Mobility vs Multihoming

Naveen Gundu
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
naveen@cc.hut.fi

Abstract

In current scenario, use of mobile and Internet has been increasing and the increasing number of users are coming forward to use new services like mobility and multihoming. Roaming users are interested to stay connected with network while moving from one network to another network with multiple network interfaces e.g. WLAN and GPRS.Problems which might arise when mobile host moves from one network to another network. Some mobility solutions have been introduced to ensure connections between networks,e.g., Mobile IPv4 & IPv6.

This paper gives a brief functional description of multihoming and mobility, given requirements, problems associated with them, related solution to fulfill each requirements and finally comparison between them.

KEYWORDS: Mobility, Mobile IP, Multihoming, Routing, Site Multihoming, Host Multihoming, Node/end-host, ISP.

1 Introduction

Now-a-days there is a revolution from formal static network connection to modern technology like wireless network has come into network technology world. Popularity is growing with wireless network and the devices which are used like PDAs, Laptops and other portable devices. Users are attracted to services which are portable and handy to use devices without any hazels with wire connections.

It has been possible to use mobile device within one wireless domain for along time but problems arise when the user is moving from one network to another network. For this reason, the system has to reconfigure before it continues communication. Current protocols are not fully supporting the system to make it work.

Some new proposals have been introduced for example Mobile IP. It was developed to enable in IPv4 networks, which is still facing some problems. Presently working on Mobile IPv6, this is right now under development. Mobile IP is one of the areas where most growth is expected in the coming years.

Current trend also moving towards feature like multihoming, it is widely used in the IPv4 Internet today and is an essential component of service for enterprises. In knowing of this, the built-in features of IPv6 make it easier for end-hosts and networks to be multihomed than in IPv4. In future, as there is a gradual growth in internet, multihoming is also likely to increase and become a common phenomenon. For example, In multihoming user subscribes different ISPs and networks for different services. User views different options like cost effective, secure, quality service from one ISP and others.

The analysis of this paper presents the idea behind the mobility and multihoming. The solutions provided with mobile IP and layer 4 for both services and how these protocol solutions are trying to fulfill the requirements. It also gives difference between them.

2 Background

Here gives an overview about mobility and multihoming at end host and site point of view. And also discusses problems and requirements for further discussion.

2.1 Multihoming

Multihoming refers to a situation where an end-host having several parallel communication paths that it can use [4].

Typically there are two types of multihoming one is *Host Multihoming* and second is *Site Multihoming*.

Host multihoming is a host with more than one global IP addresses assigned to it. These addresses could be provided by same Internet Service Provider (ISP) or from different ISPs. Furthermore, a host may be multihomed with multiple global IP addresses on a single interface or global IP addresses on several interfaces.

This is illustrated in the Figure 1. A multihomed end-host is a node that has two or more points to attach with the rest of the network.

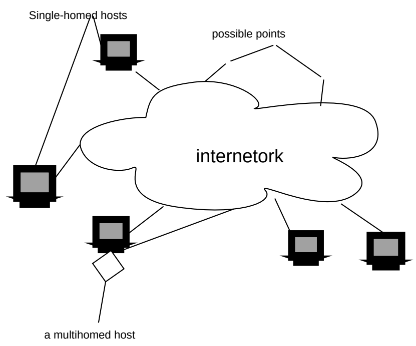

Figure 1: The host multihoming model

Site multihoming refers to a site that has more than one connection to the public Internet through either the same Internet Service Providers (ISP) or different ISPs.

As shown in Figure 2, Site connected to the public network through ISP1 and ISP2.

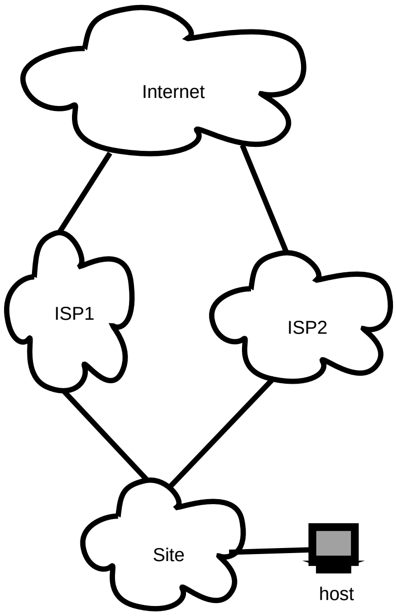

Figure 2: The site multihoming model

There are several reasons and motivations why an end-host and site may wish to be multihomed. Here are some potential multihoming benefits [8].

