2003－ＱＡＩ－９ (7)
2003／10／8

A Study on Mobile Multihoming Architecture

Radinal Rachmat† Hiroshi ESAKI‡
Graduate School of Information Science and Technology,
The University of Tokyo
7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan
TEL/FAX: 03-5841-7465, Email:
† radinal@hongo.wide.ad.jp
‡ hiroshi@wide.ad.jp

Abstract

As end users realize their Internet connectivity critical to their work, they seek ways of making their internet connectivity more robust against the operational outage. The multihoming provides the redundant and reliable connectivity to the Internet-site that traditionally can only be provided by using the routing system. We believe that it is possible to provide a fault-tolerant connectivity with a mechanism relies only on the pair of end-nodes instead of using the routing system. We propose a new multihoming architecture that is based on mobility protocol, Mobile IPv6. The architectures enables an end-node to make use of multiple address simultaneously and to control the selection of the most desirable addresses for both outgoing and incoming packets for different traffic flows.

Keywords

Multihomed Host, End-to-End Model, Mobile IP, Multi-Addressing Mechanism, Multiple Network Interfaces, IPv6

1 INTRODUCTION

As end users realize their Internet connectivity critical to their work, they seek ways of making their internet connectivity more robust against the operational outage. With current technologies, users should be able to connect to the Internet at any time and in any place. Users become so dependent on routine email, news, web, and similar access that a loss of connectivity becomes a crisis.

The multihoming often means of providing the fault-tolerant connectivity to the Internet-site. Recently, not only internet service providers (ISP) but also private organizations (e.g., universities or corporations) are often in multihoming environment. In other words, many networks in the Internet are connected to the Internet with multiple points.

It is realized that the multihoming is one of important function in IPv6. With the address allocation policy of IPv6 (i.e., IP address space is allocated by the upper service provider), each site that is connected with multiple providers are expected to be allocated multiple prefixes.

It is generally said that the multihoming could achieve a redundant connectivity provisioning or a load balancing for each user. To achieve redundant connectivity, hosts will likely require more than one type of network device. For example, multihomed hosts use 10 or 100 Mbit/s Ethernet when in a suitably equipped office or home, and also they use a slower wireless packet radio network as a backup.

Unfortunately, there is no network device assuring global scale connectivity. Because there is no single network device that can provide the desired quality of service (QoS) all the time. There is always a trade-off among bandwidth, coverage, performance, reliability, price, etc. Making use of these active network interfaces simultaneously for different flows of traffic is a technical challenge.

Though the multihoming support tradionally can only be provided by using the routing system which dependent on routing behavior of providers' border routers, we propose a new multihoming architecture that is based on "end-to-end multihoming". With the end-to-end multihoming system, a fault-tolerant connectivity relies only on the pair of end-nodes, not on routers. The proposed architecture is based on the "mobility" supporting protocols for IPv6, Mobile IPv6 (MIPv6). This architecture applies the MIPv6 protocol to provide fault tolerance to transport layer connections established between a multihomed host and hosts in the Internet. Additionally, possible mechanisms to control the selection of address for both outgoing and incoming packets for different traffic flows are explored. This architecture provides simple and efficient means for nodes to

communicate while being multihomed, or simultanously mobile and multihomed.

The rest of the paper is organized as follows: In section 2, we discuss the concepts and motivations for multihoming. In section 3, we extract some issues for multihoming. In section 4, we describe research objective and the set of functional requirements for support of multihoming system. In section 5, we describe proposal of new multihoming architecture: End-to-End Multihoming based on Mobile IP. In section 6, we detail the system design. In section 7, we list related work. Finally, we present conclusions together with some future and continuing work in section 8.

