School of Engineering and Design
Electronic & Computer Engineering

DESIGN OF MULTI-HOMING ARCHITECTURE FOR MOBILE HOSTS

A thesis submitted for the degree of Doctor of Philosophy

Adnan K. Kiani
Brunel University

Supervisor: Dr Qiang Ni

Co-Supervisor: Dr Wenbing Yao

June 2009

Acknowledgements

First of all, I would like to thank Allah Almighty for giving me the strength and courage to complete my research.

I would also like to thank my supervisors Dr. Qiang Ni and Dr. Wenbing Yao. Without their help and guidance, I would not have been able to finish my research and carry out the simulation work.

I would also like to thank my parents who have supported me throughout the course of my research. There have been many occasions where I needed their moral and financial support. Also, my friends who I stayed with through the course. They have been very caring and understanding.

Adnan Kiani

Abstract

This thesis proposes a new multi-homing mobile architecture for future heterogeneous network environment.

First, a new multi-homed mobile architecture called Multi Network Switching enabled Mobile IPv6 (MNS-MIP6) is proposed which enables a Mobile Node (MN) having multiple communication paths between itself and its Correspondent Node (CN) to take full advantage of being multi-homed. Multiple communication paths exist because MN, CN, or both are simultaneously attached to multiple access networks. A new sub layer is introduced within IP layer of the host's protocol stack. A context is established between the MN and the CN. Through this context, additional IP addresses are exchanged between the two. Our MNS-MIP6 architecture allows one communication to smoothly switch from one interface/communication path to another. This switch remains transparent to other layers above IP.

Second, to make communication more reliable in multi-homed mobile environments, a new failure detection and recovery mechanism called Mobile Reach ability Protocol (M-REAP) is designed within the proposed MNS-MIP6 architecture. The analysis shows that our new mechanism makes communication more reliable than the existing failure detection and recovery procedures in multi-homed mobile environments.

Third, a new network selection mechanism is introduced in the proposed architecture which enables a multi-homed MN to choose the network best suited for particular application traffic. A Policy Engine is defined which takes parameters from

the available networks, compares them according to application profiles and user preferences, and chooses the best network. The results show that in multi-homed mobile environment, load can be shared among different networks/interfaces through our proposed load sharing mechanism.

Fourth, a seamless handover procedure is introduced in the system which enables multi-homed MN to seamlessly roam in a heterogeneous network environment. Layer 2 triggers are defined which assist in handover process. When Signal to Noise Ratio (SNR) on a currently used active interface becomes low, a switch is made to a different active interface. We show through mathematical and simulation analysis that our proposed scheme outperforms the existing popular handover management enhancement scheme in MIPv6 networks namely Fast Handover for MIPv6 (FMIPv6).

Finally, a mechanism is introduced to allow legacy hosts to communicate with MNS-MIP6 MNs and gain the benefits of reliability, load sharing and seamless handover. The mechanism involves introducing middle boxes in CN's network. These boxes are called Proxy-MNS boxes. Context is established between the middle boxes and a multi-homed MN.

Table of Contents

List of Figures

List of Tables:

List of Acronyms:

MN	Mobile Node
MSP	Mobility Service Provider
CN	Correspondent Node
HA	Home Agent
HN	Home Network
HoA	Home of Address
CoA	Care of Address
BT	Bidirectional Tunneling mode
RO	Route Optimisation mode
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
MIP6	Mobile IP Version 6
IETF	Internet Engineering Task Force
HIP	Host Identity Protocol
HIT	Host Identity Tag
SCTP	Stream Transmission Control Protocol
mSCTP	mobile Stream Transmission Control Protocol
API	Applications programming interface
DHAAD	Dynamic Home Agent Address Discovery
BU	Binding Update
FBU	Fast Binding Update
BA	Binding Acknowledgement
FBack	Fast Binding Acknowledgement
BID	Binding Identifier

CoTi	Care of Address Test Initiator
CoT	Care of Address Test
SHIM6	Site Multi-homing With IPv6 Intermediation
HBA	Host Based Addressing
CGA	Cryptographically Generated Addressing
ULID	Upper Layer Identifier
PE	Policy Engine
FBD	Forced Bidirectional Detection
4G	Fourth Generation
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
FII	Forked Instance Identifier
WLAN	Wireless LAN
UMTS	Universal Mobile Telecommunications System
WiMAX	Worldwide Interoperability for Microwave Access
WiFi	Wireless Fidelity
GSM	Global System for Mobile Communications
SNR	Signal To Noise Ratio
AR	Access Router
AP	Access Point
RA	Router Advertisement
MAC	Media Access Control
ARP	Address Resolution Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
DHCP	Dynamic Host Configuration Protocol
IS	Information Server

FNA	Fast Neighbor Advertisement
MAP	Mobility Anchor Point
MAG	Mobile Access Gateway
PBU	Proxy Binding Update
LIN6	Location Independent Network Architecture for IPv6
MA	Mobility Agent
IFID	Interface Identifier
AAA	Authentication, Access, and Accounting
DNS	Domain Name System
ISP	Internet Service Provider
RR	Resource Record
CMULA	Centrally Managed Unique Local Address
PA	Provider Aggregatable
FQDN	Fully Qualified Domain Name
TTL	Time To Live
GGSN	Gateway GPRS support node
IP	Internet protocol
IPSec	IP security
IST	Information society technologies
LAN	Local Area Network
IeDR	Inter-domain Handover
IeTR	Inter-technology Handover
IaTR	Intra-technology Handover
IaDR	Intra-domain Handover
IeLM	Inter-link Mobility
IaLM	Intra-link Mobility
MSP	Mobility Service Provider

NAS	Network Access Server
NAT	Network Address Translation
PDA	Personal Digital Assistant
QoS	Quality of Service
RTCP	RTP Control Protocol
RTP	Real-time Transport Protocol
RTS	Request to Send
RTT	Round-trip Time
SC	Service Control
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS support node
SLA	Service-level Agreement
SP	Service Provider
UWB	Ultra-wideband
VoIP	Voice over IP
WiFi	Wireless Fidelity
WIMP	Weak Identifier Multi-homing Protocol
WLAN	Wireless Local Area Network

Chapter 1

1 Introduction

In the last decade we have seen a tremendous growth in the amount of Internet hosts both fixed and mobile. Initial protocol used to support mobility in network layer was Internet Protocol version 4 (IPv4) [2]. IPv4 addressing was based on 32-bit addresses. As Internet experienced a mushroom growth and more and more devices equipped with Internet support came out, it is clear that the IPv4 addressing scheme became insufficient to provide the necessary support [3]. Hence, a new version of IP, version 6 (IPv6) [3] was introduced. IPv6 addresses are 128-bit long. As opposed to the older version, IPv6 is considered sufficient for years to come. Mobility in the Internet of today is supported by Mobile IP [4] protocol. As Internet community shifted its emphasis from IPv4 to IPv6, a lot of the issues in different related technologies also have to make the switch. Two such important issues are multi-homing and mobility.

Multi-homing is a process of attaching a subscriber to more than a single access point in the network. This subscriber can be a single host, a router or a whole network site e.g. enterprise network.

Multi-homing can introduce great benefits in mobile environments. As multi-homed MN frequently changes its location in the Internet, it should be able to gain advantage of

being multi-homed. Potential advantages could be more reliable communication, fair load sharing capabilities, and seamless handover.

MN can be multi-homed in one of two configurations: multi prefixed or multi interfaced. In multi prefixed configuration several prefixes are advertised on the link or links to which the MN is attached. The presence of multiple prefixes results in configuration of multiple IP addresses for MN. In multi interfaced configuration, the MN has several interfaces to choose between on a single or multiple links [1]. In essence multi-homing an MN refers to a situation where the node has more than one IP addresses to choose between on the Internet.

In traditional Internet environment, IP address plays the role of both identifying a node and representing its location. This is sufficient when Internet nodes are static and single homed. However, for MNs changing their locations frequently, there is a need to decouple the identification of nodes from their location [82]. While MN's location changes due to its movement, the identification should remain unchanged. Decoupling of node identification from its location is also required for multi-homed nodes having more than one globally routable address. Each address represents location of node in Internet. However, for maintaining sessions during communication a single identity must be chosen.

IETF formed a number of working groups which were related directly or indirectly to multi-homing issues in MN. These working groups include multi6 [5], HIP [6], TSVWG [7], MEXT [8], and SHIM6 [9]. However, up until present day, multi-homing and mobility are treated as disjoint issues in IPv6

research community [24]. Separate protocols are developed to tackle them individually. There is thus no cohesion between the two issues. Recently, many new IPv6 terminals have come out which are both mobile and equipped with multiple air interfaces. Therefore there is a potential benefit to design a new architecture which unifies the capabilities of mobility and multi-homing. In doing so, multi-homing enabled mobile terminals are able to support communication with peers using multiple communication paths.

In mobility, addresses change sequentially when MN moves across networks whereas in multi-homing, node is configured with multiple addresses at a given time and it can choose the communication path according to some rules/preferences. In both mobility and multi-homing scenarios, switching takes place between different addresses. However, the motivations are different for each. MN roaming in a heterogeneous network environment should also be able to take advantage of being multi-homed. Hence, design of a multi-homing support platform in mobile environment is a challenging task. In the following section, we summarize the main features which a new multi-homing mobility architecture should have and the main research challenges which arise in order to achieve those features. Typical network scenario of multi-homed mobile environment is given in Figure 1-1.

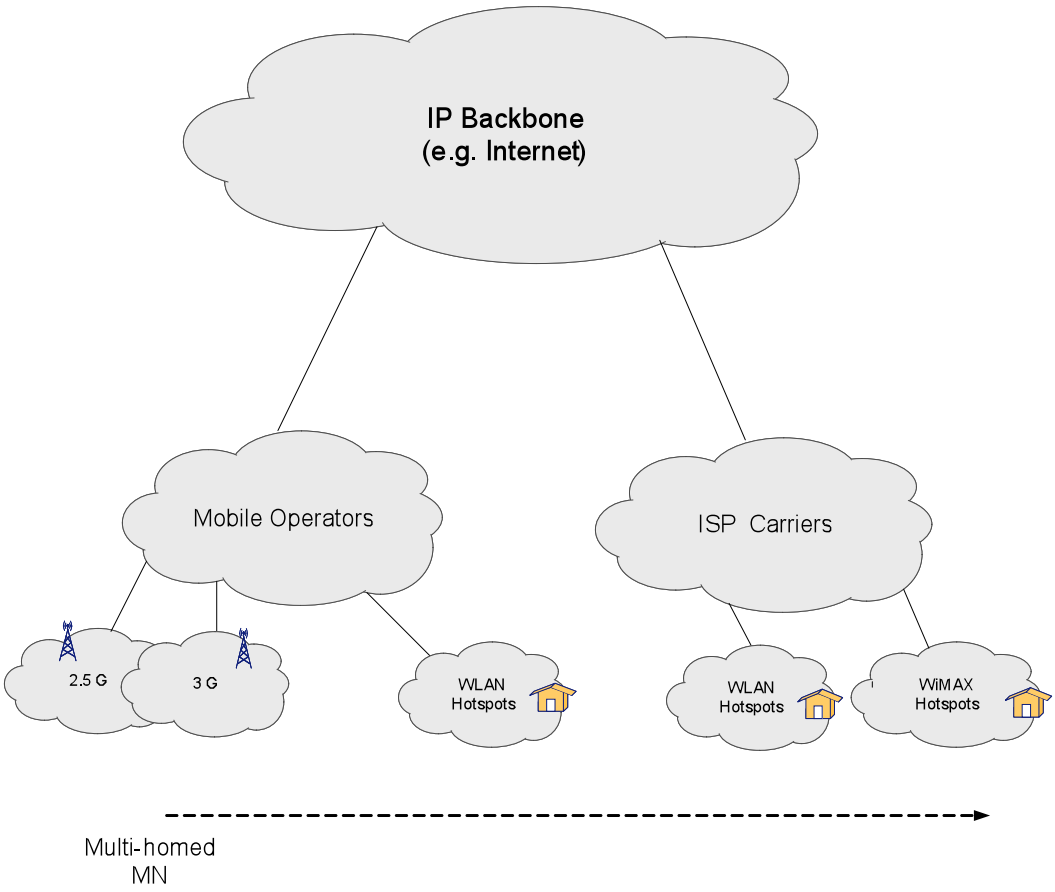

Figure 1-1: Multi-homed Mobility Network Architecture

1.1 Research Challenges

A Clean Architecture

A clean architecture should be designed where multi-homing and mobility are separated. Changes in one should not affect the other. For instance, if MN is not multi-homed, it should still be able to use mobility support protocol. Designing such an architecture involves decoupling location of IP address from

its identity while distinctively providing multi-homing support in mobility environment.

More Reliable Communication

One of the most prominent benefit of multi-homing is to provide reliable communication. Such multi-homing architecture should be defined which enables quick failure detection and recovery in the path between MN and CN. In present day wireless mobile environment, failures are much more frequent. For instance, a particular network's SNR can rapidly deteriorate resulting in failure. The multi-homing mobile architecture should be able to provide reliability support in such dynamic situations.

Network Selection Capability

Multi-homed MN should be able to use multiple communication paths between itself and CN and to select the network best suited for a particular traffic. Architecture should define mechanism which enables traffic to be routed through the best network among different networks/interfaces according to some defined rules. This is a challenging task especially in heterogeneous networks environments where quality of service parameters change their values rapidly.

Seamless Handover Capability

One of the main issues in today's mobile environment is seamless handover. Such multi-homing architecture should be defined which enable seamless handovers in mobile environments. There should be minimum delay during handovers.

Minimal Deployment Changes to Existing Infrastructure

There should be minimal changes to the existing Internet infrastructure. Efforts should be made to use existing network entities/nodes. There should also be minimal changes to the existing network applications. Ideally, existing applications running on the Internet should not be changed. This presents a great challenge as current Internet entities/nodes and applications are designed to deal with multi-homing and mobility separately.

Minimal Disruption to Communication during Switching

In multi-homed mobile environments when switch is to be made from one network/interface to another, it should cause minimal disruption to on-going communication sessions. The switch should be transparent to layers above IP. Real-time applications can only tolerate delays in the range of milliseconds. Hence, the switching mechanism needs to be very fast.

Some work has been done to address the above-mentioned challenges. We summarize the existing work in the following section.

1.2 Related Work in the Literature

Host Identity Protocol (HIP)

Host Identity Protocol [10] was first introduced in 2003 in an Internet draft document. It introduces cryptographic

identifiers called Host Identity Tags (HITs) in the application layer. These tags are mapped to multiple locators at HIP sub layer which is introduced between Transport and IP layer. HIT is 128-bit hash value of the host-identifier presented to the transport layer. Therefore, IP address has only the role of representing location of a host on the Internet. Initial HIP draft didn't support change of IP addresses once communication had been established. It only allowed hosts to use the IP addresses exchanged with their peers during initial HIP exchange. An extension to the original draft [11] was presented which allowed the IP addresses change during on-going communication with peer. When a host wishes to change its IP address, it informs its peers through HIP Readdress packet. Peer checks reach ability of the host by sending back HIP address check packet and subsequently host replies with Address Check Reply Packet. Keeping IP address to represent only the node location allows sessions survivability during movement. There is also a registrar element introduced called rendezvous server. Rendezvous server maps node identity to its location. When MN changes its location, it updates the rendezvous server with the new location. This way, the movement remains transparent to upper layers [12].

Although HIP enables decoupling of node's identity from its location, there is a massive deployment barrier. In order to deploy HIP, the current Internet infrastructure has to undergo a huge overhaul. All the network stack has to be changed. In addition, HIP mechanism does not describe the ways in which multi-homing benefits such as reliability, and load sharing could be realized.

Stream Control Transmission Protocol (SCTP)

Stream Control Transmission Protocol (SCTP) [13] is a Transport Layer Protocol first presented in IETF's Signaling Transport (SIGTRAN) working group in 2000. The work is now maintained by IETF Transport Area (TSVWG) working group. The protocol is similar to other Transport Layer Protocols [14][15] in the sense that it ensures reliable in-sequence transmission of messages with congestion control. In addition, multi-homing is inherently supported in SCTP which makes it different from other protocols in transport layer. There are two kinds of paths defined: a primary path and a set of backup or secondary paths. If a packet on primary path is lost it is retransmitted on the secondary or back up path while new packets continue to use the primary path. This way, packet transmission is guaranteed during failovers. If a primary path goes down permanently, the failure is detected through non reception of acknowledgements even after successive packet retransmissions. A new primary path is selected from the set of backup paths.

Thus, in SCTP, multi-homing is supported by simultaneously associating multiple paths with a single session. In the initial draft however, node's mobility was not considered. A new idea was presented called mobile SCTP (mSCTP) [16]. An ADDIP extension was introduced which enables an SCTP endpoint to add a new IP address, delete an existing IP address, and change the primary IP address used for association while association is active. When an SCTP endpoint wants to add, delete, or change the IP address, it sends a ASCONF (Address Configuration Change) chunk to the remote endpoint. Hence,

both mobility and multi-homing are supported through mSCTP. The procedure is shown in Figure1-2.

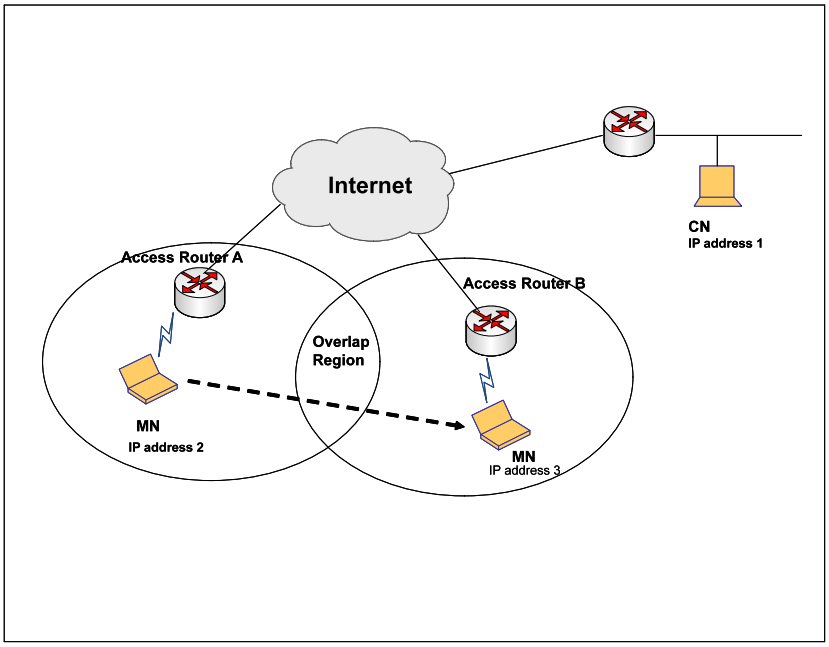

Figure 1-2: mSCTP Architecture

In the Figure, it is assumed that after an SCTP association is initiated between MN and CN, MN moves from access router A to access router B. The initial association is between IP address 2 of MN and IP address 1 of CN. When MN moves into the overlapping region, it obtains a new IP address 3 from access router B. MN then sends SCTP ASCONF chunk to CN to add the new IP address to SCTP association. CN acknowledges with ASCONF-ACK chunk. When MN moves out of the overlapping area and into access router B's coverage, it needs to change the primary IP address of SCTP association to IP address 3. The previous IP address is then deleted from the association.

SCTP nodes can only communicate with other SCTP nodes. There is no location management entity defined. This makes it

an incomplete mobility solution. For instance, there are no events defined which trigger primary address change. Similarly, there is no provision defined for when an address is to be deleted from an association. In addition, address change is not transparent to upper layers. There are no provisions on how multi-homing benefits of reliability, load sharing, and seamless handover can be realized.

Mobile IPv6 (MIPv6) and Its Extensions

MIPv6 is a widely accepted mobility solution. MIPv6 uses indirection mechanism to provide mobility support to MN. MN is assigned a permanent address in its home network known as its HoA. It also discovers a router known as its HA through Dynamic Home Agent Address Discovery mechanism. When this MN moves away from its Home Network, it obtains a new temporary address known as CoA.