- Load Sharing: Is very beneficial, In multihoming to archive higher throughput a host or site could share its traffic load through two or more ISPs.
- Service provider selection: This is already presented in IPv4 Internet but it is expected to become even more issue in the IPv6 Internet. It provides a user to select some particular services from certain ISPs and others. For example some particular services from certain ISPs may offer a cheaper price than the others.
- . Enhanced mobility support: A mobile IP network almost creates multihoming scenarios. Both in case of move between heterogeneous networks such as Ethernet to wireless or moving from WLAN to another. Often such a change involves an overlap period where the mobile host is attached to multiple networks with different addresses.

2.2 Multihoming Problems

Here are some problems might associated with the mutihoming [9], [4]:

- Many problems related to the security for example address stealing and address flooding.
- Currently available protocols only control routing table growth if routes are aggregated then problems arise.
- If the address space is large then the routing table growth could easily exceed the capacity of the hardware and protocols.
- Controlling load balancing based on address assignment is more complex. Difficult to achieve symmetric flow of packets in and out from an enterprise.
- If the host chooses IP from several global addresses, that choice overrides policy may conflict with routing intentions and it can break the connection.
- Multihoming is still under development with out multihoming support it may not be possible to deploy IPv6 on a large scale. Some protocols giving short time solutions to solve problems for IPv6 deployment.
- Use of multiple addresses from upstream ISPs provides a possible solution but results will complex address management.

2.3 Multihoming Requirements

Mentioned in above section about multihoming motivations, which are part of requirements: [2]:

- Multihoming should support redundancy
- It not be more complex than current IPv4 solutions
- It should support load sharing
- Protect from performance difficulties
- Not much impact on DNS
- Minor impact on routers
- Re-homing transparency for transport-layer sessions (TCP, UDP, SCTP)
- No changes on host connectivity
- Should allow interactions between hosts and routers
- Easy to manageable
- Packet Filtering
- It should provide proper security

2.4 Mobility

Mobility denotes the phenomenon where an entity moves while keeping its communication context active [4].

Before discussing mobility, it is good to differentiate between network mobility and node or end-host mobility. Network mobility defines where a whole subnet work moves from one location to another. Node or end-host mobility allows a communication node to change its topological location in a network. In this paper we limit our discussion to analyzing mobility from an end-host point of view. In reality, we assume that there are a number of mobile nodes that attach to a relatively fixed network. When ever a node moves from one location to another location, its location address changes. In order to continue to communicate, the node must be able to send the changes to its active peers. Shown in the Figure 3.

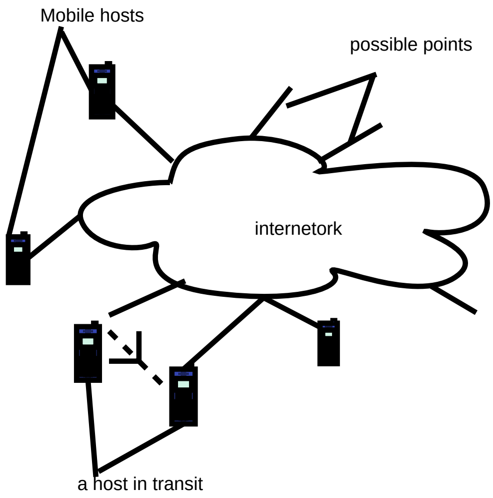

Figure 3: The mobility model

2.5 Mobility Problems

Before the Mobile IP concept, traditionally IP address is static and assigned to a physical location. Whenever host moves its location from one to another then it has to change its network configuration settings. When Dynamic Host Configuration Protocol (DHCP) has introduced and in use, the terminal configures automatically and assigns with an IP address. The Problem with the DHCP is IP address may or may not change when even terminal in the same network. IP address change makes impossible for other host to contact the host using IP address [10].

DNS (Domain Name System) name cannot be used in mobility, because they are usually statically bound to IP address.

Another problem is TCP connection, whenever IP address changes. Even if a user able to roam another network and obtain an IP address dynamically. All TCP connection will have to be reestablished. This breaks the session.

And also there are many basic security problems exist like Denial of service attacks.