2 THE CONCEPTS AND MOTIVATION FOR MULTIHOMING

The multihoming generally implies that there are multiple paths to reach a "home" destination. The two basic perspectives for interpreting the concepts of multihoming are:

- Host Multihoming: Support multihoming in IP hosts. In both versions of IP, hosts may have multiple physical interfaces as well as multiple IP addresses bound to one or more interfaces [1]. The extent and perspective of the problem is slightly mitigated in IPv6 because of the more flexible binding of physical interfaces to IP addresses.
- Site Multihoming: Support Multihoming in IP networks. In this case the emphasis is placed on a site or enterprise[1] and manipulation of its conectivity with its transit providers (i.e. Internet Service Providers - ISPs).

A host or site may establish its Internet connectivity from more than one Internet Service Provider due to the following reasons.

(1) Maintaining connectivity via more than one ISP could be realized as a way to make connectivity to the Internet more reliable. When a connectivity through one of the ISPs is down, the connectivity via the other ISPs could preserve the site or host connectivity to the Internet.

(2) Maintaining connectivity via more than one ISP could allow the site or host to distribute traffic load among multiple connections/paths. Being able to specify the incoming and outgoing connections explicitly in a natural manner is a useful feature.

3 MULTIHOMING ISSUES

The following section details specific problems that must be solved by the multihoming solution.

3.1 Mantain Established Connections

Classic Internet transport protocols use a single source IP address and a single destination IP address, as part of the identification for an individual transport data flow. For example, TCP includes these in its definition of a connection and its calculation of the header checksum. Hence a classic transport association is tied to a particular IP address pair.

The problem is how to keep an existing connection between a host of the multihoming site and the outside in case of failure, since when a host want to move connection, it will use a different IP address pair that in the case of TCP, this means a new connection.

3.2 Use The Reasonable Exit/Entrance

How to use the right exit/entrance which will get best performance. Multihoming forces hosts to choose the source and the destination address of the packets, in a way that makes the best usage, or at least a reasonable usage, of the network resource.

3.3 Ingress filtering

As a result of IP address spoofing attacks, more routers are filtering on the source address (ingress filtering [2]) and will drop a packet whose address is not "topologically correct" (whose originating network cannot be the one identified by the source address). We assume that each of the ISP may perform ingress filtering, and will reject packets whose source address does not belong to the prefix allocated to the network by that ISP. This leads to a possible failure scenario as illustrated in Figure 1.

1. Host choose source address B
2. Default route leads to router A
3. Router B forwards the packet to ISP A
4. Packet is dropped by ingress filtering

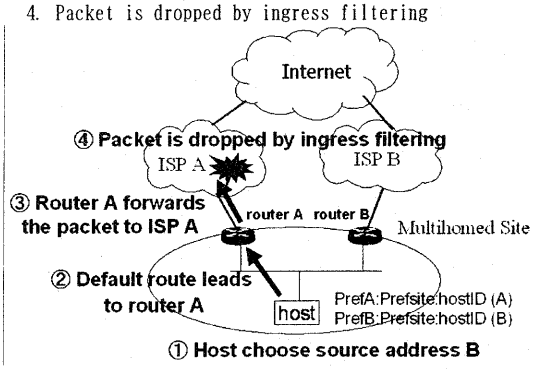

Figure 1: Ingress Filtering

3.4 Avoid using dead link

How do host detect that a link is dead and how to switch to other address when the link is dead. The problem dealt here is what happens in case of a failure of a link through an ISP in a short time scale:

- to a new connection from a node of the multihoming site to the outside
- to a new connection from the outside to a node

[1] An "enterprise" is an entity autonomously operating a network using TCP/IP and, in particular, determining the addressing plan and address assignments within that network.

of the multihoming site

4 RESEARCH OBJECTIVE AND SYSTEM REQUIREMENTS

The goal of this research is to provide a design for a multihoming solution, particularly in IPv6 network. The followings would be the system requirements for multihoming system.

(1) Redundancy:
By multihoming, a site/host must be able to insulate itself from certain failure modes within one or more transit providers.

(2) Load Sharing:
The system should be possible to perform some amount of load balancing between the multiple connections. A host should be able to distribute both incoming and outgoing traffic among multiple transit providers.

