multiple mobile router and multiple different network prefix advertisements to get a better tolerance against network faults. At the same time make an analogy with the multihomed mobile networks.

1. Default Router Selection

Purpose

Test the case where a network link has several default router.

Summary

When several default router are on a same link - i.e. announce valid Router Advertisement on this link -, the network nodes on this link manage a Default router List and act a Default Router Selection. This mechanism provide a fault tolerance benefits against default router failure.

Moreover the Redirect Message inform a host of a better first-hop node on the path to a destination. This message and its operations provide a fault tolerance benefit against losing the connexion to Internet.

References

RFC-2461 - Neighbor Discovery for IP Version 6 (IPv6)

Section 6.3.4. Processing Received Router Advertisements

6.3.6. Default Router Selection

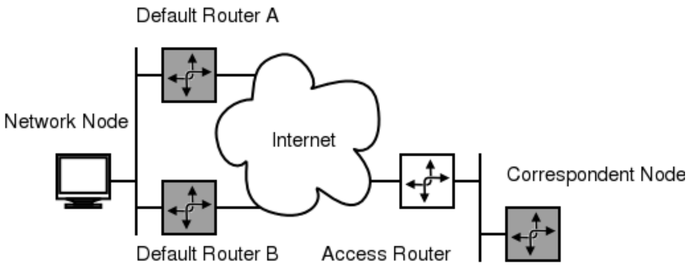
Resources Requirement

- Two Nodes: One on-link network node and one correspondent node.
- Two Default Routers.

Last Updates

None

Initial State



Initial state topology..

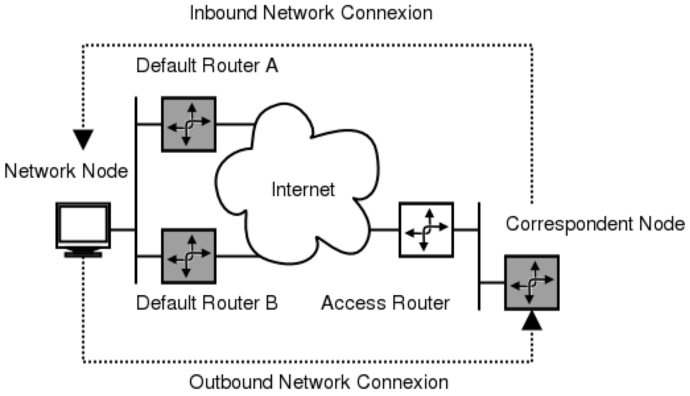
Comment: The access router is optional.

Configuration

- An routing protocol [i.e. OSPF, RIPng,...] run between the router and provide the IP packet carriage between the network node and the correspondent node.
- Both of default routers advertise the same network prefix.

Test Procedure

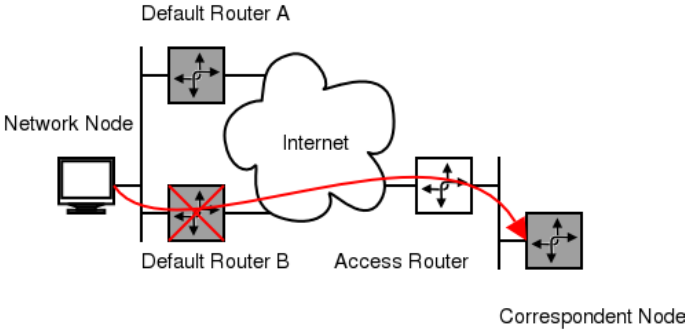
1. Verify that the network node has both default routers IPv6 link local address in its Default Router List.
2. Establish a network connexion between the network node and the correspondent node.

   Connexion between the network node and correspondent node.

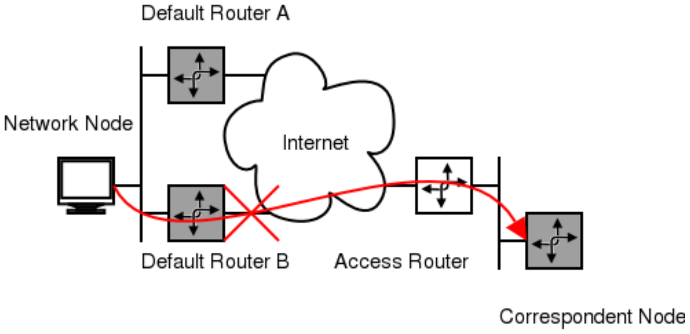
   Comments: The outbound and inbound network traffic can use the same default router or not.
3. Create a network fault:

   a. The default router used for the outbound connexion fail:



Default Router Failure.

b. A link used for the outbound connexion between a default router and the Internet fail:



Internet Connexion Failure.

Final State

The connexion between the network node and the correspondent node is keep using the other default router and then the other Internet connexion.

Observable Variable

- The time for the network node to change of Default Router.

Appendix D. Report Example: Multihoming in Fixed Network

Julien Charbon
Koshiro Mitsuya
Manabu Tsukada

August 4th, 2003

Abstract

The main purpose of these tests is study the multihoming support in IPv6 for fixed network in case of multiple mobile router and multiple different network prefix advertisements to get a better tolerance against network faults. At the same time make an analogy with the multihomed mobile networks.

1. Default Router Selection

Purpose

Test the case where a network link has several default router.

Last Updates

None

Configuration

Operating system: NetBSD 1.6.1

IPv6 Implementation: KAME Snap kit of July 28, 2003.

Commands

Default Router List: ndp -r

Routing Table: route show

Test Procedure

1. Verify that the network node has both default routers IPv6 link local address in its Default Router List.

   Result: *Done*

2. Establish a network connexion between the network node and the correspondent node.

   Result: *Done*

3. Create a network fault:

   a. The default router used for the outbound connexion fail:

      Result: The Neighbor Unreachability Protocol invalidate the failed default router entry in

Default Router List, and the network node select the other default router.

b. A link used for the outbound connexion between a default router and the Internet fail:

Result: The disconnected default router update its routing table and its default route next hop become the other default router address, and then it send a Redirect Message with target destination the other router when it receive a packet for the Internet.

Final State

The connexion between the network node and the correspondent node is keep using the other default router and then the other Internet connexion.

Result: Done, in each failure case the connexion is transparently preserved.

Observable Variable

- The time for the network node to change of Default Router.

  Result: Average time: Case a: 122ms Case b: 842ms.