2.6 Mobility Requirements

The below listed requirements are basic requirements to support mobility [17]:

- Migration Transparency: a permanent connectivity to the Internet and sessions are expected to be maintained as the mobile router changes its point of attachment.
- Analyzing and fixing basic security problems and security protocols and mechanisms.
- Performance Transparency to minimize the impact of handover over applications.
- Operational Transparency: Support to implement at Internet Protocol (IP) layer. It is expected to be transparent to the upper layer protocols so that upper layer protocols can run without changing any thing.

3 Related Work

As we have already discussed before, our work mainly based on mobility and multihoming solutions. It gives an overview of existing and proposed approaches to address mobility and multihoming solutions.

3.1 Layer 4 Solutions

The following protocols present the basic operations of each.

DCCP: Datagram Congestion Control Protocol (DCCP) is a transport protocol, which provides congestion controlled and bi-directional stream of unreliable datagrams. It is mainly intended for applications, like streaming media and internet telephony [11].

DCCP provides support for both mobility and multihoming. It supports such way that transferring a connection endpoint from one address to another. In this move endpoint must negotiate mobility support beforehand.

When host is moving from one location to another, first endpoint gets a new address. Then it sends a DCCP-Move packet from that address to the stationary endpoint. And finally the stationary endpoint changes its connection state to use the new address. DCCP uses features to identify the host node; one is Mobility capable feature to inform another node that it would like to be able to change its address during the course of the connection. Second is Mobility ID feature to inform another node with 128-bit number that will act as identification, then the opposite node changes its address during the connection.

SCTP: Stream Control Transport Protocol (SCTP) is a new reliable IP transport protocol. It has been approved by IETF as a proposed standard protocol [12].SCTP is a unicast and similar to the transport protocols such as TCP and UDP, and controls data exchange between two end points.

Like TCP, SCTP provides a reliable transport service, ensuring that data is transferred to the network without any errors and in sequence, Checks when the data is discarded, reordered, duplicated or corrupted and retransmitting damaged data as necessary. SCTP is a session-based protocol; this means relationship between two end points is maintained until all data transmission has been successfully completed. It has also an ability to support single SCTP endpoint with multiple IP address.

One of the core features of SCTP is supporting multihoming. As mentioned above it has ability for a single SCTP endpoint to support multiple IP addresses. To support multihoming, SCTP endpoints exchange lists of addresses during initiation of the connection. Each endpoint must be able to receive messages from any of the addresses associated with another endpoint. The benefit of multihoming is potentially greater survivability of the session in the presence of network failures. As we know from a conventional single-homed session, the failure of a Local Area Network (LAN) access can isolate the end system. Failures within the core network can also cause temporary unavailability of transport until the IP routing protocols can reconverge the point of failure. It also provides network-level tolerance by supporting host multihoming at either end of the connection [12].

Using multi-homed SCTP, redundant LANs can be used to reinforce the local access, while various options are possible in the network to reduce the dependency of failures for different addresses. Using addresses with different prefixes can force routing to go through different carriers. Finally in order to reduce the potential security issues,it is required that some response messages should be sent to the source address in the message that caused the response.

TCP-MH: TCP Multi-Home is a transport protocol; it is a replacement of Transmission Control Protocol (TCP). Multihoming nodes that connected to the global network through multiple up stream access lines are expected to have multiple addresses given by each ISP. The existing TCP was not designed to manipulate multiple addresses in one TCP session. In an existing TCP only one local and remote address is used through a TCP session, even when a client and server is located under multi-homed site and has Multiple IP addresses. When a network outage occurs and the access-line associated with the local and remote address is down, then the TCP session itself gets lost even though access-line is alive.

TCP-MH option makes it possible to handle multiple local and remote address pairs in one TCP session and works in situation where network failures by finding an alternative network path [13].

TCP Multi-homed options enable a host to get benefit from multi-home in an end-to-end multihoming. By introducing this TCP-MH option, TCP becomes much more reliable and powerful without loss of security and not depending on IPsec. This solution is based on and resembles SCTPs new multihoming method. TCP-MH option is trying to improve multihoming support and rapid deployment [13].

3.2 Mobile IP Solutions

Mobile IP is a standard protocol, proposed by Mobile IP working group of Internet Engineering Task Force (IETF) [14]. It builds on top of Internet Protocol (IP) to make mobility transparent to higher-level protocols like Transmission Control Protocol (TCP).

The following discussion gives the basic principles of Mobile IPv4 and Mobile Ipv6.