(3) Scalability and Simplicity:
Multihoming solution should be as simple as possible. It should be scalable beyond short-term needs. Easy to configure and administer. For example, there is no need to ISP coordination and specific protocol modification.

(4) Transport-Layer Survivability
Multihoming solutions should be able to provide re-homing[2] transparency for transport-layer sessions and keep ongoing session during handover process.

(5) The solution should be used both on stationary and mobile hosts.

5 NEW MULTIHOMING ARCHITECTURE: END-TO-END MULTIHOMING BASED ON MOBILE IP

5.1 End-to-End Multihoming and Mobility

End-to-End Multihoming supports multihoming on end terminal, not to dependent on router. A fault-tolerant connection can be achieved relying not on routers but on the pair of end-nodes only (Figure 2).

In this case, and end-to-end solution is needed. So end hosts will have to manage the different addresses and they will need to know when to use which one.

It is a natural approach to analyze the application of the available mobility solution to the end-to-end multihoming problem. The goal of the multihoming and mobility solutions is to provide a communicating end-point with uninterrupted connectivity throughout changes in the point that it is using for attaching to the public IP network. In the mobility scenario, the communicating end-point changes its attachment point because of its movement. In the multihoming scenario, the attachment point used by the end-point for communication varies because of topological

[2] The term "re-homing" denotes a transition of a host/site between two states of connectedness, due to a change in the connectivity between the host/site and its transit providers.

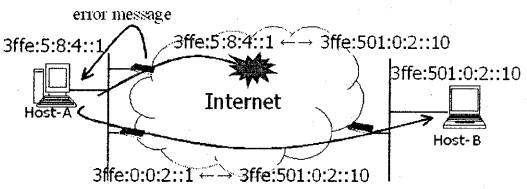

Figure 2: End-to-End Multihoming

changes caused by outages in the communication elements. While the causes are different, there seems to be enough similarities between the two scenarios to consider common solutions for both problems.

Also note that a host may be multihomed and mobile simultaneously. It looks likely that in the future many of the mobile nodes will be simultaneously mobile and multihoming, i.e., have multiple mobile interfaces.

5.2 Overview of The Architecture

MIPv6 (Mobile IP for IPv6) [3] is a well-known mobility solution in IPv6 with a global scale. We realize that mobility mechanism should be used for multihoming. Especially, this mechanism would be useful to solve the issue for the transport layer survivability, because of its capacity to support two addresses for the same node. We are analyzing the possibility to use the MIPv6 protocol to preserve established communications in multihomed environments. We describe a possible approach to this below.

The application scenario (Figure 3) consists of a multihomed site that obtains global connectivity through two (or more) ISPs i.e. ISPA and ISPB. The multihomed site has obtained two address ranges: one delegated from ISPA address range and the other one from ISPB address space. HostA inside multihomed site configured one address from each ISP address range i.e. PrefA:X:ID and PrefB:X:ID. This means that if there is a failure in one of the ISPs, ISPA for instance, HostA is still reachable using the alternative address, PrefB:X:ID.

We propose that transport layer survivability is achieved by the use of care-of-address (CoA) switching mechanism based on MIPv6 protocol in case of failure. A multihomed host principally is assigned 2 types of IPv6 addresses, home address and care-of address. The multihomed host selects its unchanging home address as the source IPv6 address for the layers which are higher than IP layer. On the other hand, the care-of address will be the source address of outgoing packets.

1. Suppose that host A established communication with hostC, somewhere in the Internet. The connection is being routed through ISPA and PrefA:X:ID (CoA1) is used.
2. ISPA goes to be down with any reasons.
3. HostA packets contain the home address destination option with home address (HoA) and PrefB:X:ID (CoA2) as source address, so that for every device

on the path source address is PrefB:X:ID and only hostB replaces this source address by home address (HoA).