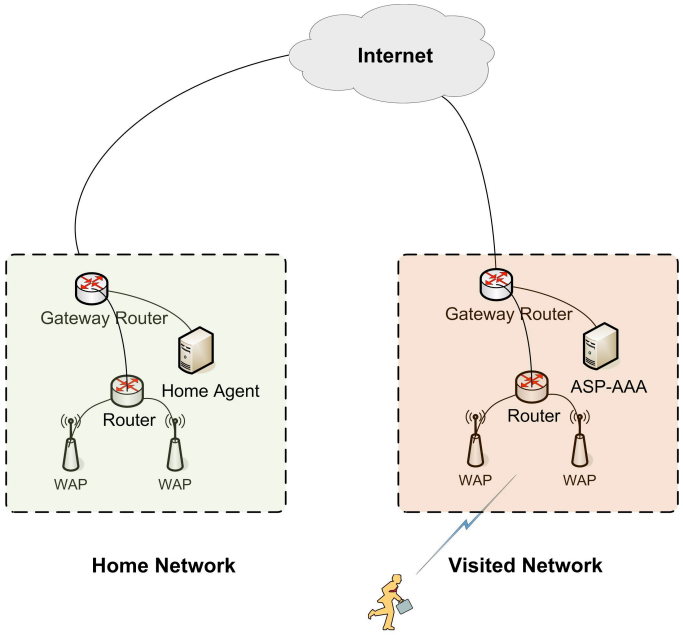

Figure 1-3: MIPv6 Network

MIPv6 is purely a mobility solution. It was proposed at a time when mobility and multi-homing were treated as separate paradigms in networking world. Hence, no need was felt to address the issue of multi-homing when defining a mobility protocol i.e. MIPv6 [17]. In recent times however, all this has changed. More and more networks are being introduced and Internet devices equipped with multiple air interfaces supporting such networks have come out. The need was thus felt to upgrade MIPv6 to support multi-homing.

IETF took up the task and a new working group MObile Nodes And Multiple Interfaces in IPv6 (MONAMI) came into existence. The main goal of this working group was to explore the possibility of how a MIPv6 supported MN or a mobile network running Network Mobility (NEMO) basic support could benefit from having multiple interfaces. MN having multiple interfaces can truly benefit from using them simultaneously.

A draft was presented in MONAMI (presently MEXT) working group of IETF [18]. According to the draft, MIPv6 could be extended such that multiple CoAs could be bound to a single HoA. A new Binding Identification Number (BID) is introduced to distinguish multiple bindings to the same HoA. When MN configures multiple IPv6 addresses on one or more of its interfaces, it registers these addresses as CoAs with its HA. Each CoA is represented by a unique BID which is stored in binding update list. MN can then register the CoA by sending a Binding Update (BU) message including the Binding Identifier mobility option containing the BID. MN can register multiple CoAs by either independently sending separate BUs to the HA

or multiple at once in a single BU. The latter is known as bulk registration. In route optimization mode also, multiple CoAs can be registered with the CN. However, bulk registration is not permitted. In addition, in route optimization mode, return rout ability operations have to be run for each CoA. This includes the exchange of CoTi/CoT messages between MN and CN.

There are different ways in which MN running MIPv6 could be multi-homed. This includes cases where MN is equipped with multiple HoAs. A general network scenario could be, for instance, the MN is provided mobility service through multiple providers. Each provider delegates an HA and thus a separate HoA for its service, thus the MN is allocated multiple HoAs. In the IETF draft such multi-homing scenarios are not considered. The main MIPv6 assumption is followed that binding is associated with a single HoA. Once HoA becomes invalid, the whole of MIPv6 instance becomes obsolete. Thus, it is fairly reasonable to suggest that although the draft tackles some multi-homing configurations i.e. those where MN has multiple CoAs, it does not tackle multi-homing in MIPv6 networks as a whole. It is not a generalized mobility/multi-homing solution.

Some work has also been carried out within IETF's NEMO working group. The aim is to provide multi-homing benefits to mobile networks where multiple prefixes are advertised i.e. site multi-homing. Although, site-multi-homing in mobile networks is an interesting area of research, it is outside the scope of this thesis. Our focus is on host multi-homing i.e. multi-homed MN.

Main advantages of multi-homing listed in [19] are that it makes communication more reliable and it enables load to be shared among different paths. The MONAMI draft uses existing MIPv6 mechanisms to detect failures and recover from them. In mobile/multi-homing configurations these techniques are often too slow which result in sessions breaking. In addition, the draft doesn't tackle the problem of how load is to be shared between different CoAs.

Hence, the draft doesn't explain how various multi-homing benefits i.e. reliability, and load sharing could be gained by using the mechanism.

Site Multi-homing With IPv6 Intermediation (SHIM6)

A multi-homing solution was presented in IETF's multi6 working group in late 2004. The proposal is called Site Multi-homing With IPv6 Intermediation SHIM6 [20][21]. A shim sub layer is introduced within IP layer of an end host. Sites are allocated multiple provider-assigned IP address prefixes. These prefixes result in configuration of multiple IPv6 addresses for each host within the site. A SHIM6 context is established between two communicating hosts. This context holds information to uniquely identify a communication session and all the available addresses of hosts. In SHIM6, set of addresses are bound to a multi-homed host by using either Host Based Addressing [22] or Cryptographically Generated Addressing [23] mechanism. Through these mechanisms, it can be verified that a given address belongs to the set. A SHIM6 context is established through 4-way handshake. Messages involved in context establishment are 11, R1, I2, R2, R1bis, and I2bis.

Message formats are given later in the chapter. The context establishment mechanism is explained through steps.

The initiator of SHIM6 context sends an I1 message and waits for R1 message from the responder. If it doesn't receive an R1 message within the timeout (4 sec), it resends I1 message. Initiator keeps retransmitting I1 message without receiving R1 message until I1_RETRIES_MAX attempt (set to 4). When the initiator receives R1 message, it sends I2 message to the responder and waits for R2 message. Again, if it doesn't receive an R2 message within the timeout, it resends I2 message. I2 message is retransmitted without receiving R2 message until I2_RETRIES_MAX attempt (set to 2). During the context establishment, hosts exchange their list of available addresses. From this list, an address is chosen as Upper Layer Identifier (ULID) for each host. The remaining addresses are set as locators. ULID is used to identify a session and remains unchanged whereas locators are used to locate the host and can change through communication. List of locators can be updated and their preferences can be set by exchanging Update Request (UR) and Update Acknowledgement (UA) messages between communicating peers.

SHIM6 deployment does not introduce many complexities to the existing Internet infrastructure. It also provides session survivability when IP addresses are switched [24].

SHIM6 thus decouples the two roles of an IP address i.e. identification and location. Main aim of SHIM6 is to failover to a different locator pair should the original pair stop working. At the same time, the switch is kept transparent to layers above IP.

Locator/identifier splitting mechanism makes SHIM6 a suitable candidate for supporting mobility in addition to multi-homing in IPv6 networks. This has been highlighted in [25]. However, there are some issues which prevent SHIM6 from being a generalized mobility solution [26]. Here, we list these issues and briefly describe the reasons why SHIM6 cannot tackle them.

- *Location Management:*

  A key feature where SHIM6 lacks as a mobility solution is the location management i.e. how to locate MN in the network. In most mobility mechanisms a centralized entity is used to locate the MN. e.g. HA in MIPv6 and Rendezvous server in HIP.

- *Simultaneous Movements*

  When SHIM6 context is established between two hosts, the set of addresses (locators) used by each hosts are exchanged. This context survives any failures/movements as long as at least one of the locator pairs (source and destination) remain valid. However, in mobility scenarios a situation can occur where both MN and CN move simultaneously resulting in all their addresses changing. SHIM6 cannot recover from this sort of movement. In MIPv6, after a lapse of sometime, communication can be restored as there exists a common communication node between MN and CN i.e. HA.

- *Support for legacy terminals*:

  For SHIM6 to be used as a mobility solution, both communication end points i.e. MN and CN need to support

SHIM6 signaling. In case where CN is not SHIM6 enabled, communication would not survive after MN moves.

In light of the above points, it can be concluded that although SHIM6 has desirable features in terms of a mobility solution, it cannot serve as a stand-alone mobility/multi-homing solution.

Although all the proposals described in this section have some desirable features, they do not satisfy some very important issues when it comes to defining a unified mobility/multi-homing mechanism. Following highlights some of the weaknesses in the existing proposals:

- There is no clean architecture defined which allows multi-homing and mobility to be treated distinctively. Change in multi-homing aspect of a scenario should not affect mobility support and vice versa.
- There is no existing mechanism which describes procedure to make communication more reliable in mobile/multi-homed environment.
- There is no network selection procedure defined in the IP layer which allows the best network/interface to be chosen for a particular application and user in heterogeneous network environment.
- There is no support for seamless handover in any of the existing proposals.
- Some of the proposals have a very high deployment barrier which requires massive changes to existing Internet infrastructure.

- All the proposals fail to define procedures which would allow minimal disruption to communication during switching.
- Most of them do not cover all the scenarios in which an MN can be multi-homed.

Therefore, in this thesis we present a new multi-homing architecture which resolves the above issues in mobile environments.

1.3 Contributions of the thesis

The contributions of this thesis are:

- A novel Multi Network Switching in MIPv6 (MNS-MIP6) architecture is proposed for mobile networks. The architecture clearly separates multi-homing and mobility by defining a multi-homing MNS sub layer within a host's protocol suite. When multiple communication paths exist between MN and CN, the architecture allows multi-homing benefits to be achieved. Switching from one network/interface to another remains transparent to layers above IP. Through our proposed mechanism applications will experience very low disruption during switching.

- A new path failure detection and recovery mechanism is designed for multi-homed mobile environments. The mechanism allows a prominent multi-homing benefit i.e. reliability to be realized by quickly detecting failures in the path between MN and CN and recovering from them. It is shown that our proposed mechanism out performs existing MIPv6 failure detection and recovery techniques.

- A new network selection mechanism is designed to choose the network/interface that is best suited for a particular application. A Policy Engine (PE) takes network parameters and compares them according to different application profiles. A decision is made based on user inputs and application requirements. In this way, the network/interface most suited for a particular application is chosen.

- A new mechanism is designed to support seamless handovers in multi-homed mobile environments. Link layer triggers are used to anticipate the handover. SNR values on MN's interfaces are periodically checked. When an SNR value on an active interface approaches a low threshold, a trigger is generated to indicate a switch to different network/interface. Actual switching is done through our proposed multi-homing sub layer. It is shown that applications encounter much less disruption during handover as compared to MIPv6 and its various extensions.

- A new scheme is defined through which non MNS-MIPv6 supporting legacy hosts can communicate with MN and still enjoy the main multi-homing benefits of reliability, load sharing and seamless handovers. A box known as Proxy-MNS box is introduced at the edge of legacy CN's network. This box acts as a proxy for CN when communicating with MN. Through this scheme, the main benefits of reliability, load sharing, and seamless handover are gained.

- Simulations have been carried out to test our proposed multi-homing architecture in mobile environments. A process model was created using OPNET 14. This process model was then integrated as a child process model within IP layer of host's protocol suite. Various simulations were run to test our proposed architecture's performance in terms of reliability, load sharing, and seamless handover in multi-homed mobile environments.

1.4 Structure of the Thesis

The structure of this thesis is as follows:

In chapter 2, we design architecture to support multi-homing in mobile environments. The architecture is called Multi Network Switching in MIPv6 Networks (MNS-MIP6). We recognize that MIPv6 is the most popular and widely deployed protocol to support mobility in IPv6 networks. We first describe different configurations in which a MN running MIPv6 can be multi-homed and explain how MIPv6 and its multi-

homing extension fall short of providing main multi-homing benefits. Then we propose a new multi-homing architecture for MIPv6 networks called MNS-MIP6. A new MNS sub layer is introduced within the IP layer of hosts. A context is established between MN and CN and all the additional addresses are set as locators for the context. This context is then used to switch between different networks/interfaces. This switch remains transparent to layers above IP ensuring survivability for on-going communication sessions. We briefly describe how our architecture enables reliability, load sharing, and seamless handovers in MIPv6 networks.

In chapter 3, we propose a mechanism to ensure reliability in multi-homed MIPv6 environments. A new failure detection and recovery mechanism is defined which enables quick detection and recovery from path failures between MN and CN. Context is established between MN and CN and the additional addresses form the locator set. The procedure is based on Forced Bidirectional Detection (FBD). When there is data traffic in one direction, there should be data traffic or keep alive messages flowing in the opposite direction. In absence of any data traffic or keep alive messages for a specific time out, failure is detected. Probe messages are sent using locator from the locator set. This is continued until a working pair in both directions is found. The reliability mechanism is compared with existing MIPv6 failure detection and recovery scheme and a marked improvement is noted.

Chapter 4 describes a network selection mechanism for multi-homed MN running MIPv6. Through this mechanism, network best suited for particular application and user preference is

chosen. The mechanism involves two basic functions. One is to make a decision of which network to use for a particular application and user. The second function is to actually switch the traffic to the particular network if it is not currently being used.

A policy engine (PE) is defined which takes parameters from the different networks. These network parameters are compared with pre-defined application profiles. A decision algorithm is run to choose the network which suits a particular application and user preference. There are four network parameters we use for making the decision. These are available bandwidth, latency, cost and link quality. The decision algorithm takes user preference and application requirements and chooses the most suitable network. Actual switch to the particular network/interface is made through SHIM6 signaling. Simulations are run to test our proposed mechanism and the results are satisfactory.

In chapter 5 we design a mechanism to support seamless handover in multi-homed MIPv6 environments. A context is established between MN and CN. Link layer Triggers are used to assist mobility. Three triggers are defined. These are Link_GoingDown, Link_Down, and Link_Up triggers. When signal on a particular active interface becomes low, Link_GoingDown trigger is generated. A switch is made from a particular interface to another. We follow the procedure of Fast Mobile IPv6 (FMIPv6) where SNR on each interface of MN is periodically scanned. When the SNR value on an active interface approaches low threshold, a Link_GoingDown trigger is generated. Switch is then made to a different

network/interface through MNS sub layer. When SNR value on an interface becomes too low, a Link_Down trigger is generated. IP address associated with the down interface is deleted from locator list of MNS sub layer. Similarly, when an interface becomes active and an IP address is assigned, a Link_Up trigger is generated and IP address on the new interface is added to the locator list.

We compare our proposed seamless handover mechanism with a promising MIPv6 extension FMIPV6 and recognize that our proposal performs better.

In chapter 6, we design a procedure which enables a legacy non-MNS-MIP6 CN to communicate with MNS-MIP6 enabled MN and gain the multi-homing benefits described in Chapters 3, 4, and 5. A Box known as Proxy-MNS box is introduced in the legacy CN's network. This box acts as a proxy for CN. A context is established between MN and the box and multi-homing benefits of reliability, load sharing, and seamless handover are realized.

In chapter 7, we summarize the thesis and discuss future work.

Chapter 2

2 MNS-MIP6: A New Multi-homing Mobile Architecture

In today's heterogeneous network environment, mobile Internet devices are often configured with multiple interfaces/addresses belonging to distinct access technologies i.e. they are multi-homed. These devices should be able to use these interfaces/addresses to gain true benefits of multi-homing. In the previous chapter we have outlined some of the work done so far in defining a unified mobility/multi-homing solution. However, all these solutions have short comings. These solutions either require massive changes to the existing Internet infrastructure in order to be deployed e.g. HIP, fail to provide mobility e.g. SCTP, SHIM6, or multi-homing MIPv6 and its extensions.

We consider all these issues and conclude that existing mobility/multi-homing mechanisms should be employed so Internet infrastructure experiences least changes.

In this Chapter, we present a new multi-homing mobile architecture which mitigates the shortcomings of other solutions. We introduce a new MNS sub layer within IP layer of host's protocol stack. The resulting architecture is called MNS enabled MIPv6 or MNS-MIP6. In our proposed MNS-MIP6 architecture, some of the rich attributes of SHIM6 are used along with MIPv6.

With our design, minimal deployment changes are needed to the existing Internet infrastructure. The reason to adapt MIPv6 in our design is that MIPv6 is a widely accepted mobility solution for the Internet. However, MIPv6 does not support multi-homing. In our proposal, a new MNS sub layer is used to support multi-homing in MIPv6 networks. Multi-homed MN running MIPv6 gains advantage of using multiple interfaces/addresses. The main advantages of being multi-homed are reliability, and network selection. We analyze how MIPv6 and its IETF extension fail to provide these advantages.

After describing the MNS-MIP6 mechanism in this chapter, we analyze how performance is improved in three key areas of reliability, network selection and seamless mobility in chapters three, four, and five respectively.

2.1 Introduction/Problem Statement

As Internet communication is evolving, there is a greater need to develop systems that can take full advantage of the heterogeneous network environment. Mobile Internet devices of today are equipped with multiple interfaces belonging to distinct access technologies. More than one of these interfaces may be active at a time. This gives rise to a situation where multiple paths exist between communicating devices or devices are said to be multi-homed. Although, as explained in the last chapter, some effort has been made to come up with a solution which enables such mobile Internet devices to benefit from being multi-homed, they all have some problems. Solution should cover all the mobility/multi-homing aspects and should be such that it requires minimum changes to the existing Internet infrastructure. A mobile Internet device having multiple interfaces should be able to switch from one

network/interface to another without disrupting on-going sessions. In other words, the switch should be transparent to layers above IP. Keeping this in mind, it seems logical to come up with an idea which uses existing Internet stack and enables a mobile device to be multi-homed.

In the Internet infrastructure of today, MIPv6 is widely accepted network layer protocol for providing mobility. Thus, aim should be to come up with a solution which provides multi-homing support in MIPv6 networks [27]. Although some work within IETF aims to tackle the issue, we notice that there are many short comings. In addition all the multi-homing configurations are not covered. Multi interfaced mobile Internet device running MIPv6 could be multi-homed in different ways. It can be allocated multiple HoAs from different MSPs. Multiple CoAs could also be configured on mobile device's interfaces.

In such situations, the device having multiple interfaces can be allocated multiple IP addresses. In order to take true advantage of multi-homing, the device should be able to use these addresses simultaneously. Current specification of MIPv6 lacks this support.

In MIPv6, mobile device is referred to as MN. Path between this MN and CN can be divided into two portions: the path between HA and CN and the path between MN and HA. In route optimization mode, an additional path exists between MN and CN. Being multi-homed means that one or all of these paths have at least one alternative. Main goals of multi-homing outlined in [28] are reliability, network selection and flow distribution. These goals are only achieved when alternative paths can be used as backup in case of failure, or used

simultaneously along with primary path for network selection. As explained in the draft, in order to achieve session survivability, the use of alternative paths should be transparent to layers above IP.

In addition to multi-homing benefits, a multi interfaced MN running MIPv6 should be able to roam through various access networks seamlessly without loss of connectivity. There is no existing mechanism to tackle this issue.

In this chapter, we propose a unified multi-homing/mobility mechanism called MNS-MIP6. The architecture enables a device running MIPv6 to gain true advantages of multi-homing by integrating some aspects of an existing site multi-homing solution with MIPv6. A new MNS sub layer is introduced in the host's protocol stack just above MIPv6 sub layer. In addition to providing multi-homing advantages, i.e. reliability, network selection etc, it is shown that through the use of our proposed mechanism a seamless handover procedure is introduced in MIPv6 networks. This results in less session disruption.

Multi-homing Scenarios in MIPv6 Networks

MN running MIPv6 is multi-homed in cases where either it has multiple HoAs, multiple CoAs or a combination of both. MN would have multiple HoAs if multiple prefixes are available on the home link or if it has multiple interfaces attached to distinct home links [29]. In our study we consider the latter case. Similarly, MN would have multiple CoAs if multiple prefixes are available on the foreign link or if it has multiple interfaces attached to distinct foreign links. Again the latter case is considered. In addition, MN could also be multi-homed if HA has multiple addresses. Although MN equipped with a

single air interface could be multi-homed, a more interesting and realistic configuration is when a multi-homed MN has multiple air interfaces bound to distinct access technologies. The focus of this thesis is on multi-homing a multi-interfaced MN running MIPv6. Hence, in all the subsequent discussion we use the term multi-homed MN to refer to an MN with multiple air interfaces.

All possible ways in which MIPv6 enabled MN could be multi-homed are listed in [28]. Here, we discuss them again. Note that n is a natural number greater than 1.

a) 1 HoA, 1 CoA

In case where MN has two interfaces, a situation may arise where MN is simultaneously connected to its home link and a foreign link. The HoA is configured on the interface connected to the home link while a CoA is configured on the second interface.

b) n HoA, 1 CoA

A MN is multi-homed when it is configured with multiple HoAs. Multiple HoAs exist when access to the Internet is provided through different HAs which are possibly belonging to different access technologies. MN will thus have an HoA per HA. Another possibility is when MN's home network is multi-homed to the Internet through multiple providers. As a result, multiple prefixes are advertised on MN's home link giving rise to configuration of multiple HoAs. A single CoA is configured on the visited foreign network. This CoA is bound to all the HoAs. When MN has multiple interfaces, only one interface would be attached to the foreign network. All the other interfaces are either attached to the home links or are inactive.

c) 1 HoA, n CoA

MN is multi-homed in this configuration as there are multiple CoAs. This may occur when MN has multiple interfaces attached to different links. There is also a possibility of foreign network being multi-homed giving rise to multiple prefixes being advertised on a single link. When MN has multiple interfaces, one of them may be connected to the home link.

d) n HoA, n CoA

MN is multi-homed in this configuration as it has multiple addresses. This case can be taken as a combination of cases b) and c). i.e. MN has multiple HoAs and CoAs.