Mobile IPv4: Mobile Internet Protocol Version 4(MIPv4) introduces the use of two IP address called fixed home address and another is care-of-address (COA). Home address defines the permanent address of the host this can be used by other nodes. COA defines the current location of the host. In the home network the host called a Mobile node (MN), it has a home agent (HA). When the mobile node changes its locations to another then it is called foreign network, it registers itself to a foreign agent (FA) and obtains a COA. The mobile node may register its care-of-address to the HA or this may happen directly through HA or FA. The host wanting to communicate with the mobile node is called the corresponding node (CN).

As shown in Figure 4. Routing in Mobile IP is based on tunneling. A CN always sends all datagrams to the home address of the MN. While the mobile node is registered in a foreign network; the HA will receive all its datagrams and tunnel them to the COA. When datagram reaches the FA delivers it to the mobile node.

In other way around when the MN wants to communicate with the CN it will send directly to it. The MN keeps using its home address as a source address that is why every packet going from CN to the MN will be routed through the HA.

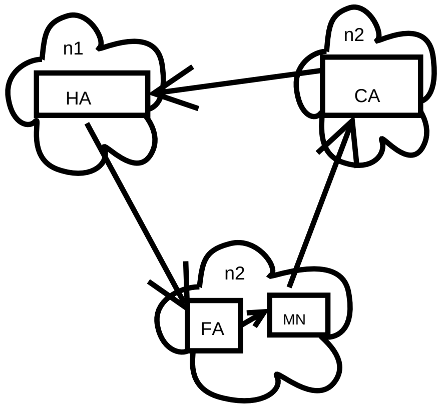

Figure 4: Mobile IPv4 routing model

Mobile IPv6: Mobile Internet Protocol Version (MIPv6). it follows the same basic principles as Mobile IPv4 including home and care-of-address. The main difference is foreign agent no longer exists. CN and MN can communicate directly. And also some of security has been improved. MIPv6 is still under development. Optimized routing showed in Figure 5.

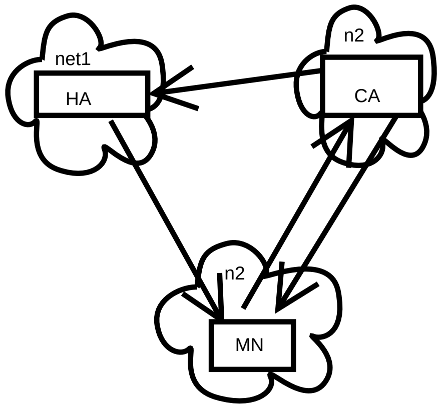

Figure 5: Mobile IPv6 routing model

4 Comparison and analysis

Following discussion presents the analysis from the above protocols. How protocols effecting multihoming and mobility, Comparison between them.

DCCP:

- As already we have mentioned in related work section DCCP is intended to solve only the simplest problems for mobility and multihoming. For instance, there is no support for simultaneous moves.
- It does not support complex mobility and security semantics. Applications should keep more complex mo-

bility semantics or stringent security guarantees them self.

- It recommends using an existing solution like Mobile IP for mobility and security
- DCCP mobility may not be useful in the context of IPv6, with its mandatory support for Mobile IP. [11]
- In Mobility DCCP does not provide cryptographic security guarantees. It only provides security when Mobility ID known as a valid ID. For example an attacker cannot move a DCCP connection to a new address unless it knows a valid Mobility ID.
- To Avoid attacks mobility slightly changes DCCPs security properties by introducing a new mechanism.

To fulfill the requirement of multihoming features DCCP proposes some additional design considerations that should be considered in designing a new transport protocol. Mechanisms for multihoming and mobility are one area of additional functionality. [11]

SCCP: As mentioned in before section Session Control Transport Protocol (SCTP) provides transport-layer support for multihoming and mobility. But still there are some problems.

- SCTP multihoming supports only communication between the two end points of which are assigned with multiple IP addresses and multiple network interfaces.
- It does not deal with communication ends that contain multiple endpoints for example clustered endpoints that can switch over to an alternate endpoint in case of failure of the original endpoint [15].
- In the current form of SCTP does not do any load sharing, which means multihoming is used only for redundancy purposes. A single address is chosen as a primary address and is used as the destination for all DATA chunks for normal transmission [12].

TCP-MH: There are some advantages using TCP-MH. This is based on SCTP method. It is trying to solve problems like multihoming support and fast deployment. TCP-MH option makes it possible to handle multiple local and remote address pairs in one TCP session and works in situation where network failures by finding an alternative network path [13].