4. HostA sends a binding update containing PrefB:X:ID as a care-of address.
5. HostC sends a binding acknowledgement. This packet and all next packets are sent with home address (HoA) as final destination included in a routing header and PrefB:X:ID as next destination included as destination address. Consequently, all packets are sent towards HostA using ISPB, and address translation is performed at destination host (HostA) when packets reach HostA.

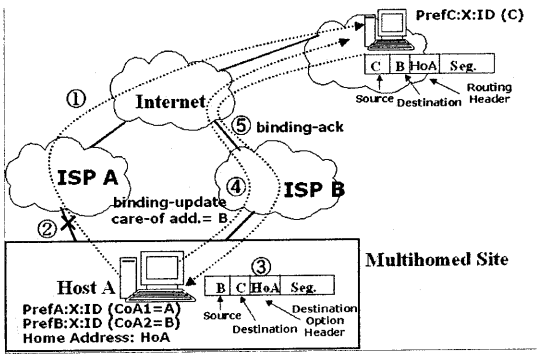

Figure 3: Multihoming with MIPv6 Mechanism

5.2 Load Sharing Policy

Multihomed host may have multiple addresses assigned to multiple interfaces. On a multihomed host, these interfaces instead represent different ways this host can communicate with the outside world. For example, it may want to use two different interfaces (one for ssh and another for file downloading) for communication with the same host. When the multihomed host is connected through several network interfaces, it is expected to use them all at the same time.

In our framework, a multihomed host may choose to send and receive the packets belonging to particular flow on any of its interfaces by looking up Load Sharing Policy Table (LSPT). Load Sharing Policy Table contain entries that associate a particular flow specification with a multihomed host's care-of address. This Load Sharing Policy Table specifies the multihomed host's care-of address(es) that both of multihomed host and it's correspondent host should use to send packets belonging to particular flow.

For example, a multihomed host (host A) has 2 network interfaces and also 2 care-of addresses in figure 4. When the correspondent host starts to send packets to multihomed host, the correspondent host checks the flow type and finds the most appropriate policy from the Load Sharing Policy Table. Once the policy is found, the correspondent host routes the packet to the care-of address matched with the policy.

Any flow can be assigned to any network interfaces, because the policy held by both the multihomed host and the correspondent host dictates which interface will be used.

The Load Sharing Policy Table can be registered to the correspondent host not only by Mobile IP operation, different protocol is possible. When a network interface status is changed, a multihomed host will update the remote binding and the policy table.

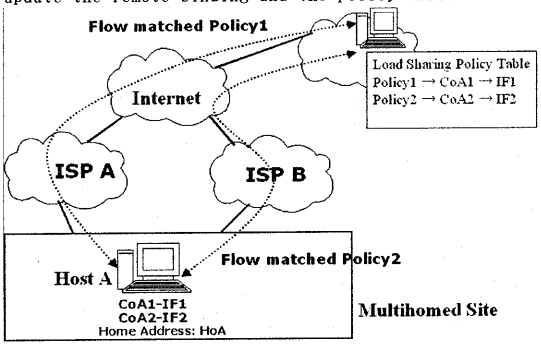

Figure 4: Load Sharing Policy

6. SYSTEM DESIGN

6.1 Overview of System

A multihomed host principally has 2 types of IPv6 addresses, home address and care-of address which are handled in the network layer. The multihomed host selects its unchanging home address as the source IPv6 address for the layers which are higher than IP layer. The care-of address selection system then decides care-of address which is equal to deciding the outgoing network interfaces on the multihomed host. The multihomed host control the selection of the most desirable addresses by looking up appropriate entries in the Load Sharing Policy Table (LSPT). Selected care-of address will be the source address of packets.

Figure 5 shows protocol stack overview on the Multihomed Host. The figure basically shows multihomed host, but most of the parts in the figure is similar between multihomed host and correspondent host.

To maintain reasonable processing overhead, policy table entries can be cached in a manner similar to routing table entries. If the characteristics of the traffic match a cached entry, the application uses the cached entry to speed up the process of policy lookup. Whenever the load sharing policy table is modified, the cached entries are flushed.