Different scenarios in which a MIPv6 enabled MN could be multi-homed are illustrated in Figure 2-1. In the Figure CoA1, CoA2, and CoA3 are bound to HoA1 on Interface 1 and Interface 2 and CoA3 is bound to HoA2 on Interface 2.

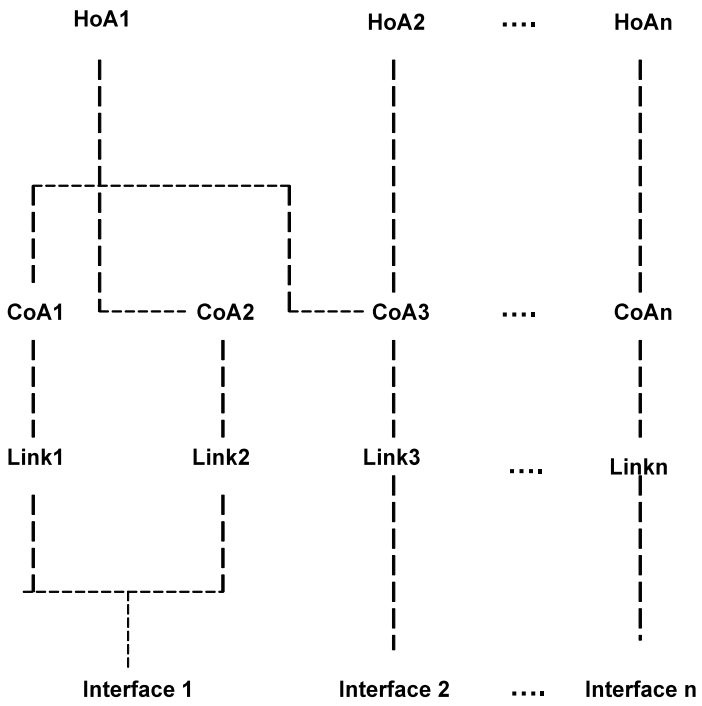

Figure 2-1: Multi-homing Scenarios for MIPv6 enabled MN

Problems with MIPv6 in Multi-homing Scenarios

Main goals of multi-homing are reliability, load sharing, and flow distribution. In the configurations listed above, we analyze how MIPv6 and its MONAMI extension falls short in achieving these goals.

Reliability

HoA failures: In MIPv6, HoA is used to identify a binding. Hence, MN with multiple HoAs implies that there are multiple MIPv6 instances running. HoA failures may occur in one of the following two ways: first, the HA associated with a particular HoA fails. The second case is when HoA is no longer routed

through the HA. For HA failures, MIPv6 or its MONAMI extension doesn't provide a mechanism to transparently hand over to a different HA. Although some mechanisms have recently been introduced [4], they fail to cover the whole paradigm of HoA failures. A robust failure detection and recovery mechanism is required to switch from a failed/obsolete HoA to a new HoA.

Sessions have to be broken and restarted using a different HA. Similarly, when HoA is no longer routed to HA, again sessions have to be terminated.

CoA failures: Failures can occur anywhere along the path between MN and CN. However, in the present environment, due to the extensive use of wireless technologies, failures tend to happen more often at edges of the network. An efficient failure detection mechanism is required for such cases. In MIPv6 and its extensions, local failures are generally detected only by non reception of router advertisements within stipulated time [4]. As a result, sessions are terminated. This is not sufficient especially for applications where session continuity is essential. Once failure is detected, a new working CoA has to be found and flows have to be redirected to the new CoA. Although the MONAMI proposal enables multiple CoAs to be registered to a single HoA in MIPv6, the failure detection and recovery mechanism is the same as MIPv6 i.e. too slow.

Network Selection

Multiple HoAs: With multiple HoAs available, a mechanism is needed to select which HoA to use when a new communication flow is initiated. Similarly, CN would also be required to make a decision of which HoA is to be used when communicating with the MN. In MIPv6, such a mechanism doesn't exist. Load

should be shared between different interfaces/networks to reflect application requirements.

Multiple CoAs: A mechanism is needed to enable multiple CoAs to be registered to a single HoA. Load should be shared between different CoAs. Similarly, flow can be distributed through different paths available. Again, although the MONAMI proposal enables multiple CoAs to be registered to a single HoA in MIPv6 networks, it fails to explain how load could be shared among the different CoAs.

Robust handover mechanism in heterogeneous environments

In addition to lack of multi-homing support in heterogeneous network environment, MIPv6 also fails to address the issues related to handovers between different networks. MN equipped with multiple interfaces, should be able to move between different networks without much traffic disruption. When MIPv6 enabled MN loses connectivity to the active access router or base station, all communication is terminated. Communication doesn't resume until connectivity is established with a new access router or base stations. The disruption caused is sometimes intolerable for real-time traffic.

2.2 Proposed Architecture

In this section, a stand-alone generalized mobility/multi-homing architecture is presented which enables MN running MIPv6 to take advantage of multi-homing. In the previous chapter, it was discussed that SHIM6 is a promising multi-homing idea which fits well into the existing Internet infrastructure. However, SHIM6 is a site based instead of end host based idea. SHIM6 has some features which are quite promising for end host multi-homed/mobile environments. In

our proposed architecture, we use some attributes of SHIM6 along with MIPv6 and design a new mechanism which allows MIPv6 enabled multi-homed MNs to roam in a heterogeneous network environment and gain full multi-homing benefits.

The mechanism is called Multi Network Switch enabled MIPv6 or MNS-MIP6. It defines a new MNS sub layer within IP layer of MN's protocol stack. This layer resides above MIPv6 sub layer. Figure 2-2 shows the system architecture of MNS-MIP6.

MN which is multi-homed through multiple access networks would use MIPv6 for mobility support. MNS sub layer compliments this by allowing MN to take full advantage of having access to multiple networks. MNS sub layer resides above the MIPv6 sub layer which enables MN to switch between different networks/interfaces, or to use them simultaneously. We show that through this mechanism, multi-homing benefits of reliability and load sharing are attained. We also describe how seamless handover is supported by MNS-MIPv6.

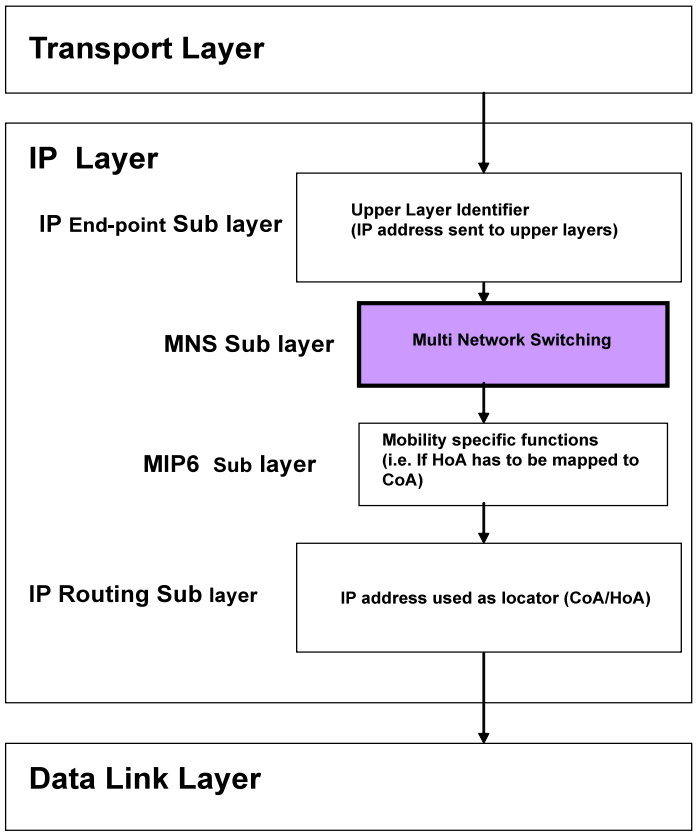

Figure 2-2: System Architecture of the Proposed MNS-MIP6

Functional block diagram of MNS sub layer is given in Figure 2-3. Three basic functions are reliability, network selection and seamless handover. Reliability consists of detecting failures and running a recovery mechanism. Network selection involves obtaining parameters from available networks, comparing the network parameters with predefined application profiles, taking user preference and making a decision. Seamless handover functionality involves accepting layer 2 triggers and making the handover decision. The three main functions are further explained in later section.

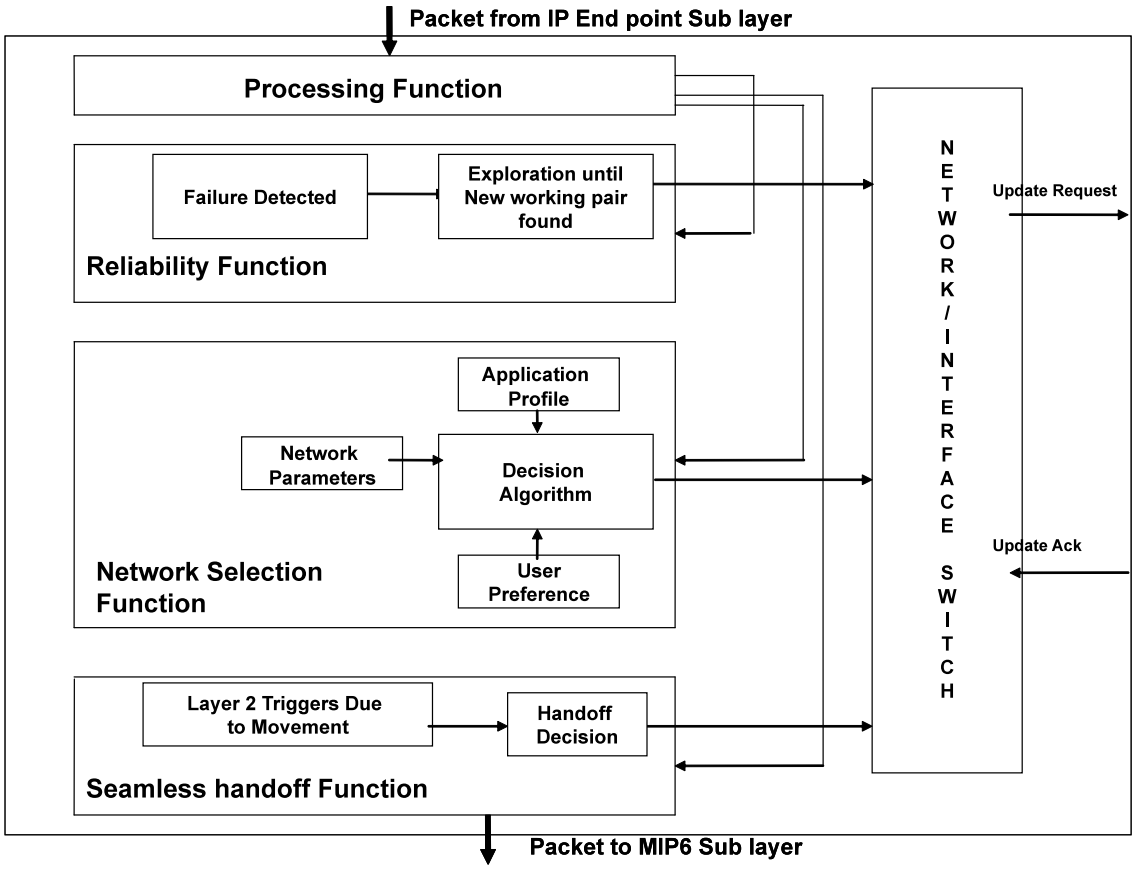

Figure 2-3: MNS Sub layer Functional Block

To gain multi-homing benefits, CN with which this MN is communicating should also have a MNS sub layer. This CN could be mobile or stationary. If CN is mobile, it also has a MIPv6 sub layer below the MNS sub layer. When BT mode of MIPv6 is being used HAs also have to be modified such that they support MNS signaling. Hence, MNS sub layer has to be introduced within HAs IP layer. MNS-MIP6 enabled MN can also communicate with non MNS legacy nodes. Although in such a scheme, multi-homing benefits would not be gained.

The architecture of MNS-MIP6 is explained with help of building blocks. After describing the various building blocks, it is explained how an MNS-MIP6 enabled MN could benefit from being multi-homed.

2.2.1 Building Blocks

Building block of an MNS-MIP6 system are the following:

Context Establishment:

In our proposed MNS-MIP6 architecture, multi-homing benefits are gained by first establishing a context between MN and CN. Context establishment is through SHIM6 signaling. Both ends of communication need to support SHIM6 signaling. An MNS-MIPv6 enabled MN uses simple IPv6 procedures when it wants to initially communicate with CN which can also be MNS-MIP6 enabled MN, MNS enabled host or just a legacy non MNS host. It obtains the IP address of CN through DNS lookup. In addition to this primary path, additional communication paths might exist between the MN and CN. In order to take full advantage of these additional paths, two ends establish a context. Through this context, MN and CN exchange all the additional IP addresses which they can use for communication. For MNS-MIP6 supported MN the additional IP addresses are the set of additional CoAs/HoAs on multiple interfaces whereas for CN the addresses can either be CoAs/HoAs if its an MN or simple normal IPv6 addresses. The set of additional addresses is called locator set of each host.

This context is similar to a normal SHIM6 context described in previous chapter. However, addresses are not generated through HBA or CGA mechanisms. Rather, normal IPv6 address configuration mechanisms are employed and in case of MNS-MIP6 supported MN they are additional CoAs/HoAs. The context could be used to switch over to a secondary communication path in case the primary path becomes unavailable i.e. reliability, or to use multiple paths simultaneously i.e. load sharing. The context could also be

used to support transparent switch/handover between different interfaces for multi interfaced MN.

Context between two hosts is actually a context between two ULIDs. The context is identified by a pair of context tags. These context tags are 47-bit randomly generated numbers. Each end of communication allocates a context tag. Once context is established, MNS control messages contain the context tag which the receiver of the message allocated. Four control messages are exchanged between communicating entities. These are I1, R1, I2, and R2 in that order. Figure 2-4 shows the normal context establishment message exchange.

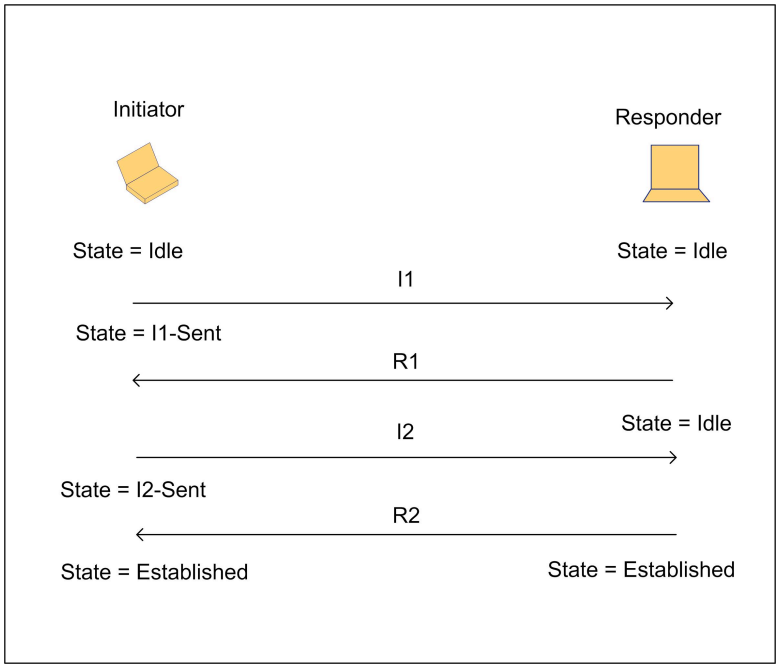

Figure 2-4: Normal Context Establishment

Control Message Formats:

All control messages have the same header. The header format is given in Figure 2-5.

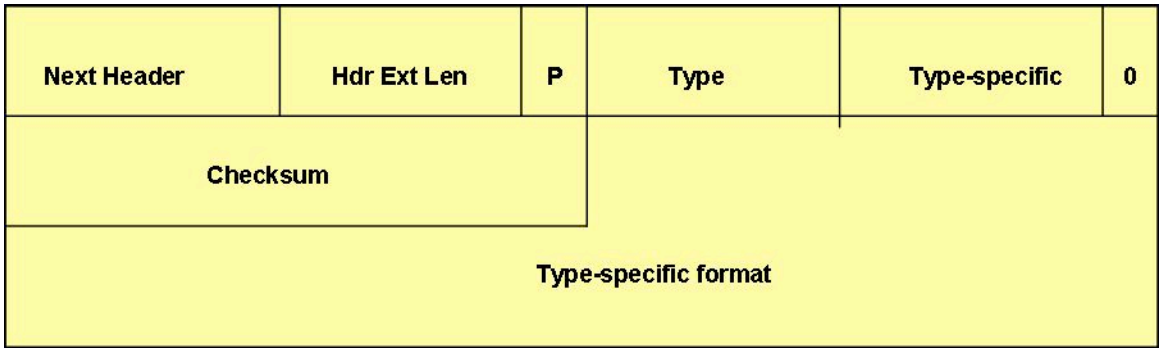

Figure 2-5: MNS-MIP6 Control Header

Fields:

The Next header and Hdr Ext Len fields are consistent with other IPv6 extension headers.

P: This bit is used to distinguish the control header from SHIM6 payload extension header. Set to zero means a MNS control message.

Type: Identifies the actual message type according to the following table 2-1.

Type-specific format: This field is different for different message types.

Type Value	Message
1	I1 (first message in context establishment)
2	R1 (the message sent in response to I1 message)
3	I2 (second message sent from the initiator)
4	R2(message sent in response to I2 message)
5	R1bis (reply to reference to non-existent context)
6	I2bis (reply to R1bis message)
64	Update Request
65	Update Acknowledgement
66	Keep-alive (modified REAP protocol)
67	Probe Message (modified REAP protocol)

Table 2-1: MNS Control Message Type Codes

I1 Message:

I1 is the first message in context establishment exchange. The Type field in MNS header is set to 1. Initiator of communication generates a context tag and sends it in I1 message. In addition, initiator sends a nonce to responder

which is a randomly generated 32-bit unsigned integer. This nonce is to be returned by responder in R1 message.

Also, if source and destination IP addresses in the IPv6 header are different from ULID pair, a ULID pair option is included in I1 message. This option contains the ULID pair for the context. Once an initiator sends I1 message, it goes to I1_Sent state and waits for R1 message from responder

R1 Message.

This is the second message in context establishment phase sent from the responder when it receives I1 message. The Type field in MNS header is set to 2. Initiator nonce is copied from I1 message and sent back in R1 message. The responder randomly generates a 32-bit unsigned integer value and sends it as responder nonce. This value is to be copied and sent back by initiator in I2 message.

I2 Message.

The third message in context establishment phase is I2 message. The Type field is set to value 3. I2 message is sent by the initiator when it receives R1 message from responder. In this message, the initiator context tag, initiator nonce, and responder nonce are sent. In addition, an options field is added at the end of I2 message. This field contains the following information.

ULID pair: When the IPv6 header source and destination addresses are different than original ULID pair, the ULID pair option is included.

Forked Instance Identifier (FII): Is part of original SHIM6 protocol. In I2 message all the bits are kept 0.

Locator List: Initiator can send the list of HoAs/CoAs it wants to use for the specific context.

Locator Preferences: If preferences are to be set for different locators, this option is added in I2 message.

R2 Message.

This is the fourth message in context establishment phase. The Type value in MNS header is set to 4. R2 message is sent by the responder when it receives I2 message. Also, if both the hosts send I1 messages at the same time, R2 message is sent.

The responder generates a 47-bit Responder Context Tag and sends it in R2 message. Additionally, Initiator nonce is copied from I2 message and sent. The following options are also added in R2 message:

Locator List: List of locators which the responder wants to use for the context.

Locator Preferences: Has the same function as the option in I2 message.

R1bis Message.

The four messages explained earlier are involved in context establishment exchange. A situation could arise when a payload packet or Update Request/Probe message arrives at a host for which there doesn't exist any context. The receiver of such messages would then generate an R1bis message. Through this message, the host informs its peer that there doesn't exist any context. When the peer receives R1bis message, it tries to re-establish the lost context and sending I2bis message back.

The Type field in MNS header is set to 5. R1bis message contains the packet context tag field having context tag from the received message for which there was no existent context. A responder nonce is also sent in R1bis message which is to be copied by the initiator and sent in I2bis message.