TCP Multi-homed options enable a host to get benefit from multi-home in an end-to-end multihoming. TCP becomes much more reliable and powerful without loss of security. TCP-MH option is trying to improve multihoming support and rapid deployment.

But the same time on the security side the work did not really address the authentication or denial of service problems [4].

Mobile IP: Mobile IPv4 has been solved many of the basic problems mentioned in previous mobility section. But still some major problems are exist and unsolved. Routing in Mobile IP is inefficient because of the tunneling; Datagrams from the mobile node (MN) to the (CN) are not tunneled. It means that the delay for datagrams to the MN, which may cause problems for TCP congestion control

Another major problem in IPv4 is security. There s no authentication between the foreign agent and the mobile node or home network.

Mobile IPv6 solved all the problems except some security related problems. For example: Security in False-binding updates and DOS (Denial of Service) attacks.To solve security problems other protocols have been introduced for example, HIP (Host Identity Payload) for security and LIN6 for IPv6 multiple interface.

IPv4 multihoming fulfills the basic requirements but some major problems exist, like routing is a major issue. Routing is one of the most discussed area in multihoming because mutihomed sites will cause large number of routing table entries to be created in the backbone of the Internet, it slower the system and more expensive.

In the future IPv6 multihoming might fulfil all the requirements. It has covered all the existing vulnerabilities in IPv4 multihoming.

5 Conclusion

Mobility solutions are required to enable roaming users to maintain their connections when changing their locations; Multihoming is required to use multiple interfaces and addresses to connect the network. This paper presented and compared the solutions (DCCP, SCTP, TCP-MH and Mobile IP) for both multihoming and mobility. From the study it is difficult to solve some problems which cannot be done by above solutions. From this it shows that none of these solutions fulfil total requirements of mobility and multihoming.

References

[1] D. Johnson, C. Perkins and J.Arkko. Mobility Support in IPv6. *IETF Mobile IP Working Group,Internet-Draft, December 29, 2003*

[2] J. Abley, B. Black and V.Gill. Goals for IPv6 Site-Multihoming Architectures. *RFC 3582, IETF Network Working Group, August 2003*

[3] P. Savola. IPv6 Site-Multihoming: Now What). *Internet Engineering Task Force, Draft October 2003*

[4] Pekka Nikander, Jukka Ylitalo and Jorma Wall. Integrating Security, Mobility and Multi-homing in HIP Way. In *Proc.Ericsson Research nomadicLab*

[5] Jukka Ylitalo, Petri Jokela, Jorma Wall and Pekka Nikander. *End-Point Identifiers In Secure Multi-Homed Mobility*

[6] Ronan J. Skehill,Sean McGrath. *IP Mobility Management* In *Proc.Department of Electronic and Computing Engineering,University of Limerick*

[7] Sally Floyd and EddieKohler. Profile for DCCP Congestion Control ID 2:TCP-like Congestion Control. *Internet Engineering Task Force, Draft August 2003*

[8] 6net.org publications *http://www.6net.org/publications*

[9] Richard Draves. *(*Default Address Selection for IPv6). *IPng Working Group, Draft August 6,2002*

[10] Elina Mäkinen, General reference. *(*Comparison IP mobility). *Seminar paper*

[11] Eddie Kohler, Mark Handley and Sally Floyd *(*Datagram Congestion Control Protocol (DCCP)). *Internet Engineering Task Force, draft, Feb 2004*

[12] L. Ong and J. Yoakum *(*An Introduction to the Stream Control Transmission Protocol (SCTP)). *RFC 3286 Network Working Group , Informational, May 2002*

[13] arifumi Matsumoto, Masahiro Kozuka, Kenji Fujikawa and Yasuo Okabe *(*TCP Multi-Home Options). *Internet Engineering Task Force , draft, 7 oct 2003*

[14] C. Perkins *(* IP Mobility Support for IPv4). *RFC 3344 Network Working Group, August 2002*

[15] l.Coene *(*Stream Control Transmission Protocol Applicability Statement) *RFC 3257, Network Working Group , April 2002*

[16] C. Perkins *(* Mobility Support in IPv6). *IETF Mobile IP Working Group, June 30, 2003*

[17] Thierry Ernst *(* Network Mobility Support Goals and Requirements). *NEMO Working Group , February, 2004*