6.2 Extensions on the Network Stack

This section shows the extension on the Network Stack for supporting the system.

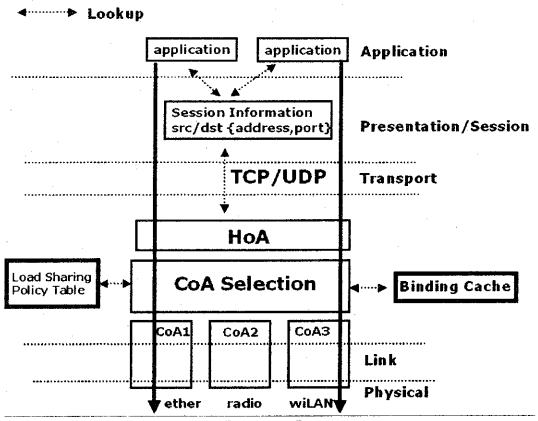

Figure 5:
Protocol Stack Overview on the Multihomed Host

6.2.1 Multiple Care-of Addresses Support

According to the current specification of Mobile IPv6, a node can register only one of care-of addresses as its primary care-of address even if the node has multiple active care-of address. It means that the specification does not allow a node to register multiple care-of addresses. Correspondent host always overwrites the existing binding cache when received a new binding update.

Therefore, such extension that lets multihomed host to register multiple care-of addresses for all of its network interfaces to correspondent hosts is needed. It requires some changes on message format of binding update and binding cache structure and management for registering multiple care-of addresses.

The Mobility option defined in [3] can be used to notify several care-of addresses to correspondent host. When the correspondent host received several care-of addresses it creates multiple bindings to it's binding cache and handles them as normal bindings of Mobile IPv6 specification. After correspondent hosts has multiple bindings, they can deliver packets to multihomed host via multiple paths

If a network interface becomes invalid, the multihomed host deletes the dead address then resends the Binding Update with different entries. Correspondent host then search the binding cache and modify the entries.

6.2.2 Load Sharing Policy Table

The Load Sharing Policy Table is added to the network layer for specifies how the care-of address should be selected for each traffic flow matching certain characteristics.

Policy is installed as a information for selection of care-of addresses. The policy allows hosts to share various flows to appropriate network interfaces. The policy can be based on:

- Communication Protocol (HTTP, SSH, FTP, etc)
- Correspondent Host IP address
- Flow Label, etc

Policies are configured with a priority number by user and maintained in multihomed host and it's correspondent hosts. The multihomed host gets configured policies from a local policy database and sends them by optional protocol to correspondent hosts. The multihomed host and correspondent hosts use the appropriate care-of address which is designed in policy if outgoing flows match with any policies from local database. If no entry is found, the packet is forwarded to the multihomed host's default care-of address

7 RELATED WORK

There are a number of proposals focusing on providing multihoming support at different layers of the network software stack.

7.1 Network Layer Solution

7.1.1 Exit Router Approach (RFC2260)

Exit router approach [4] tries to deliver the packets of any source and destination pair during failure on corresponding exit link. With the exit router approach, the border routers establish secondary links (tunnels), between ISPs and site exit border routers. The drawbacks of this approach are:

- No available tools for ISP selection to achieve a load sharing.
- Co-operation among the ISPs are mandatory requirement. This approach may have management complexity because of the need of tunnel configuration among ISPs.
- Can not provide a fault tolerant operation in case of ISP failure.

7.2 Transport Layer Solution

7.2.1 SCTP

Beside the network layer solution, there is a transport layer solution such as the Stream Control Transmission Protocol (SCTP) [5]. SCTP is a reliable transport protocol for multiplexed data streams. It includes modern mechanisms for safe initiation of a connection, as well as the necessary tools for reliability and congestion control. It also has a mechanism for communication access to multiple IP addresses between the participation host pair.