I2bis Message:

I2bis message is sent when the initiator receives a R1bis message. The purpose of this message is to recover from a lost context. Type field for this message is set as 6. Initiator Context Tag, Initiator Nonce, and Responder Nonce copied from R1bis message are sent in I2bis message. In addition, the Packet Context Tag copied from R1bis message is also sent in this message. The options fields contained in this message are the same as for I2 message. Once the responder receives an I2bis message, it sends back an R2 message resulting in context being fully established.

Locator Switch:

In MNS-MIP6 system switching between different locators is done through UR/UA message exchange. In MNS-MIP6 architecture there are three flags defined within the UR message. These are change_loc_pref, add_loc, and remove_loc flags. When an MNS-MIP6 enabled MN wants to switch locators for a specific context, it sends UR message with change_loc_pref flag set. The locator to which communication is to be switched to is put in the locator field. . When CN receives the UR message, it checks the context tag, updates locator preference for the context, and sends back an UA message to MN. Subsequent packets are sent using the new preferred locator.

We now give the semantics of messages used in locator switch.

Update Request Message (UR):

Once context is established between two hosts, the locator switch is made through UR Message. Type field in MNS header is set to 64. UR message contains Receiver Context Tag which is the context tag receiver allocated for the context. Also Receiver Nonce is sent which is a 32-bit unsigned integer picked by the initiator for the context and returned in Update Acknowledgement message. The locator associated with UR message is included in options field.

Update Acknowledgement Message (UA):

This message is sent in response to UR message. The Type field in MNS header is set to 65. Through this message, the receiver of UR message indicates to the sender that the locator update is accepted. UA message contains a Receiver Context Tag, and Receiver Nonce.

We now discuss the three basic functions of MNS sub layer.

Link Failure Detection and Recovery Scheme:

In the IETF SHIM6 proposal a failure detection and locator pair exploration mechanism is defined known as Reach ability protocol (REAP) [30]. Although REAP provides a failure detection and recovery mechanism, the process is too slow especially for wireless media where failures are much more frequent. We devise a new failure detection and recovery procedures based primarily on REAP but tweaked to fit the real-time mobility environment. We call it Mobile-REAP or M-REAP. We briefly explain the mechanism here. The detailed explanation is given in chapter 3.

As shown in Figure 2-3, MNS reliability function consists of first detecting failures in the path between MN and CN and then running an exploration procedure through different IP addresses/locators.

Reach ability of an address pair (source/destination address) is verified by a procedure called Forced Bidirectional Detection (FBD). If there is traffic only in one direction and no return traffic, it is assumed that failure has taken place and an exploration procedure kicks in. During the exploration procedure, a host or peer send probe messages using different address pairs in sequence. Probe messages carry information about the state of connectivity between peers. When different address pairs are tried sequentially exponential back-off procedure is employed to avoid signaling storm. When the other end of communication receives a probe message, it starts an exploration process of its own sending probe messages in opposite direction. This is continued until a new working address pair in both directions is found. Communication switches to the new working address pair. This switch remains transparent to upper layers.

Certain parameters are defined and are assigned values. These include Send Timeout, Keep-alive interval, initial probe timeout, number of initial probe messages, and maximum probe timeout.

We now give the semantics for messages used in M-REAP.

Keep-alive Message:

When the end receiving data traffic doesn't have any traffic to send back, it sends a keep-alive message. An interval known

as keep-alive timer is set which defines the time period between each keep-alive message.

The Type field in MNS header is set to 66 for this message. This message contains the Receiver Context Tag.

Probe Message:

These messages are sent to check whether pair of locators (source/destination) work in one direction. When failure takes place, the communicating hosts use probe messages to check reach ability of alternate working locator pair.

Type field in MNS header is set to 67 for this message. Probe messages also contain the Receiver Context Tag.

We describe the procedure with the help of general network scenario of Figure 2-6.

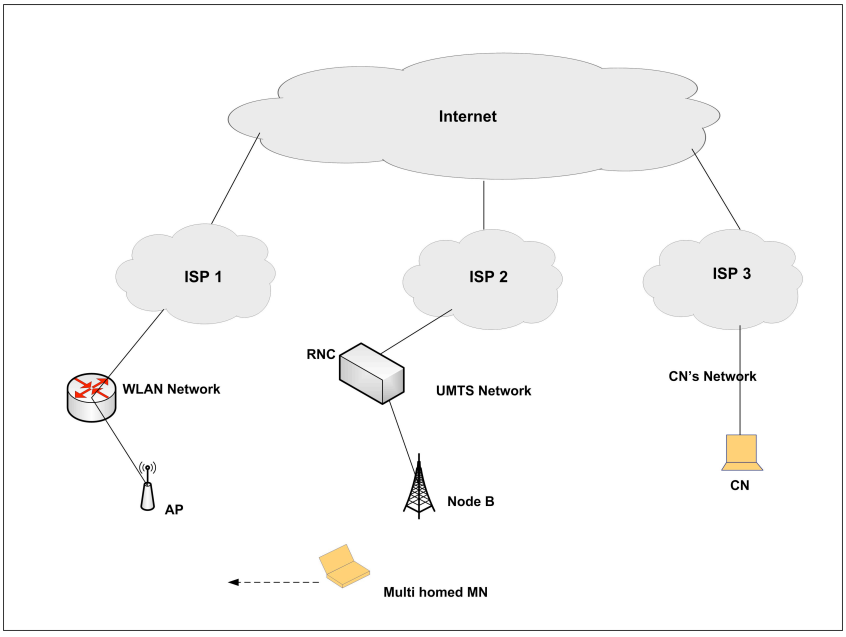

Figure 2-6: MNS-MIP6 General Network Scenario

In the scenario of Figure 2-6 a multi-homed MN is initially communicating with CN through UMTS network. As this MN moves into the coverage area of WLAN, an additional path becomes available between MN and CN. Through use of MNS-MIP6, MIPv6 supported MN equipped with multiple interfaces can switch between different access networks or to share the traffic load among them. Switching could be due to failure of one of the interfaces (reliability). We assume in Figure 2-5 that both UMTS and WLAN interfaces are simultaneously active and only one of them is used to communicate with CN. HoA associated with the communicating interface becomes ULID for the session. A context is established between MN and CN and HoAs/CoAs associated with the second interface become part of MNS locator set. This locator set is sent to CN via SHIM6 signaling. We assume in the Figure that UMTS interface/network is initially used for communication. We next assume that failure occurs and communication through the interface is halted. This failure is detected through M-REAP mechanism and communication is switched to the second interface/network which is WLAN through MNS. This switch remains transparent to layers above IP. Detailed M-REAP procedure is described in chapter 3.

Network Selection:

MNS-MIP6 can be employed in heterogeneous network environment to select a most suitable network among different access networks/interfaces. Our network selection mechanism is explained in detail in chapter 4. Here, we briefly touch on the procedures involved.

A multi interfaced MN may encounter different network conditions on its interfaces as it roams in heterogeneous

environment. When multiple applications are run between MN and CN, the requirements for these applications might be different or the requirements might change with time. For optimal performance, best network should be chosen among the different access networks/interfaces according to the network condition. MNS-MIP6 system provides a way network to be selected depending on suitability of network for particular application.

The network selection function is shown in Figure 2-3. It consists of obtaining parameters from available networks, comparing the network parameters with application requirements which are defined in application profiles. User preference is taken and a decision is made on which network/interface to use for the particular application traffic.

When application is initiated on an MN, communication with CN is through a particular interface. As mentioned earlier, context is established and the initial HoA is chosen as the ULID. All the additional HoAs/CoAs form locator set. Depending on the application requirements and network conditions a different network/interface might be more suited to route the application traffic. Also, if there is already an application being run between MN and CN using the first interface, it might be more optimal to use a second interface for the new application. Decision to distribute the traffic is taken at a Policy Engine running within the MNS-sub layer.

When it comes to choosing an access network for a particular application, in our opinion the most important parameters are bandwidth efficiency, cost, network latency and link quality. The main function of Policy Engine is to obtain network parameters and make a decision on which path traffic is to be

routed through. Policy Engine chooses the network/interface based on parameters values. Once a decision is made to choose a network/interface other than the current one being used, UR message is sent to the peer requesting switch.

As an example, let us consider network architecture of Figure 2-6. A roaming MN scans parameters of bandwidth, SNR and network latency from the two access networks and sends them to the Policy Engine. In addition, cost of using the two networks is also calculated and compared. Based on the comparison, Policy Engine makes a decision on how to distribute the traffic between two access networks. Let us assume that an audio application is running between MN and CN using UMTS network/interface. The MN then decides to also run a video conferencing application with CN. Policy Engine obtains parameters associated with the two networks, compares them, and makes a decision on which network to use for video conferencing. We assume that Policy Engine chooses WLAN network for video conferencing traffic. MNS sub layer is informed of this and it adds MNS header to all video conferencing packets with WLAN interface address as the locator. All video conferencing traffic is now routed through WLAN interface. When an application is to be initiated at CN, the initial source and destination addresses are chosen through existing mechanisms. Policy Engine running on MN obtains network parameters and evaluates them against the application requirements. A decision is accordingly made on whether to use the same ULID pair or to switch the traffic to a different address pair/interface.

Seamless Handover:

An MNS-MIP6 enabled MN can roam through heterogeneous network environment without loss of connectivity. Here we briefly explain the procedures involved. A detailed explanation is given in chapter 5.

The MNS-MIP6 seamless handover procedure involves anticipating handover through layer 2 triggers and taking a decision accordingly. This is shown in Figure 2-3. The layer 2 triggers are similar to the ones used in FMIPv6 mechanism. Each interface is periodically scanned for SNR values. The SNR values are compared with a threshold. When SNR value on an active interface starts approaching the threshold value, a Link_GoingDown trigger is generated. MNS sub layer sends a UR message to peer to request a switch to different network/interface.

When there is movement from coverage area of one access network to another, application sessions experience no disruption. In network scenario of Figure 2-6, we assume that an MNS-MIP6 enabled user has both the interfaces active. MN is initially communicating through the WLAN interface. A context is established between MN and CN. The locator set contains the additional HoA/CoAs. As MN moves, it comes to the edge of coverage area of WLAN. A Link_GoingDown trigger is generated. MNS sub layer on MN request change of locators which in our case is the HoA/CoAs by sending UR to CN. CN replies with the UA message. BU/BA messages are also exchanged between MIPv6 sub layers running on MN, HA and CN to update the binding entry with new CoA. Hence, in MNS-MIPv6 system a handover is anticipated through layer 2 trigger and communication is shifted to a different network/interface.

On-going communication sessions experience very low disruption.

The support for seamless handovers is not provided by MIPv6 or its various enhancements. Hence, through MNS-MIP6 a distinct advantage is gained especially for real-time traffic where session survivability is of critical importance.

Furthermore, in cases where both ends of communication don't support MNS, mobility could still be provided through simple MIPv6 procedures. MNS-MIP6 is thus backward compatible with legacy nodes supporting basic MIPv6. However, in such cases multi-homing benefits of MNS-MIP6 would not be realized.

2.3 Chapter Summary

In this chapter, we presented a unified mobility/multi-homing solution called MNS-MIP6. We recognized some of the drawbacks of existing solutions and addressed them. MN equipped with multiple air interfaces can take full advantage of being multi-homed. An MNS sub layer is introduced within IP layer of a host's protocol stack.

MNS-MIP6 provides a mechanism through which multi-homed MN can switch between different networks/interfaces. The switch can be due to failure of an active interface i.e reliability, to select a network between different networks/interfaces i.e. network selection or due to mobility i.e. handover. Furthermore, the switch remains transparent to layers above IP. Hence, on-going communication sessions are not disrupted.

In the next three chapters, we will describe in depth how our proposed architecture makes communication more reliable,

allows the suitable network selection, and how seamless handover is supported.

Chapter 3

3 Towards Reliable Communication In Multi-homed MIPv6 Networks

One of the main advantages of multi-homing is to make communication more reliable. In mobile multi-homed scenarios where more than one communication path exists between MN and CN, a robust mechanism is needed to support reliability.

When an MN running MIPv6 is multi-homed there exist multiple communication paths between it and CN. In such scenarios, when failure takes place in the currently used path between MN and CN, it should be detected quickly and a switch should be made to a different path without disrupting on-going communication sessions. In current mobile Internet environment and specifically in MIPv6, such a robust mechanism doesn't exist.

In this chapter, we present a mechanism which tackles the issue of reliability in mobile multi-homed Internet environments. Failures in the path between MN and CN are quickly detected and communication is switched to a different working communication path. All this is done without disrupting on-going communication sessions. We use MNS-MIPv6 architecture described in the last chapter and introduce a reliability mechanism which helps to quickly detect failures in the communication path between MN and CN and switch to a different working locator pair. This switch remains transparent to layers above IP. Our reliability mechanism is called Mobile Reach ability protocol (M-REAP).

The performance of M-REAP is analyzed and it is noted that it outperforms those techniques currently used to support reliability in the mobile Internet.

3.1 Introduction/Problem Statement

Reliability is one of the main benefits of multi-homing. In multi-homing scenarios, the term reliability refers to detecting failures in communication path and recovering from them. There is a need to develop a robust reliability mechanism.

This need becomes more profound in mobile multi-homed environments where real-time traffic is involved. We have concluded through our research that, although some efforts have been made to introduce multi-homing in mobile Internet environment, the issue of quickly detecting the failure and recovering from them has not been addressed.

When MN running MIPv6 is equipped with multiple interfaces, it is multi-homed. The interfaces could be belonging to different access technologies. The performance of a particular access technology may vary throughout a single communication session. If signal strength on a particular interface used for communication deteriorates beyond acceptable value, reliability becomes an issue. There needs to be a mechanism defined to quickly detect the failure and switch the traffic from failing communication path/interface to another one.

In present day mobile Internet environment, reliability is tackled mostly at the transport layer. Different transport layer protocols e.g. TCP, UDP, and SCTP use mechanisms to ensure reliable delivery of traffic between end hosts. However, these techniques often suffer from long delays which are undesirable

for real-time traffic [31]. In addition, such measures do not ensure session survivability. Hence there is a strong motivation to develop an IP layer based reliability mechanism which keeps failure detection and recovery transparent from upper layers. This would ensure session survivability. In the TCP/IP protocol suite on which Internet is based, IP layer is mostly exempt from employing any reliability mechanism. For instance, in MIPv6 which is the most popular mobility support protocol on the Internet, failure on the link is detected only through periodic non-reception of Router Advertisement (RA) message from the serving Access Router (AR) [32]. After failure is detected, a new CoA is configured and registered with the HA before it can be used. This can involve delay of many seconds again resulting in sessions being terminated and restarted. The same procedures for failure detection and recovery are followed in the multi-homing extension of MIPv6 presented in Mobility EXTention for IPv6 (MEXT) working group of IETF.

Hence, in multi-homed MIPv6 environments there exists a need to come up with an efficient reliability mechanism to ensure quick detection of failures and recoveries. In this chapter, we present a mechanism within MNS-MIP6 architecture to ensure reliability in multi-homed MIPv6 environment. We analyze the proposal and conclude that it is more robust than existing techniques.

3.2 Related Work

In this section we analyze how MIPv6 and its MEXT multi-homing extension detect failures in the path between MN and CN and recover from them. We also identify the shortcomings. As discussed previously, in MIPv6 scenario failure can occur

anywhere in the path between MN and CN. There can be a failure in the path between MN and HoA, home link of MN can be disconnected from the Internet, a failure can occur in the path between HA and CN, or HA itself can go down.

In MIPv6 and its extensions, there doesn't exist a robust failure detection and recovery mechanism. However, some generic techniques are used to detect path failures. These techniques often result in long delays. One of the techniques to detect failures is through non reception of RA message within a stipulated time from the AR to which MN is attached. As ARs send out RAs after periodic intervals which often span seconds, this technique often results in slow failure detection. Once failure is detected, MN either configures a new CoA or in case of MEXT extension uses a different CoA from the list of multiple CoAs. A BU message is then sent to HA to register the new CoA. The whole process involves long delay and results in communication sessions being disrupted.

One of the more common types of failures in MIPv6 system is when HA serving MN goes down [79]. Such HA failures are detected in MIPv6 only when MN moves and sends BU messages to HA and doesn't receive any BA message back until MAX_BINACK_TIMEOUT. Another way of detecting HA failure is when MN's HoA global address prefix expires and it keeps sending Mobile Prefix Solicitation (MPS) message to HA without receiving Mobile Prefix Acknowledgement (MPA) message back from HA and the MAX_BINACK_TIMEOUT expires.

According to the MIPv6 specification, after MN sends BU to the failed HA, it waits for an INITIAL_BINACK_TIMEOUT which is one second for BA. This timeout period will be doubled for

each subsequent BU sent until MAX_BINACK_TIMEOUT (32 seconds) is reached which indicates that a failure has taken place. As shown in Figure 3-1, this procedure involves sending 6 BU messages.

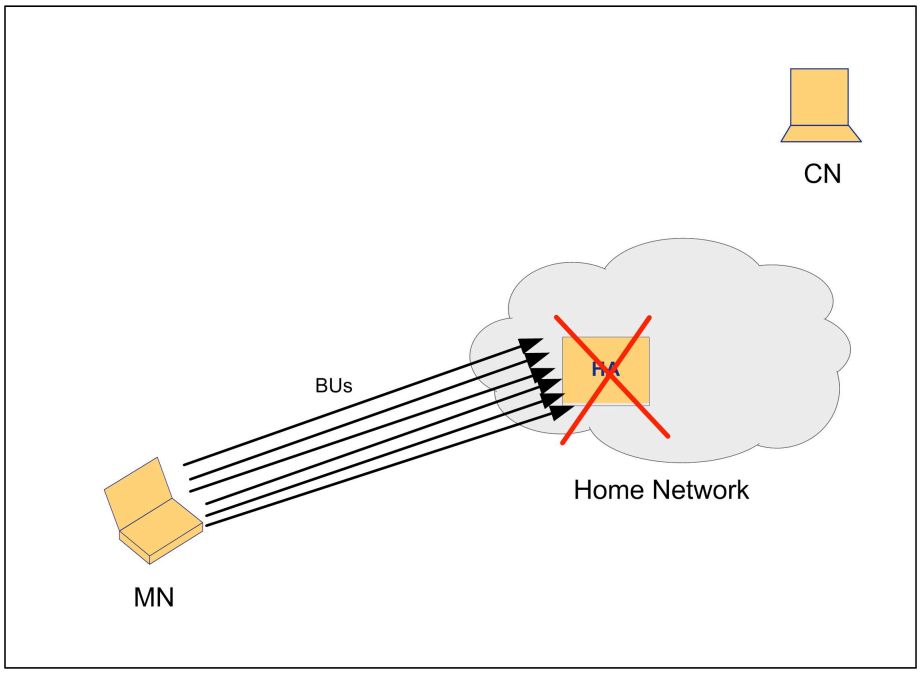

Figure 3-1: MIP6 Failure Detection

Similar to MPS message the INITIAL_SOLICIT_TIMER is set to 3 seconds. Hence, 5 MPS messages will have to be sent by MN to HA before failure could be detected.

Although, some proposals have been presented to address the issue of HA failures in MIPv6 systems [33] [34] [35], there is yet to be a universally adopted approach to quickly detect such failures in MIPv6 and recover from them. Furthermore, although HA failures are more common in MIPv6 systems, failures can occur anywhere along the path between MN and CN. These proposals are focused on HA failures and do not

cover the whole paradigm of failures in MIPv6 systems. We now discuss the main features of these proposals.

One of the more popular proposals is known as Home Agent Redundancy Protocol (HARP) [33]. This proposal allows HA functionality to be shared between one or more peers. Each HARP peer is configured with information about its other HARP peers and forwards any MIPv6 registration message it receives to its peers. Hence, peers share MIPv6 registration information. HARP peers are located in different networks but are within the same routing domain. The peers announce the same MIPv6 home prefix. Depending on routing, MIPv6 messages are routed to either peer. When one of the peers fails, it will not announce the prefix anymore. Upon detecting this failure all the MIPv6 traffic will be routed to a different peer. Although HARP provides a mechanism to switch MIPv6 traffic to a different peer or HA once failure takes place, the actual failure detection mechanism is very slow.

Fault Tolerant Mobile IP [34] is another proposal which aims to address the issue of HA failures in MIPv6. In the mechanism, when MN sends binding request to HA, it is forwarded to another HA which acts as a backup. The secondary HA sends binding acknowledgement to MN's primary HA, which in-turn sends binding acknowledgement to MN. All this is done to ensure binding synchronization between primary and secondary HAs. When failure of primary HA takes place, the secondary HA performs gratuitous ARP to take over the failed HA. In gratuitous ARP process a host informs other hosts of a new MAC address by sending ARP message. If the primary HA becomes alive again, it takes over again through gratuitous ARP. In the proposal HA failure detection is not

tackled. Gratuitous ARP procedure is used to replace a failed HA which is often too slow.

A third HA reliability proposal which has gained significance is Virtual HA Reliability Protocol (VHARP) [35]. Multiple HAs exist on the home link where each HA has a unique link-local address. However, all the HAs have the same global IP address known as “Global HA address”. This global address is resolved to only one of the HAs on the home link. This HA is known as the Active HA. HAs on the home link can be in one of three states. These are Active, Backup, and Inactive. A binding synchronization is kept among the HAs on the home link where at least two HAs hold MN’s binding at a time in their binding caches. Each HA has to multicast RA known as heartbeat message on the home link. Hence, failure is detected when heartbeat message is not sent by Active HA. A mechanism to balance load among the different HAs using VHARP is presented in [78]. In such a case Backup HA takes over and its state changes to Active. Again, failure detection mechanism is based on non-reception of RA (heartbeat messages) which is a slow process.

From our research, we can conclude that although some effort has been made in the area, there is no existing mechanism to quickly detect and recover from path failures in MIPv6 networks [36]. In addition, most of the proposals/techniques deal with HA failures and do not cover the whole paradigm of path failures in MIPv6 networks. In IETF’s multi-homing extension for MIPv6, the same techniques are used to detect and recover from path failures. Hence, a very important benefit of multi-homing i.e. reliability is not addressed properly in IETF draft.

In the next section we introduce robust failure detection and recovery mechanism for mobile multi-homed node running MIPv6. The mechanism is compared with existing MIPv6 failure detection and recovery technique through mathematical analysis and simulation.

3.3 Proposed Architecture

We designed a mechanism within MNS sub layer to support reliability in multi-homed MIPv6 environment. The mechanism is based on Forced Bidirectional Detection (FBD) to detect and recover from path failures. We call the mechanism M-REAP.

When MN running MIPv6 is multi-homed, more than one communication paths exist between itself and CN with which it is communicating. In case failure takes place on the path being used for communication, M-REAP mechanism allows communication to quickly detect the failure and switch to a different path without disrupting on-going sessions.

Normal MIPv6 procedures are followed when multi-homed MN is communicating with CN. After some time, a context is established and the additional HoAs/CoAs are set as locators for the MN. Failure detection and recovery is carried out by FBD which is briefly explained in last chapter. The procedure involves an end host i.e. MN or CN sending keep-alive messages when there is no data traffic to send. Hence, there should be traffic in both directions at all times. Failure is detected when there is traffic in only one direction without any return traffic. Once failure is detected, an exploration procedure kicks in where a host or a peer sends probe messages using different source/destination address combinations. These source/destination addresses are chosen

from the locator set. Different locator combinations are tried sequentially and exponential back-off is employed to avoid signaling storm. Once the other end of communication receives the probe message, it starts exploration procedure of its own where it sends probe messages in opposite direction. This procedure is continued until a new working pair of source/destination locators is found. The communication is then switched to the working pair. There are some similarities between M-REAP and reach ability sub protocol of SHIM6. However, M-REAP is designed to work in mobility environments where HoAs/CoAs are part of locator set for MN. In addition, in BT mode of MIPv6, M-REAP procedure involves sending probe messages via MN's HN. HA forwards the probe messages to MN.

On a given context with a given peer, a node can be in one of three states. These states are operational, exploring, or inboundOk. In operational state the address pair is assumed to be operational. In exploring state the node has observed a problem and has currently not seen any traffic from the peer. In inboundOk state node sees traffic from the peer but peer may not see any traffic from this node and the exploration process needs to continue.

There are certain parameters defined for M-REAP. These are Send Timeout, Keep-alive interval, initial probe timeout, number of initial probe messages, and maximum probe timeout. When node sends any traffic, a timer is started to reflect the need that peer should generate return traffic. If this timer reaches the maximum value of Send Timeout without receiving any traffic from peer, a failure is detected and a full exploration is started. When node has no data traffic to send, it sends keep-alive messages at regular intervals. This

interval is known as keep-alive interval. Interval between initial attempts to send probes is known as initial probe timeout. Maximum probe timeout specifies a limit beyond which probe interval may not grow.

In wireless mobility scenarios where MN is moving fast and frequently, the chances of failures taking place increases manifold. Table 3-1 gives the values of parameters defined in M-REAP for failure detection and recovery.

Send Time Out	500 msec
Keep-alive Interval	150 msec
Initial probe Timeout	200 msec
Number of initial probes	4
Maximum probe Timeout	2.5 sec

Table 3-1: M-REAP Parameter Values

In Figure 3-2 it is shown how M-REAP is used along with MNS-MIPv6 to detect failures and recover from them switching the traffic to a different address pair. Considering a scenario where MN has two HoAs, HoA1 and HoA2. This MN is communicating with CN having IP address IPCN. A context exists between MN and CN. Currently used address pair are (IPCN, HoA1) and (HoA1, IPCN). Assuming failure takes place and HoA1 becomes invalid. An exploration process is started. A new address pair (IPCN, HoA2) is explored and communication is switched to this address pair.

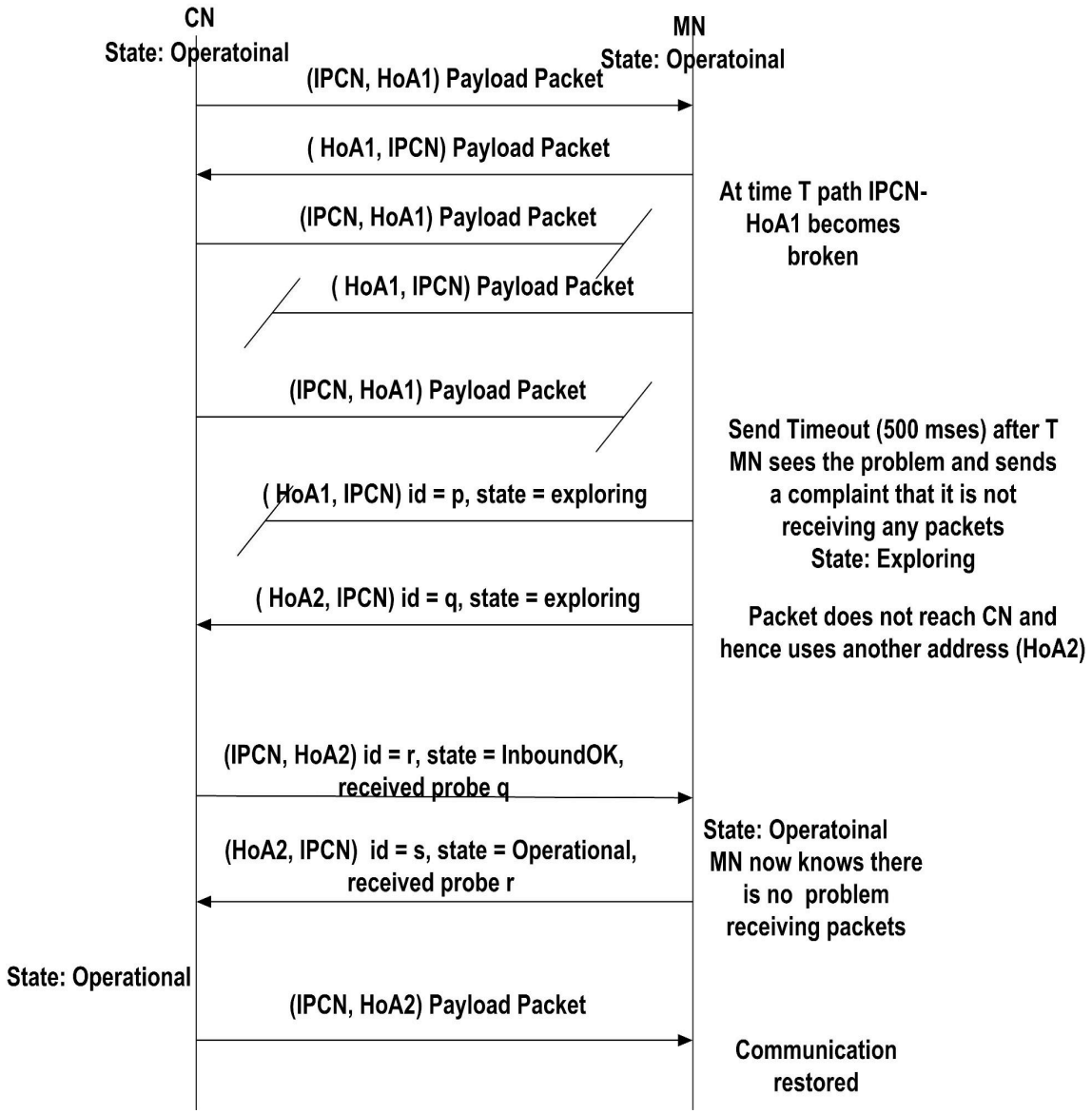

Figure 3-2: MNS-MIPv6 Failure Detection and Recovery Signaling

3.3.1 General Network Scenario

The M-REAP procedure is further explained by considering typical network scenario of Figure 3-3. An MNS-MIP6 supported MN is equipped with a WLAN and UMTS interface. These interfaces are simultaneously active.

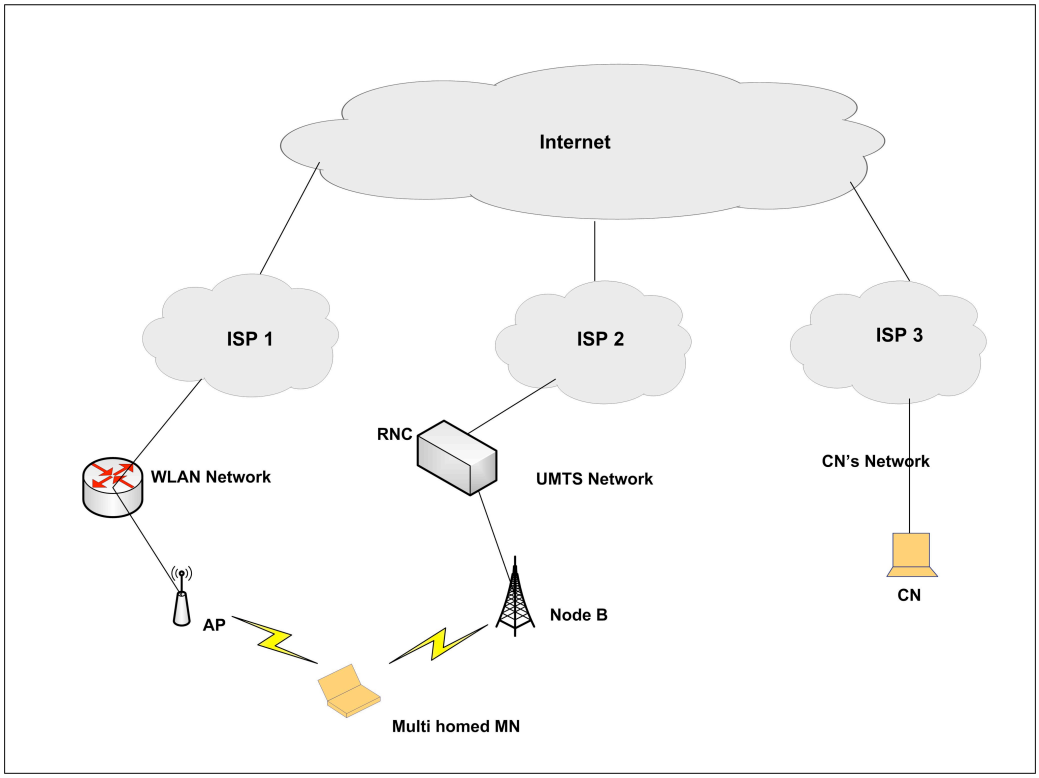

Figure 3-3: M-REAP General Network Scenario

Communication is made more reliable through the use of M-REAP. It is assumed that both WLAN and UMTS interfaces are simultaneously active and only one of them is used for communicating with CN. HoA associated with the communicating interface becomes the ULID for the session. A context is established between MN and CN and HoAs/CoAs associated with the second interface become part of the locator set. This locator set is sent to the CN.

When failure takes place and communication through the first interface is no more possible, M-REAP switches communication to the second interface without disrupting on-going session.

Signaling involved in the process of switching from one interface to another is shown in Figure 3-4. Note here that we show the switching from HoA1 associated with interface 1 to HoA2 associated with interface 2. There is also a possibility of

switching from HoA1 to CoA2 incase the second interface is in a foreign network.

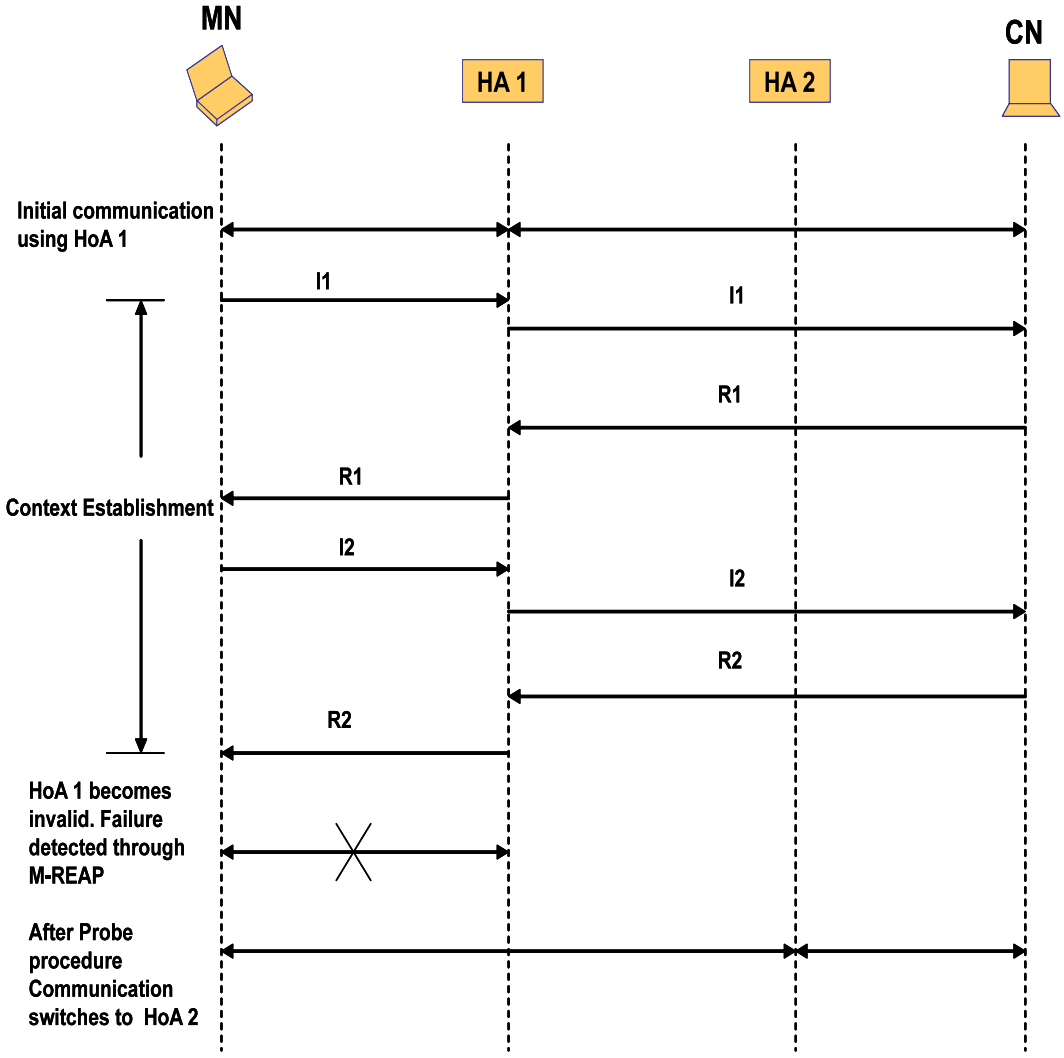

Figure 3-4: MNS-MIP6 Switching due to Reliability

3.3.2 Process Flow

In this section, the process flow for M-REAP mechanism is explained. Considering the network scenario of Figure 3-3, HoA used in initial communication is also MN's ULID. Multiple HoAs/CoAs are provided by MIPv6 sub layer to MNS sub layer. A context is established between MNS layers of MN and CN. During this phase the set of MN's locators which are additional

HoAs/CoAs are sent to CN via either the HA i.e. BT mode, or directly i.e. RO mode.

Traffic between MN and CN follows the principal of FBD. When there is data traffic in one direction, there should be either data traffic or keep-alive messages sent in the other direction. Hence, when one end of communication does not have any data traffic to send, it sends keep-alive messages at regular intervals known as keep-alive intervals. When an end of communication fails to send keep-alive messages in the absence of any data traffic, and the keep-alive timer expires, failure is detected.

When failure is detected, a probe mechanism kicks in. Probe messages are sent using different source/destination address pairs until a working pair in both directions is found. These source/destination address pair are chosen from amongst the locator set. This essentially means that probe messages are sent using different HoAs/CoAs as locators of MN. Communication then switches to the new working address pair. In most cases, communication sessions survive failures as the detection and recovery time is very short. MNS sub layer maps the ULID pair to the working locator pair. A context tag is attached with each packet. Hence, the HoA used as ULID becomes non routable IP address and attains the sole role of identifying the session in TCP layer. In Figure 3-5 the procedural flow chart for MNS-MIP6 failure detection and recovery or M-REAP is given.

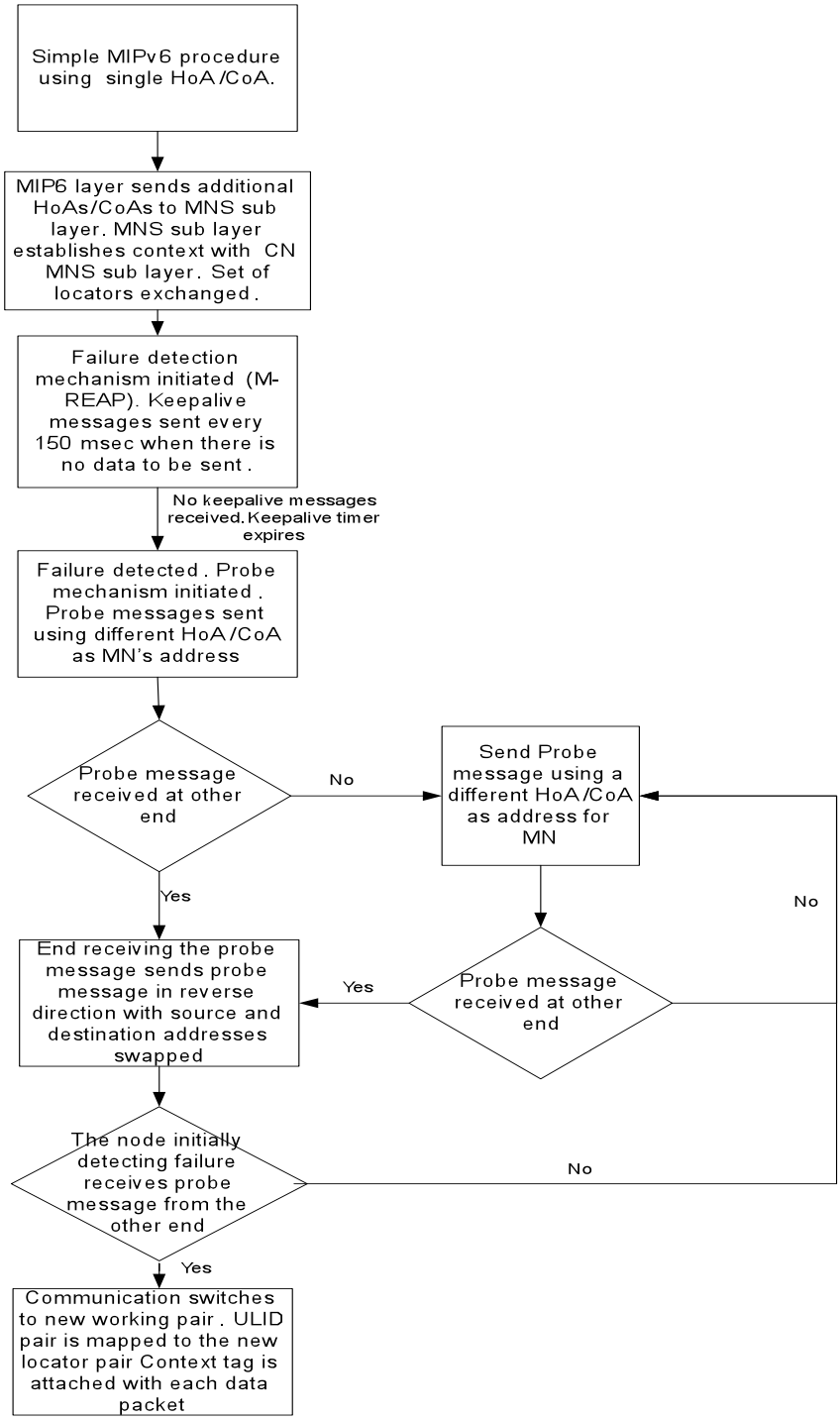

Figure 3-5: M-REAP Procedure Flow Diagram

3.4 Performance Analysis

We evaluate the performance of M-REAP by comparing it with base MIPv6 failure detection and recovery. We first show

through mathematical analysis how M-REAP outperform basic MIPv6 failure detection and recovery procedure. Then we run some simulations to enforce the results of our analysis.