In the initiation phase (protected by cookies), each endpoint can specify the set of addresses (IPv4, IPv6 addresses or DNS resolvable names) it will use. Using a "heartbeat" mechanism, the reachability of a destination address can be probed.

SCTP is designed for fault tolerance and has no real mobility support, for instance the address set must be specified at the association establishment only. It lacks a readdressing capability (i.e., address set management out of the establishment phase) and a rendezvous mechanism (for simultaneous address

changes).

But the main limitation of SCTP is an application must be modified in order to use it and take advantage of its innovative features.

7.2.2 M/TCP

Multipath Transmission Control Protocol (M/TCP) [6] is an end-to-end transport protocol that is designed as an alternative TCP option to improve reliability and performance/throughput. M/TCP allows a sender to simultaneously transmit data via multiple controlled paths to the same destination. The protocol requires no modification in IP layer. Congestion control and error recovery in M/TCP are developed based on those in TCP. Because a host running M/TCP implementation maintains parameters to independently probe network congestion of each path, data can be transmitted via multiple controlled paths. When congestion exists in a path M/TCP can perform retransmission causing esential error recovery.

But the main limitation of M/TCP is in order to establish multiple paths, two endpoints communicating through M/TCP need to be subscribed to multiple ISPs.

7.3 Session Layer Solution

The session layer provides functionality above transport and below the application. In effect it is a way of institutionalizing application-level support. The merit of placing multiaddressing support at the session layer is that it can use multiple transport services.

The concept of session migration was introduced on [7], which enabled service centric networking systems. A service user can start a session using one service provider and continue it on another. In this manner, the service user can select the best suited service provider when the session is initiated.

The problem with this approach is that a full session layer typically replicates substantial portions of the transport service, in order to ensure reliability and in-order data sequencing. This makes the session-level approach notably complicated and inefficient.

8 CONCLUSION AND FUTURE WORK

In this paper, we proposed a new multihoming architecture based on the protocols to support "mobility" for IPv6, Mobile IPv6. By this mechanism multihomed host can achieve fault-tolerant connection and control incoming and outgoing flow sent over any network interface using load sharing policy. The system relies only on the pair of end-nodes. Furthermore, we also presented the design of system.

We are currently working on building the experiment environment. For the future works, we plan to do implementation and experiment on the proposed solution. We also plan to propose solutions for handling interface information to detect changes in a link status.

References

[1] R.Braden, "Requirements for Internet Hosts - Communication Layers", RFC 1122, October 1989

[2] P.Ferguson, D.Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2827 - BCP 38, May 2000.

[3] D. Johnson, C.Perkins, J. Arkko, "Mobility Support in IPv6," draft-ietf-mobileip-ipv6-24.txt, June 2003

[4] J. Hagino et al., "IPv6 multi-homing support at site exit routers," IETF RFC 3178 , October 2001.

[5] R. Stewart, Q. Xie et al., "Stream Control Transmission Protocol", RFC 2960, October 2000.

[6] R. Kultida, H. Aida, "An Evaluation of Multi-path Transmission Control Protocol (M/TCP) with Robust Acknowledgement Schemes",2002

[7] Kjetil Myhre., "Policy based networking in a mobile, multiconnected environment," May 2003.

[8] C. Perkins (ed.), "IP Mobility Support for IPv4," RFC 3220, January 2002.

[9] Hinden, R. and S. Deering, "IPng working group minutes/Tokyo meeting," September 1999.

[10] R.M. Hinden and S.E. Deering,"IP version 6 addressing architecture", RFC2373, July 1998.

[11] J. Namiki,"IPv6: New Internet Era", IEICE, Tokyo, 2001.

[12] F. Dupont: "The Host Identity Payload protocol: toward a secure solution to mobility and multi-homing," 22 may 2002.

[13] IETF Site Multihoming in IPv6 (multi6) WG, http://www.ietf.org/html.charters/multi6-charter.html

[14] A. Matsumoto et al., "Multihoming Support for Mobile Network Architecure LIN6," 2002