3.4.1 Delay Analysis

In order to analyze the performance of M-REAP, we consider the general network scenario of Figure 3-3. A multi-homed MN is attached to two networks namely WLAN and UMTS. Initially MN is communicating with CN through WLAN network. The MN moves out of the coverage area of WLAN network and into the coverage area of UMTS network. The mobility of MN is considered a special case of failure as the communication has to switch from WLAN to UMTS network. We now analyze the delays associated with failure detection and recovery both for base MIPv6 and M-REAP.

Failure detection and Recovery in MIPv6:

As explained earlier, HA failures are the slowest to recover from in MIPv6 networks. However, there are other failures which are quicker to recover from. The most common one is when MN moves and communication switches from on CoA to another. In MIPv6 terminology, this is known as handover. We analyze the delay associated with handover in MIPv6 networks. The failure detection and recovery procedure consists of Link layer handover and Network layer handover. The Link layer handover consists of probe phase, Authentication phase, and Re-association phase. Network Layer handover includes Router Discovery phase, Duplicate Address Detection (DAD) phase, and Binding Update phase. The total delay is given by:

$$D_{MIP6} = D_{Prob}+D_{Auth}+D_{Ass}+D_{RD}+D_{DAD}+D_{BU/BA} \quad \text{(a)}$$

Here D_{MIP6} is the total MIPv6 failure detection and recovery delay. D_{Prob} is the delay associated with MIPv6 probing mechanism, D_{Auth} and D_{Ass} are the delays associated with authentication and association phases of Link layer handover respectively. D_{RD} is the delay associated with router discovery of Network layer handover, D_{DAD} and $D_{BU/BA}$ are the delays associated with DAD and Binding Update/Binding Acknowledgement phases respectively. The experimental values of these delays as given in [84] are:

$D_{Prob}+D_{Auth}+D_{Ass} \approx 50$ msec

$D_{RD} \approx 100$ msec

$D_{DAD} \approx 1$ sec

$D_{BU/BA} \approx 150$ msec

Putting these values in equation (a) the total delay for MIPv6 switch from one CoA is given by:

$D_{MIP6} \approx 1.3$ sec (b)

Failure Detection and Recovery through M-REAP:

In M-REAP mechanism HA failure is detected when two way traffic between MN and CN via failed HA stops. In the network scenario of Figure 3-3 HoA associated with WLAN network is set as ULID while HoA/CoAs associated with UMTS network form the locator set for MN. When MN moves out of WLAN coverage area and into UMTS coverage area, MN or CN would detect failure when keep-alive messages are not received from the other end and keep-alive timeout expires. Once failure is detected, probe messages are sent using locator which is HoA/CoAs associated with UMTS network. When probe message reaches the other end, a second probe message is

sent in the opposite direction again using the locator. When this probe message reaches the end initiating exploration it is concluded that a new working locator pair are found. All the consequent messages between MN and CN contain MNS header with WLAN HoA as the ULID for MN. Assuming that the time for probe message to travel between MN and CN is D_{probe}. The total delay associated with M-REAP failure detection and recovery can be given by:

$$D_{M\text{-}REAP} = 500msec + ND_{probe} \quad (c)$$

where N is the total number of probe messages.

From our experimentation we have observed the average values of N and D_{probe} to be 6 and 55 msec respectively. Putting these values in equation (b) the total delay in M-REAP failure detection and recovery is given by:

$$D_{M\text{-}REAP} \approx 830 \text{ msec} \quad (d)$$

From (b) and (d), it can be concluded that failure detection and recovery time for M-REAP is smaller than MIPv6. This supports our claim that in MIPv6 there doesn't exist a robust failure detection and recovery scheme. Instead some crude methods are used to determine that failure has taken place and to recover from it. For instance, MN would send BU only if it moves and attempts to register a new CoA with HA. When there is no movement of MN, the HA failures can not be detected as BUs are not sent. The only other way is when the HA global address prefix expires and MN sends an MPS message to HA.

In contrast, M-REAP provides a quick mechanism to detect failures and recover from them. In most cases the whole failure detection and recovery time is within a second. This is suitable for real-time delay sensitive traffic.

3.4.2 Simulation Model

The general network scenario of Figure 3-3 was simulated using OPNET 14. Simulated network model is shown in Figure 3-6. In order to realize the network model, the following modifications had to be incorporated in OPNET 14.

- Design of MNS process model.
- Using OPNET's UMTS module in MN.
- Design of dual interface MN equipped with UMTS and WLAN support.

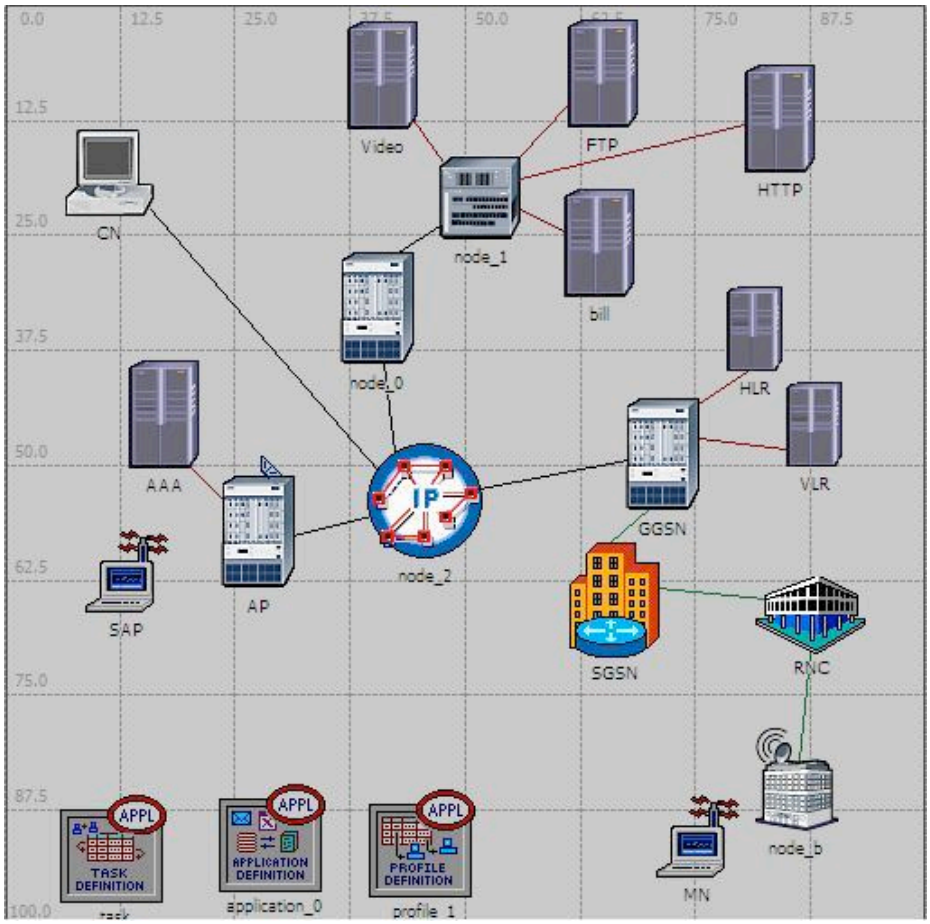

Figure 3-6: MNS-MIP6 Reliability Network Setup

Traffic Model

Using the simulation model of Figure 3-6 a series of simulations runs were conducted under the following assumptions. A maximum of 10,000 simultaneous MNs at any time use the network. The network traffic load was varied from 1,000 to 10,000 users in steps of 1000 users. This was done to assess the effect of loading on traffic delay. For MNS-MIP6 simulations MNS process model was incorporated within the MN model. All users are initially connected to both the networks. However, only WLAN interface is used by all MNs to communicate with CN. HoA associated with UMTS network becomes part of the locator set.

The trajectory of MN is made such that it moves out of WLAN network coverage area when simulation is run for 10 percent of simulation time. M-REAP failure detection and recovery mechanism kicks in and communication switches to UMTS interface. Simulations were also run using REAP for failure detection and recovery by changing the parameter values for keep-alive timer, Send TimeOut, Initial Probe TimeOut, and maximum probe TimeOut. The values of REAP parameters were taken from [30]. Failure is also detected in base MIPv6 and normal handover process is initiated and to switch from CoA associated with WLAN to UMTS CoA. Delays associated with the three mechanisms are compared. Traffic throughput in the three cases is also compared.

Three types of applications are run, FTP, HTTP, and video conferencing.

Simulation was run for 1000 seconds. Results were taken considering two types of application mixes. Application mix refers to the percentage of each type of application exchanged

by MNs when communicating with a CN. These mixes for FTP/HTTP/Videoconferencing were 20/40/40 and 10/30/60. The former to simulate scenario for most users while the latter for extreme heavy load and its effect on system performance.

Throughput and Delay analysis

We obtained results for average disruption time experienced by a single MN in the two mixes when switching from WLAN to UMTS network due to failure. The results of M-REAP, REAP, and MIPv6 in the two mixes are compared in Figures 3-7 and 3-8.

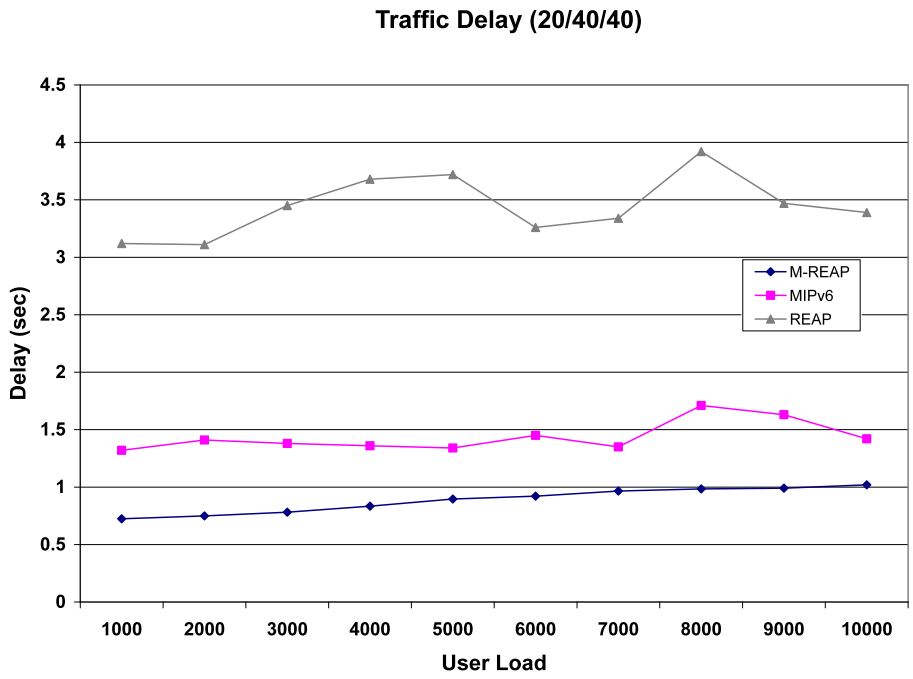

Figure 3-7: Average Delay for Traffic Mix (20/20/40)

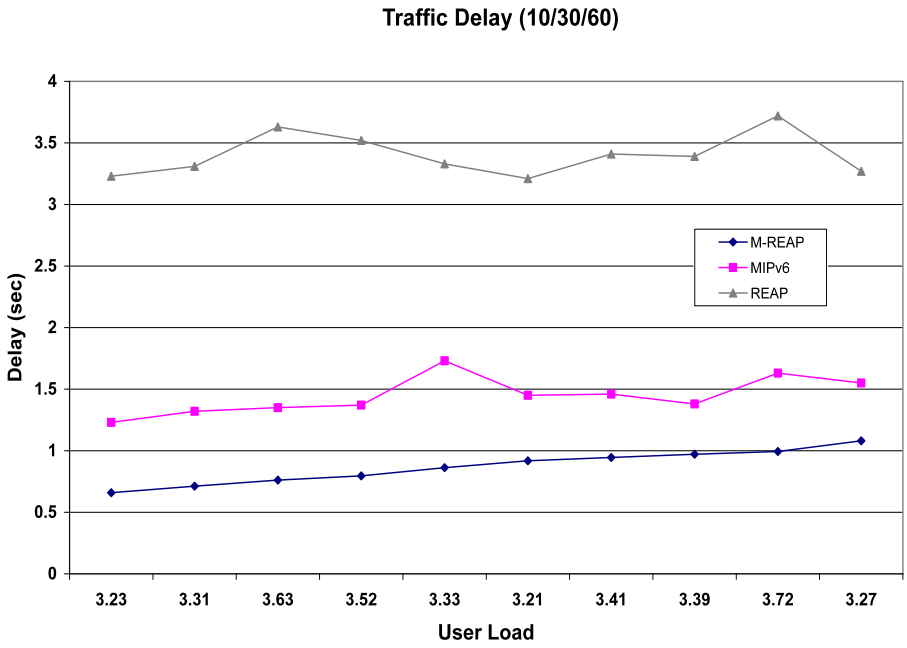

Figure 3-8: Average Delay for Traffic Mix (10/30/60)

From the results it is evident the disruption time for traffic failures is small when using M-REAP as compared to base MIPv6 and REAP. In base MIPv6 and REAP, the disruption time is around 1.5 seconds and 3.5 seconds respectively. In M-REAP the delay is in milliseconds (600-1000msecs).

Next, we compare the traffic throughput. This is the traffic throughput at CN when communicating with MN. We use the same simulation setup. However, we keep the user load at 5000 users and traffic mix of 10/30/60. Simulation is run for 1000 seconds and the failure occurs at 100 seconds mark.

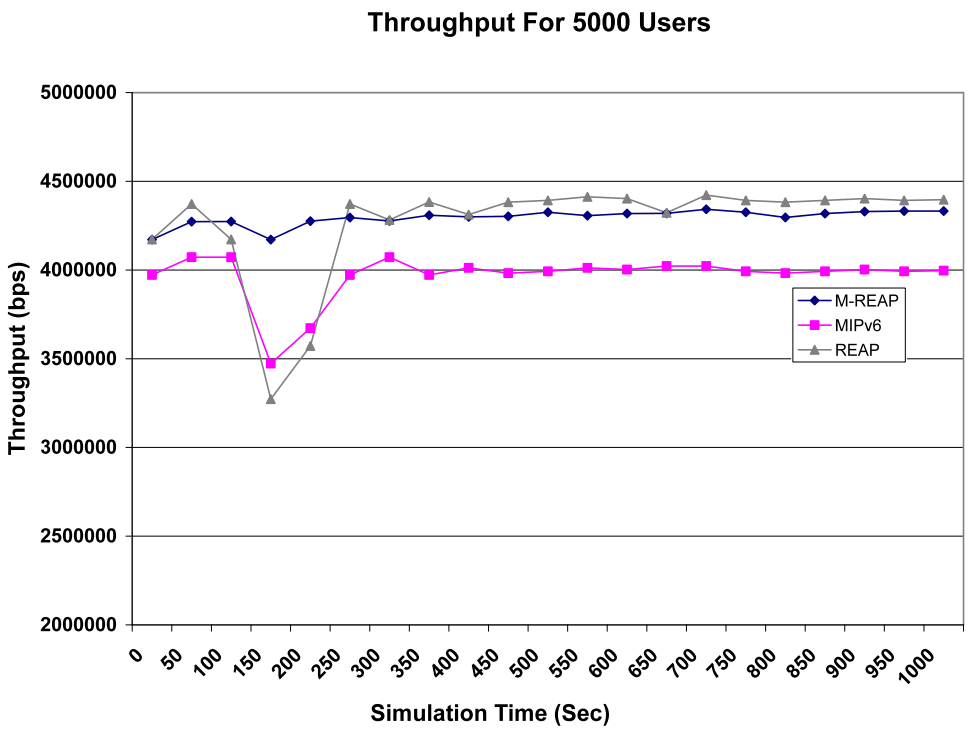

Figure 3-9: Throughput Comparison of M-REAP, REAP and MIPv6

The results show that the glitch experienced in the MIPv6 and REAP cases is much more prominent than in M-REAP. This is again the measure of the amount of disruption experienced by the traffic. Again, the recovery is faster in M-REAP.

It can be concluded here that when M-REAP is used to switch due to failure from WLAN to UMTS network, the total disruption time is in milliseconds. This is significant as most application sessions are tolerant to delays in this range. Hence, for most applications, session continuity is guaranteed. This also guarantees reliable communication. It can also be noted that when load is increased, the effect on traffic delay is minimal. Hence, it is reasonable to assume that MNS-MIP6 systems cope well in heavy load environments. The results also show that when the application mix is changed from light to

heavy traffic, MNS-MIP6 systems performance does not deteriorate.

The results also show that failure has a minimal effect on throughput compared to base MIPv6.

Using the same setup, we ran additional simulations using audio stream having packet size 185 bytes and rate of 30 packets/second. The simulation was run for 1000 seconds. After 10 percent of simulation time, the MN moves from WLAN to UMTS coverage area. The packet loss during switch from WLAN to UMTS networks is plotted in Figure 3-10. The packet loss is plotted for ten trial runs. Again, the result shows how M-REAP outperforms MIPv6 failure detection and recovery.

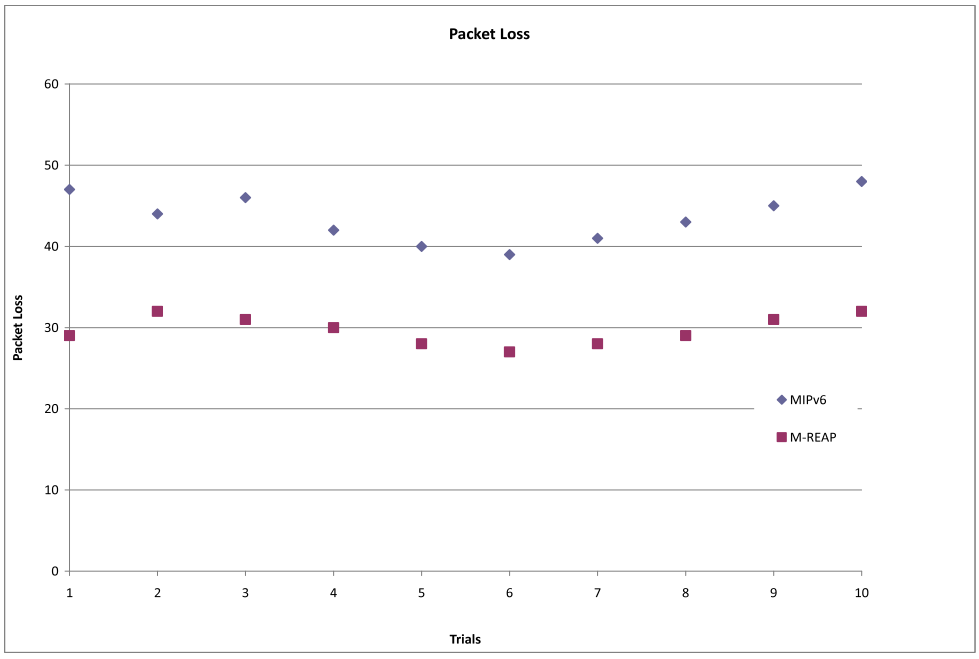

Figure 3-10: Packet Loss Comparison

We also calculated mean recovery time for our MNS-MIP6 system. We used video conferencing traffic and ran 10 trials each time MN moving from WLAN to UMTS network. The recovery times for 10 trials were obtained and are plotted in Figure 3-11.

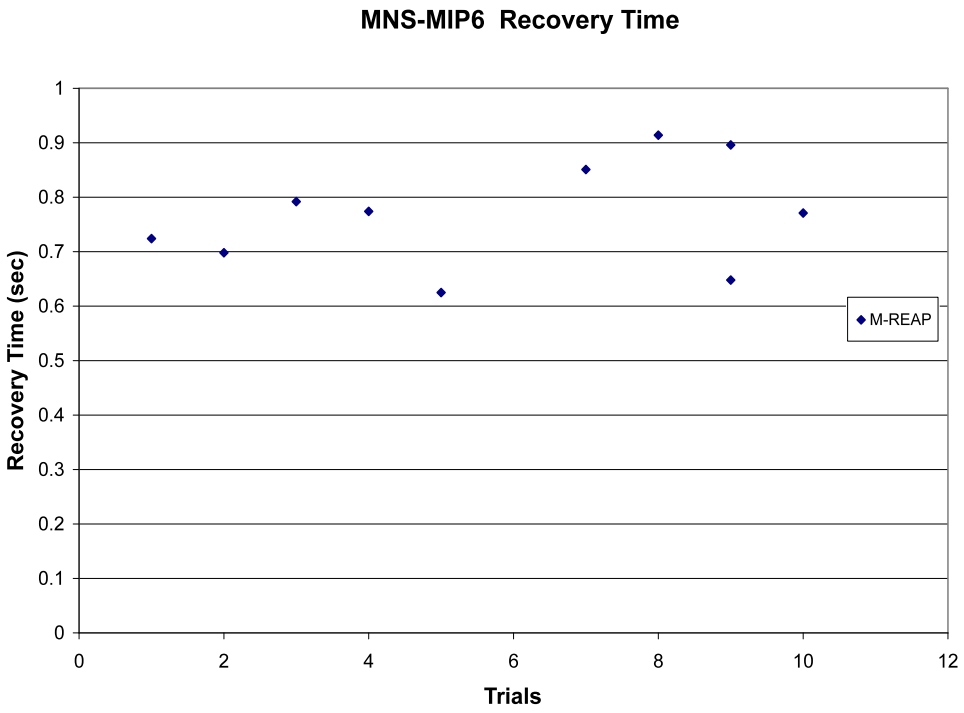

Figure 3-11: MNS-MIP6 Recovery Time

From the result of 10 trials the mean recovery time for MNS-MIP6 system was calculated and comes to be 769 msecs. Again, this supports our claim that in the proposed MNS-MIP6 M-REAP mechanism, the time to recover from a failure is very small. This is ideal for many real-time delay-sensitive applications where session's survivability is a key.

3.5 Chapter Summary

In this chapter we proposed a mechanism to quickly detect failures quickly and recover from them in multi-homed MIPv6

environment. We call the mechanism M-REAP. It is based on IETF's REAP protocol but is tweaked to satisfy the needs of wireless mobile Internet of today. MNS-MIP6 mechanism presented in the previous chapter is used to establish a context with CN with which MN is communicating. When failure takes place in the path between MN and CN, M-REAP quickly detects it and starts an exploration process. Probe messages are sent using different locator pairs. This is done until a working locator pair is found in both the directions. The communication switches to using these locators. All the subsequent messages contain MNS payload extension header.

Failure detection and recovery mechanism is tested and it is shown that when failure takes place, the communication recovers in a very short time through M-REAP. This is especially significant for applications where traffic disruption is of great concern.

Moreover, we showed through simulations and analysis that M-REAP out performs the existing MIPv6 and REAP failure detection and recovery techniques. We showed through simulations that increasing the traffic load has minimal affect on failure detection and recovery time for M-REAP. Delays experienced by traffic remains within tolerable bounds even with large traffic load.

M-REAP does not introduce much complexity to the existing network infrastructure. There is no requirement for introduction of additional entities/nodes. Keep-alive messages are to be sent by each end host when there is no data traffic to send. Hence, with some minor modifications a robust failure detection and recovery mechanism is introduced.

Chapter 4

4 A New Network Selection Mechanism in Multi-homed MIPv6 Enabled MN.

One of the main advantages of multi-homing is that in heterogeneous network environment, it allows a user to choose a particular network for traffic. In this chapter, we build on the MNS-MIP6 idea presented in Chapter 2 and use it to design a mechanism to select a network/interface among different networks/interfaces.

A Policy Engine (PE) is defined which takes certain network parameters, and compares them according to different application profiles. An algorithm is run which takes in user input to choose the best network/interface to use for the particular application. A decision is accordingly taken on the network to use. Through MNS sub layer, the network/interface switch is made when required for optimal performance.

When an interface switch is made, MIPv6 sub layer is informed and BU/BA messages are exchanged with HA/CN to change the binding cache entry.

4.1 Introduction/Problem Statement

In an environment where multiple access networks are present, a multi interfaced MN should be able to use the different networks for optimal performance. There needs to be a mechanism which allows the traffic to be routed to a

network/interface best suited for a particular user/application.

In this chapter we design such a mechanism based on MNS-MIP6 architecture. Various application profiles are defined and based on certain network information and user preference the most suitable network/interface is chosen for a particular application.

There are two basic functions involved in our mechanism. One is to make a decision on which network to use for communication for a particular application and user. The second is to actually switch the traffic to the chosen network/interface. In the proposed mechanism, the initial address pair for communication is chosen through DHCP process. HoA is the source address for MN. A context is established with CN where HoA is the MN's ULID for the context and the additional IPv6 addresses on the interfaces form the locator set. The network parameters are obtained either by introducing an Information Server (IS) or by network broadcasting. In the case of an IS, a query is sent by the MN. In response to the query, IS sends network parameters. In the second case, network periodically broadcasts the parameters. PE then compares these parameters and based on the application profile and user preference, it makes a decision on which network to use for communication. This is conveyed to MNS sub layer in MN. If the network chosen is different from the current network, a switch is made to the associated locator/IP address. A UR message with Change_loc_pref flag set is sent to the CN. CN replies with a UA message. A BU/BA message is sent from MN to HA/CN to update binding cache entry with new CoA which is the new locator used for routing.

The locator set can be updated when there is change in any of the addresses configured on interfaces.

In our network selection mechanism, the decision to choose a particular network for applications is taken by considering four parameters. These are network latency, available bandwidth, cost and link quality. IS is located in each network and provides the PE with these three parameters. The comparison is made and according to the application requirements and user preference optimal network/interface is chosen for communication.

In the research community, there have been some proposals which address the issue of network selection in heterogeneous network environment. In these proposals switch is made from one interface/network to another based on a particular set of criteria e.g. mobility, user preference, application preference or a combination. However, all the proposals introduce major changes to the existing Internet infrastructure. Decision making is not distinctively separated from the switching mechanism. Some of the proposals don't support session survivability. When switch is made from one interface/network to another, on-going communication sessions have to be broken and re-started. This results in some unnecessary disruption to real-time traffic flow.

In this chapter we introduce a mechanism which allows a interface/network switch to take place without disrupting on-going communication sessions. The switch is transparent to upper layers. There is no complexity introduced in Internet infrastructure. A system is developed which separates decision making from interface switching. This allows one process to be changed without affecting the other. i.e. a different decision

making algorithms can be employed with the same switching mechanism and vice versa. In addition, the mechanism enables smooth interface/network switch without disrupting on-going communication sessions.

4.2 Related Work

There have been some proposals which address the issue to interface/network switch in mobile/multi-homed environment. In this section, we describe some of the most recent/advanced mechanisms that have been developed and tested.

a) Seamless Connectivity Based on Predictions (SCBP)

A mechanism to facilitate ubiquitous application users to migrate from one network to another without user interaction is given in [37]. It involves introducing Ubi-system in the network. Ubi-system consists of ubi-subsystems and soft switches in each network. Ubi-subsystem registers any new user and provides him/her with information server address based on its contexts. When user is registered, its movements are tracked by soft switch. Soft switch consists of a mov-monitor and SCBP predictor, and roam facilitator modules.

Prediction algorithm is run in predictor module. Predictor module gets the user coordinates from mov-monitor module and communicates with roam facilitator module for smooth migration. Prediction algorithm considers current movement patterns and past movement history statistics to make predictions. A user profile data structure is formed which contains information such as user's interests, his/her qualification, age, name, history of places last visited etc. Based on past history for specific applications (healthcare system, traffic system etc) and categories (Engineers, Doctors

etc), a human movement pattern is estimated in SCBP. Migration is made based on prediction algorithm. Mov-monitor module is run to give statistics information and current user movement pattern respectively to generate predictions. Once a switch predicts migration of a user to a foreign network, it contacts the foreign networks switch and sends it the user profile. All information provided by previous switch is used by current switch to provide smooth migration to the migrating user.

Although SCBP provides a criterion to switch from one network to another, it is essentially a mobility management mechanism. Decision to handovers from one network to another is made based on user statistics and movement monitoring. Switching takes place only when there is movement of MN. Application requirements are not considered. In multi-homed environment where more than one networks/interfaces are available at a given instance, applications should be able to choose the network/interface best suited-even when there is no movement. This issue is not addressed by SCBP.

b) Active Application Oriented (AAO) Vertical Handover in Next-Generation Wireless Networks

A mechanism for vertical handovers based on application requirements is presented in [38]. An entity known as Location Service Server (LSS) is introduced. LSS provides MN with neighbouring networks information such as coverage area, bandwidth, latency etc. There are two modes of operation. In the active mode MN can request LSS for neighbouring networks information when it needs to. In the passive mode, BS periodically requests neighbouring networks information from LSS and forwards it to the MNs in its coverage area.

MN evaluates the neighbouring networks information compares it with its currently attached network and makes a decision of whether to switch to a different network for the particular application. The network parameters considered are bandwidth, latency and packet error rate. For each network parameter, an application defines its upper and lower bounds to indicate the maximum and minimum requirements respectively. If the currently attached network satisfies the requirements, no switch is made. However, if the requirements are not satisfied by currently attached network, the most suitable network is selected.

AAO mechanism takes into account application requirements in making the decision to switch to a different network. It assumes that only one application runs on MN. It doesn't tackle situations when multiple applications are running simultaneously. The mechanism also doesn't take into account any user preference.

c) A Context-aware Handover Management for Seamless Connectivity in Ubiquitous Computing Environment

An intelligent context-aware handover management mechanism is introduced in [39]. There are four types of profiles defined, application profile which gives some important application requirements, user profile which gives specific user requirements, work profile which gives information related to application of work, and abstracted profile which is the set of requirements based on work profile. An application profile consists of many service modes of an application.

A user profile consists of using time, which is the average time spent for a given work process completion in previous work process, transferred data volume which is the average amount

of transferred data in the same process, and priority for any specific application in each work.

From application and user profile, and network parameters, a work profile is created. Work is a group of applications in given situations, Work profile gives information related to the application of work.

Abstracted profile is generated from work profile. It is a set of requirements for a specific work profile. Abstracted profile is used to determine whether switch is to be made to a different interface/network.

In context-aware handover proposal, every time there is a handover, application sessions have to be broken. Thus, the interface switch is not transparent to layers above IP. Also, the proposal does not define a mechanism on how network/interface information is sent to the decision manager and how this information is obtained from different networks.

d) Ubique

An interface selection mechanism known as ubique is presented in [40]. Different factors such as interface capabilities, access network characteristics, application requirements and user preferences are analyzed to make a decision on a particular network/interface to use for a particular application. All the necessary information is specified in profiles.

The middleware is composed of a profile manager, profile databases, and selection decision algorithm. The profile manager analyzes all the information received and takes a decision on whether selection decision algorithm is to be invoked. Profile database module stores all the profiles. The

selection decision algorithm decides which interface to use based on internal and external environment. Four types of profiles are defined and stored in profile data base. These are preference and resources profile, flow description profile, network interface profile, and access network profile. Profile data base assists the selection decision algorithm to make a decision.

Ubique is an adaptive interface selection mechanism. The decision to switch from one interface to another is taken by considering external as well as internal factors. However, on-going application sessions are broken during interface switch. This can result in great amount of communication disruption.

4.3 Proposed Architecture

In this section we explain in detail our proposed network selection architecture.

When an application is run between MIPv6 supported multi interfaced MN and CN, one of the interfaces is used. When the MN is away from its HN, HoA is mapped to the CoA which is the IPv6 address configured on the interface used for communication. Additional IPv6 addresses are configured on other interfaces. After some time context can be established between MN and CN. ULID for MN is the HoA while the locator set consists of these additional addresses. When an interface becomes active, the IPv6 address configured on it is added to the locator set by sending a UR message to CN with Add_loc flag set.

While the initial communication is through a certain interface/access network, we propose a mechanism which enables application traffic to be routed through the network

best suited for it. For this purpose a Policy Engine (PE) is defined. Main function of this PE is to make a decision on which network to use based on application profile and user preference. Actual switching takes place through MNS signaling. The interface/network switch is kept transparent from upper layers. Hence, already established communication sessions are not broken during the switch.

There are four network parameters we use for decision making. These are available bandwidth, latency, cost and link quality. The parameters are sent to Policy Engine in one of two ways. They can either be sent by running a query/response process with Information server or by network broadcasting them after periodic intervals. In the former case, IS exist in each network and are populated with relevant network information. We also define application profiles. The minimum required bandwidth and maximum tolerable latency values for a particular application are defined in the profile. The available bandwidth and latency values obtained from different networks are then compared to the application profile values. Those network/networks are chosen whose available bandwidth is greater than minimum required bandwidth for application and whose latency is less than maximum tolerable latency. In addition, the link quality available on the interfaces is also checked against a set threshold. If SNR on a particular interface is below the threshold, the interface is not selected.

From the criteria explained, more than one network maybe suitable. User preference is now added to the mix. User can set the preference to either low cost or low latency. If low cost is set as the preference, the suitable networks are again compared and the one which has lowest cost is chosen. Similarly, if low latency is the user's preference, the latency

values from networks are compared and that with least value is chosen. This is sent to the MNS sub layer. If the network chosen is different from the one being used, a switch is made through UR/UA message exchange. This way, switch can be made to a network most suitable for a particular application without disrupting on-going sessions.

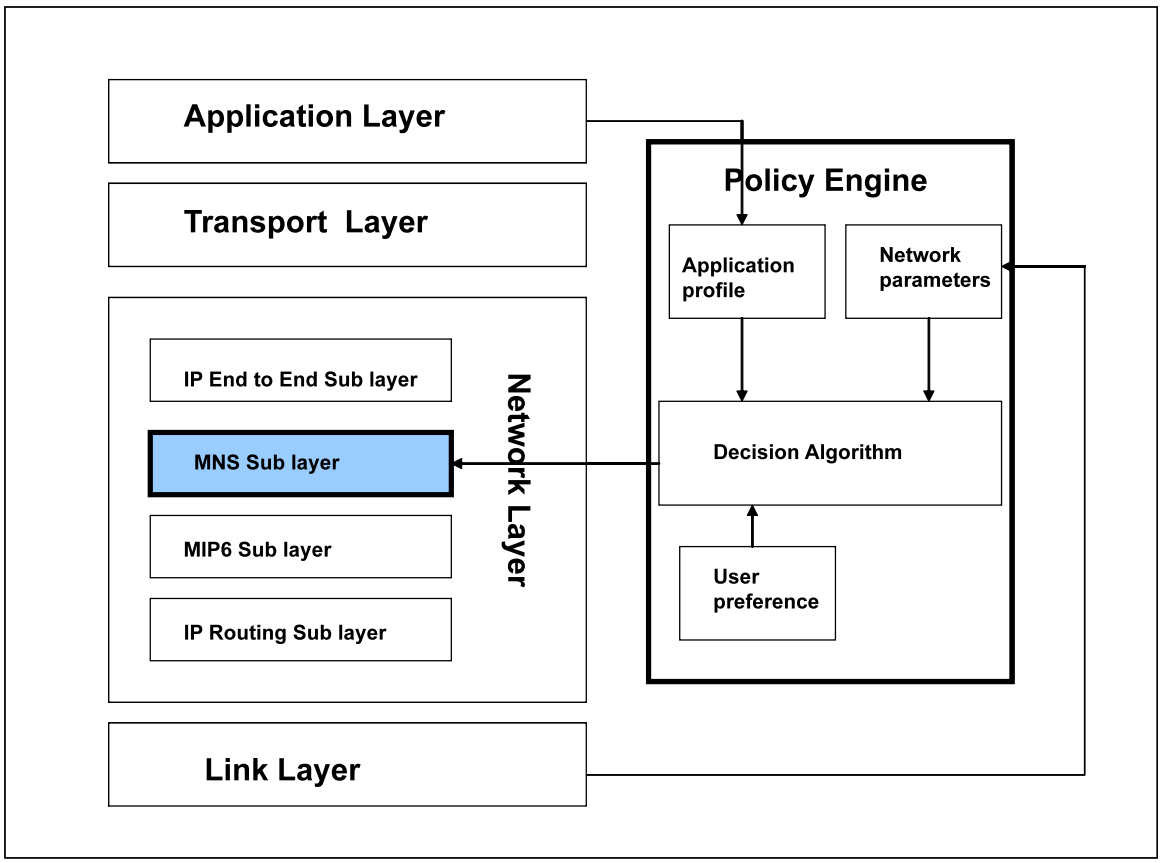

Figure 4-1: MNS-MIP6 Network Selection Architecture

4.3.1 Building Blocks

MNS-MIP6 based network selection proposal has the following building blocks:

a) Policy Engine

Policy engine defines the criteria for selecting a particular network for communication. When application is running between multi interfaced MN and CN and a context is established between the two, Policy Engine is informed. Parameters of available bandwidth, latency, cost and SNR are taken as inputs from each network. Policy Engine contains the profiles for various applications such as audio, video, ftp, and http etc. Example of application profiles is given in Table 4-1. These profiles are based on bandwidth requirement and latency for a particular application. Minimum acceptable value of bandwidth and maximum tolerable value of latency are defined for each type of application. e.g. from Table 4-1, minimum bandwidth required for video streaming traffic is 50kbps and the maximum tolerable latency is 150msec. The parameters of available bandwidth and latency obtained from different networks are compared with application requirements. The networks whose parameters satisfy the application requirements are chosen for next step. In addition, the SNR from different networks is compared with a threshold and only those networks whose SNR values are more than threshold are chosen for the next step.

There maybe more than one network which satisfies this criteria. If such a case exists, user preference is considered. User can prefer between low network cost and low latency. When low cost is desired by the user, the cost from the suitable networks is compared. Network giving the lowest cost is chosen. Similarly, when low latency is user's preferred choice, latencies from the suitable networks are compared and network giving minimum latency is chosen.

---

b) Decision.

A particular network for communication is chosen by running decision algorithm. As described earlier, profiles are defined for different types of applications. These profiles are based on bandwidth and latency requirements for a particular application. The decision algorithm compares network parameter values with those for the application. The network or networks which have available bandwidth greater than the minimum required bandwidth for application, latency lower than the maximum tolerable latency for application and SNR above the minimum set threshold are chosen.

When more than one network satisfies the above mentioned criteria, decision algorithm brings user preference into consideration. User can set the preference either to low cost or low latency. Accordingly, the respective network parameters are compared and the most suitable network is chosen. Figure 4-2 gives the pseudo code for decision.

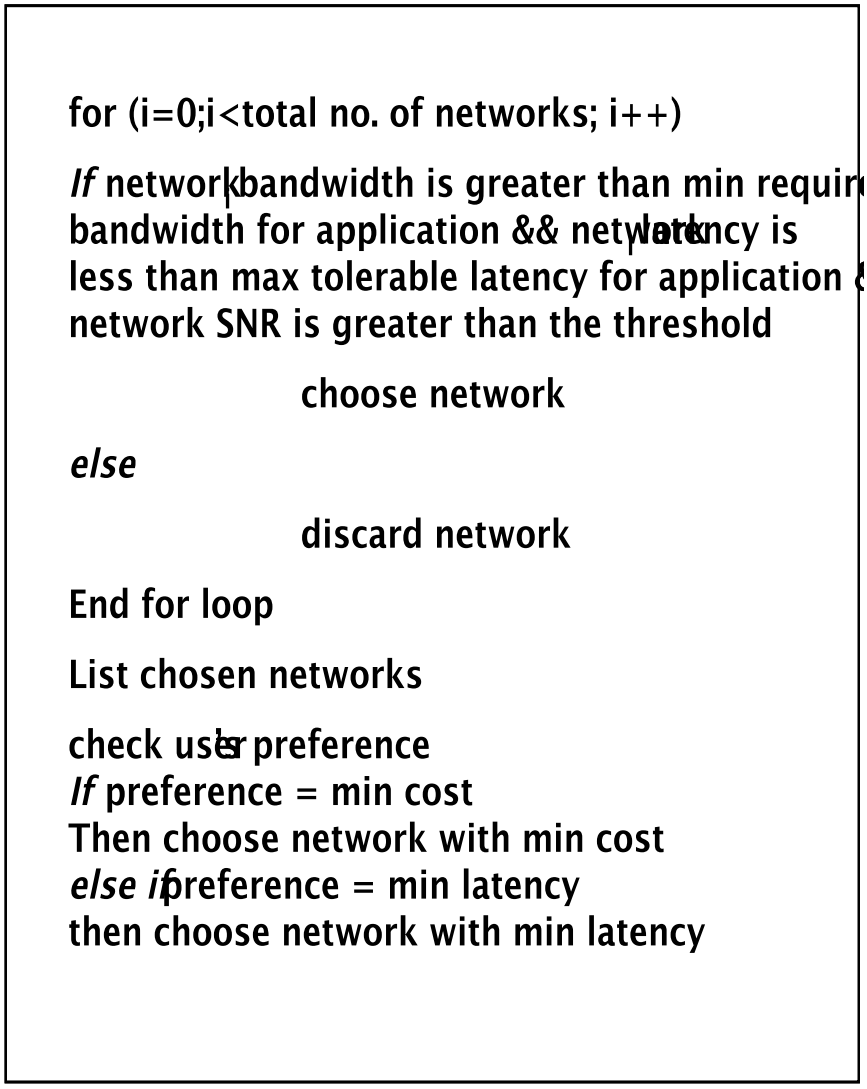

Figure 4-2: Pseudo code for Decision

c) Network parameters

In our proposed architecture network parameters given significance are available bandwidth, latency, cost and SNR. We feel that these are four very important parameters that make our network selection mechanism robust and adaptive. These parameters are sent to the Policy Engine in one of two ways. Policy Engine can request the parameters from Information Servers located in the networks. Networks can also broadcast the parameters periodically. The network

parameters are compared and, based on the application requirements and user preference, Policy Engine makes a decision on which network to use.

d) Application profile

Application profiles are defined based on minimum required bandwidth and maximum tolerable latency. Different applications have different bandwidth and latency requirements. These requirements are compared with available bandwidth and latency values obtained from different networks. The networks which satisfy the application requirements are considered suitable and are further scrutinized through user preference. A typical application profile for video streaming and voice conversation are given in Table 4-1.

	Voice Conversation	**Video Streaming**
$Bandwidth_{min}$	9.6kbps	50kbps
$Latency_{max}$	150msec	150msec

Table 4-1: MNS-MIP6 Network Selection Application Profile

e) User preference

In addition to application profiles, user preference is used to select a particular network for communication. A user can prefer either a network with low cost or low latency. The reason for making a choice between these two parameters is that they are disjoint i.e. networks with low cost have higher latency values and vice versa.

User preference is hence a tie breaker between different networks which satisfy the application requirements. For

example, there maybe more than one networks which satisfy a particular application requirement. Depending on user preference, the network with least cost or least latency is chosen.

f) Link Quality

Link quality is measured through periodically obtaining SNR from each interface. The SNR values from all interfaces are compared with a minimal threshold. The minimal threshold is taken from FMIPv6 scanning mechanism [44]. Only the networks whose SNR values are above the minimum threshold qualify to be selected.

Link quality is of great importance when considering network selection. It is measured through scanning SNR from different interfaces belonging to distinct networks. In mobile Internet environment, SNR value on a specific interface may vary considerably from time to time. Hence, scanning should be done periodically where the scanning time interval is small. In our proposed mechanism we use standard FMIPv6 scanning interval [44].

Periodic measure of link quality makes our network selection mechanism adaptive to changing network conditions.

f) IS Discovery

Decision to choose a particular network for application traffic is taken considering the four network parameters. As explained earlier, there are two ways in which these network parameters are retrieved by MN. They can either be retrieved through sending a query to IS or through network broadcasting.

In the former case, IS IP address is sent by AAA server during boot strapping phase. When MN sends an authorization request message to AAA server, AAA server responds with a message containing among other things IS IP address. When application is run between MN and CN, MN sends a network parameter request message to IS. IS responds with a message containing the parameters. IS is populated with corresponding network parameters.

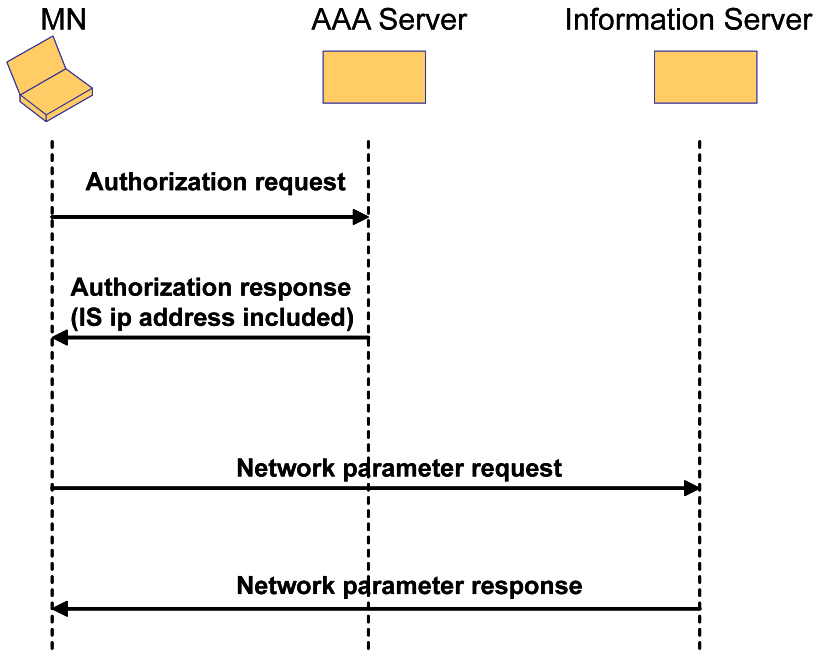

Figure 4-3: IS Discovery

Networks can also broadcast their parameters periodically. A time interval is set for periodic broadcasts. PE obtains the parameters and compares them to application profile requirements.

4.3.2 Typical Network Scenario

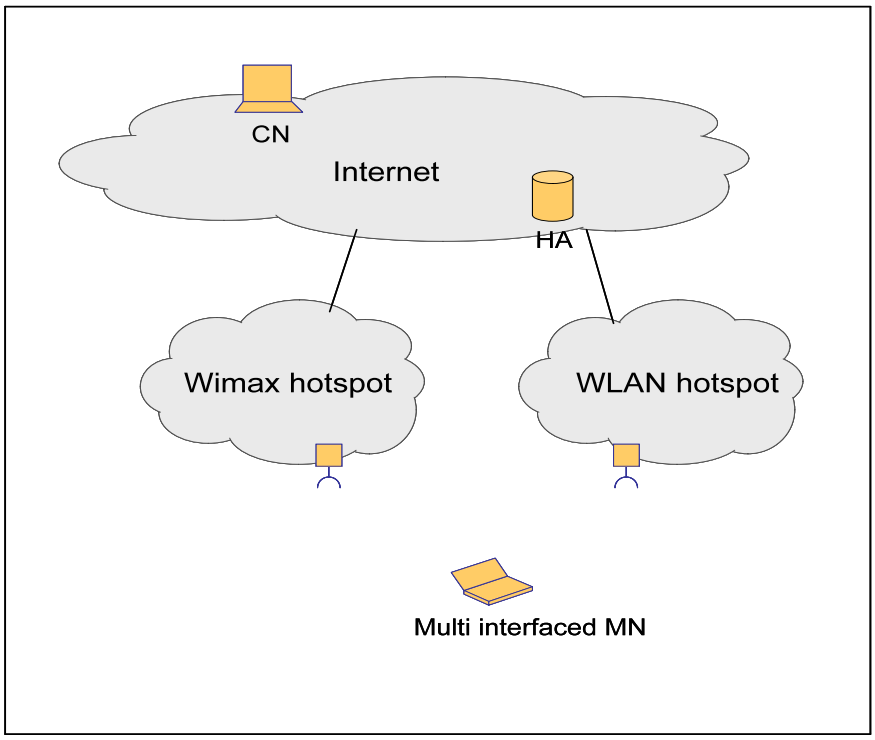

Figure 4-4: MNS-MIP6 Network Selection Scenario

The procedure is further explained by considering a typical network scenario. MN equipped with multiple active air interfaces is communicating with CN. All the application traffic is routed through a single interface. Context is established between MN and CN. The locator set contains all the IPv6 addresses on interfaces. Policy Engine is activated to make a decision on which access network/interface is best for the running application. Policy Engine makes a decision based on application profile and user preference.

4.3.3 Signaling

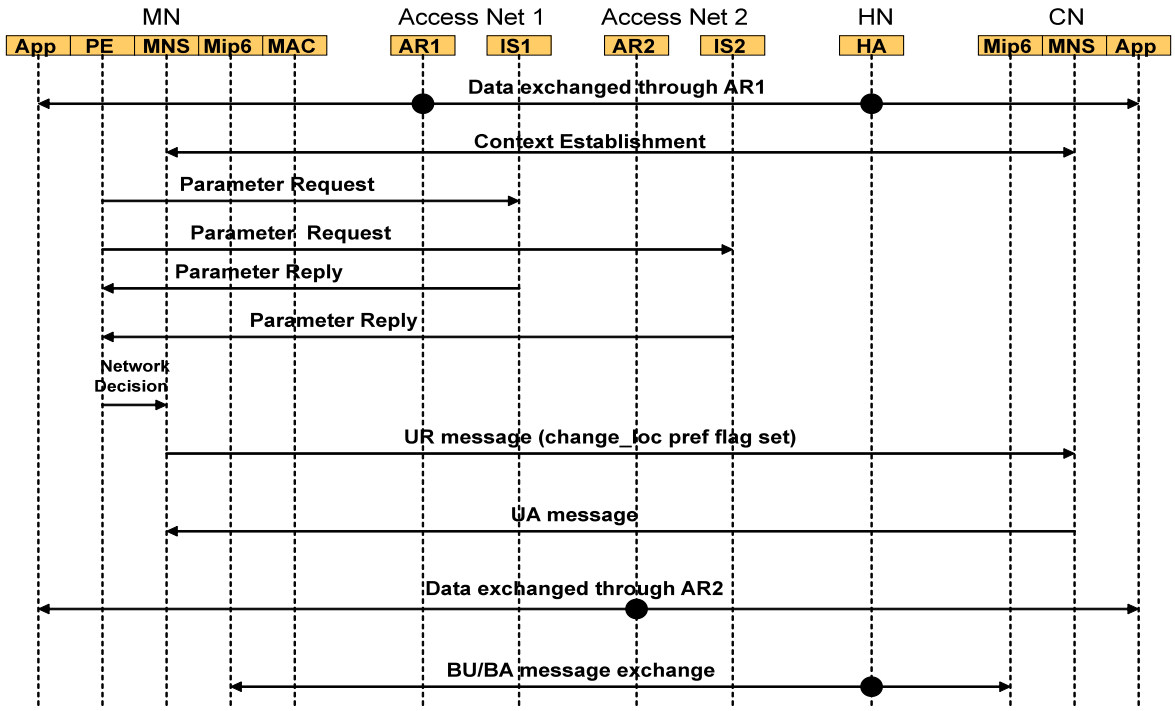

Figure 4-5: MNS-MIP6 Network Selection Signaling

Figure 4-5 shows the signaling involved in MNS-MIP6 network selection mechanism. When application is run between multi interfaced MN and CN a particular network/ interface is used to route the traffic. It is assumed that all the remaining interfaces on MN are also active. These additional addresses form locator set for the context. When context is established, MN requests parameters from all the ISs of different networks. Each IS sends back parameters of the corresponding network. MN can also obtain the parameters through network broadcasts.

Policy Engine compares these parameters based on application requirements and user preference and chooses the most

suitable network. This decision is conveyed to MNS sub layer. In case the chosen network is different from the one being used, MNS sub layer sends a UR message to CN with Change_loc pref flag set. CN replies with a UA message. MNS header is appended to all the subsequent packets. Hence, switch is made to the new network/interface. MN also sends a BU message to HA and CN to update the binding cache entry. HA and CN reply with BA message.

4.4 Simulation Analysis

We run some simulations to analyze our proposed network selection mechanism.

4.4.1 Simulation Setup

The proposed network selection mechanism was analyzed using OPNET 14. The simulation setup is shown in Figure 4-6. MN with three network interfaces is created using OPNET's custom node creation facility. This MN has a WiMAX 802.16e, a WLAN 802.11b and a UMTS interface. CN is connected to the Internet through a 100Mbps Ethernet connection. WiMAX is MN's home domain where HA is located. Analysis is carried out running three traffic types between MN and CN: video conferencing, voice, and online gaming. A Policy Engine, described in the previous section, is defined in MN to make a decision on which network/interface to use for particular traffic. For simulation purposes, voice application is hardwired in Policy Engine to be always routed through the UMTS network. The MNS process model is incorporated in OPNET within MN's IP layer as a child process. We use the application profiles defined in [38]. For each type of application traffic, there is a minimum required bandwidth and maximum

tolerable latency. User preferences or priorities are set as follows:

For video conferencing application, low cost is given a high priority, for online gaming low latency, and voice traffic is programmed to always be routed through UMTS interface. These preferences are set after investigating requirements for each type of traffic.

Parameters of available bandwidth, latency, and cost are periodically read from each network while SNR on each interface is also checked. The checking interval is set as 50msec. These parameters are periodically made available to the PE.

MN communicates with CN by first running each application individually and then all at once. Traffic routed through each interface is plotted. Simulations are run for 300 seconds each.

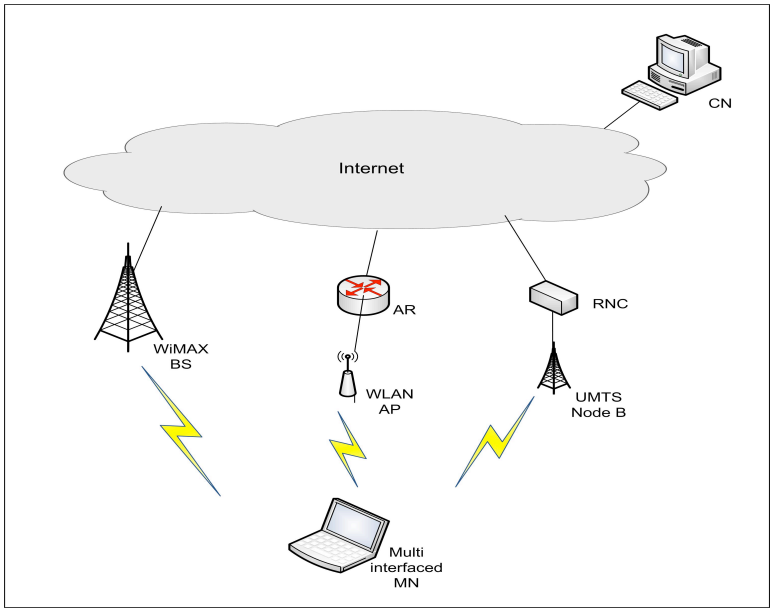

Figure 4-6: MNS-MIP6 bases Network Selection Simulation Setup

Figures 4-7, 4-8, and 4-9 give the plots of traffic throughput on each interface when video conferencing, voice, and online gaming applications are run respectively. These throughputs are measure of traffic volume on each of the interfaces. In each of the plots a single traffic is transmitted at a time. Three distinct color plots show the traffic on each interface. We observe that on each of the simulations, traffic is initially routed through the WiMAX interface. This is because when MN starts communicating with CN, its HoA/CoA is in the WiMAX domain. Figure 4-7 gives the measure of throughput on each interface when video conferencing application is run from MN to CN.

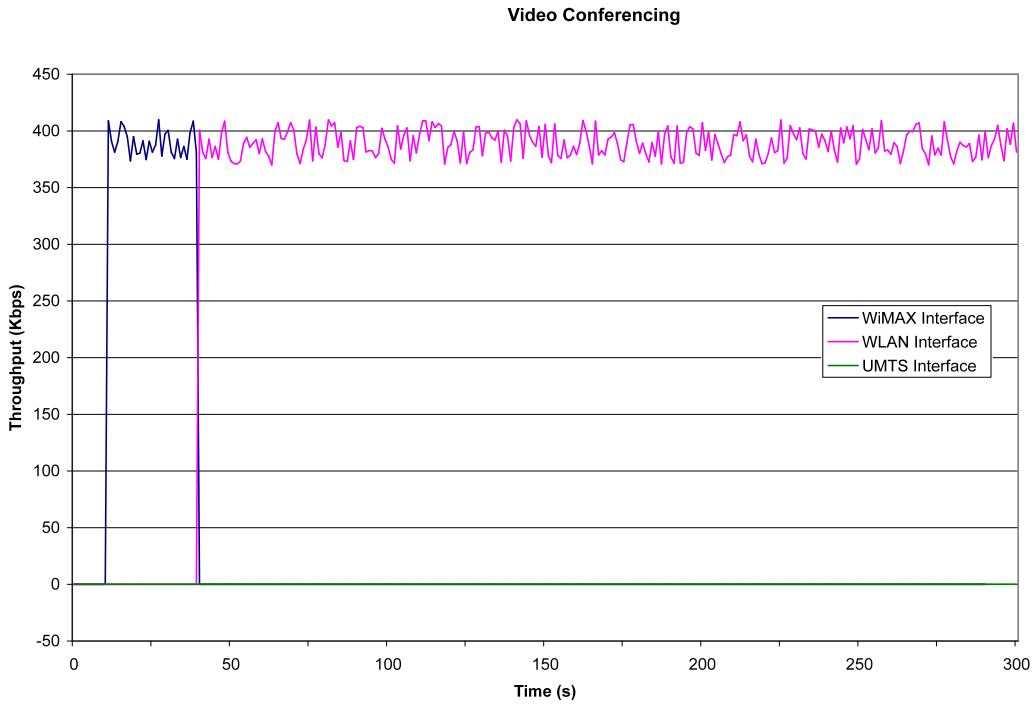

Figure 4-7: Video Conferencing Traffic

From the plot, it can be seen that initial communication is through the WiMAX interface as shown by the blue curve. However, after some time a switch takes place and traffic starts to go through a different interface i.e. WLAN interface

(pink curve). In our PE, we had set preference for video conferencing to be low cost. When all the other application requirements are satisfied, it is less costly to run traffic on WLAN interface than on WiMAX interface. Figure 4-7 confirms this as for video conferencing traffic when parameters from the three networks are compared, the network with low cost is chosen i.e. WLAN network.

Figure 4-8 gives the measure of throughput on each interface when voice application is run from MN to CN.

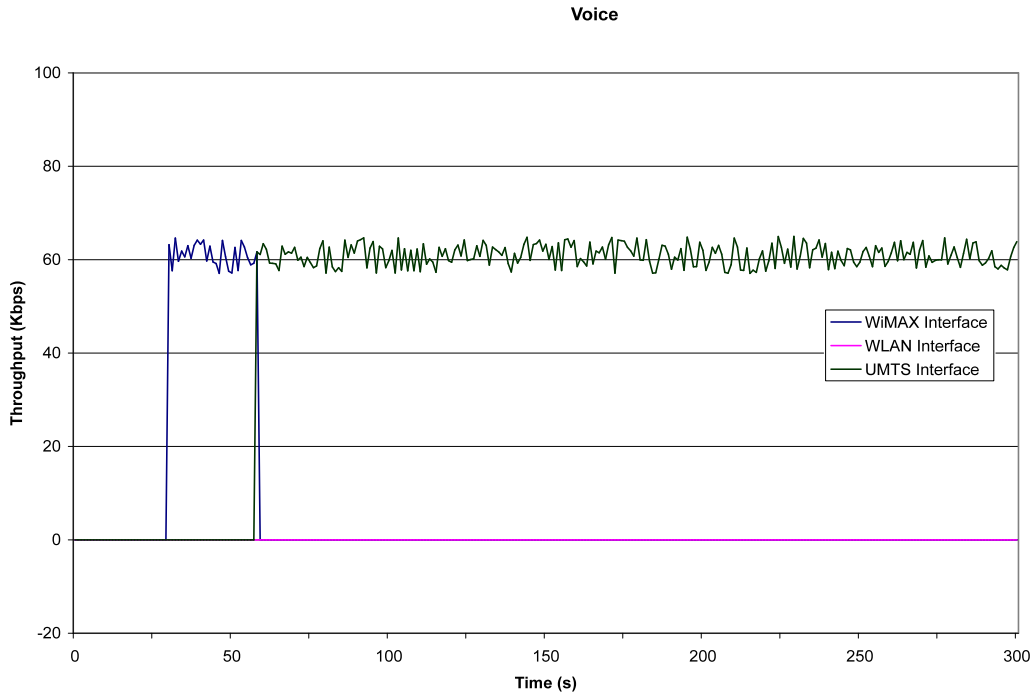

Figure 4-8: Voice Traffic

From the plot, it can be seen that initially traffic goes through WiMAX interface. After some time a switch is made and the traffic starts going through UMTS interface as shown by the green curve. In the PE we had set the rule that voice traffic is routed through UMTS interface. Figure 4-8 confirms this.

Figure 4-9 gives the measure of throughput on each interface when online gaming application is run from MN to CN.

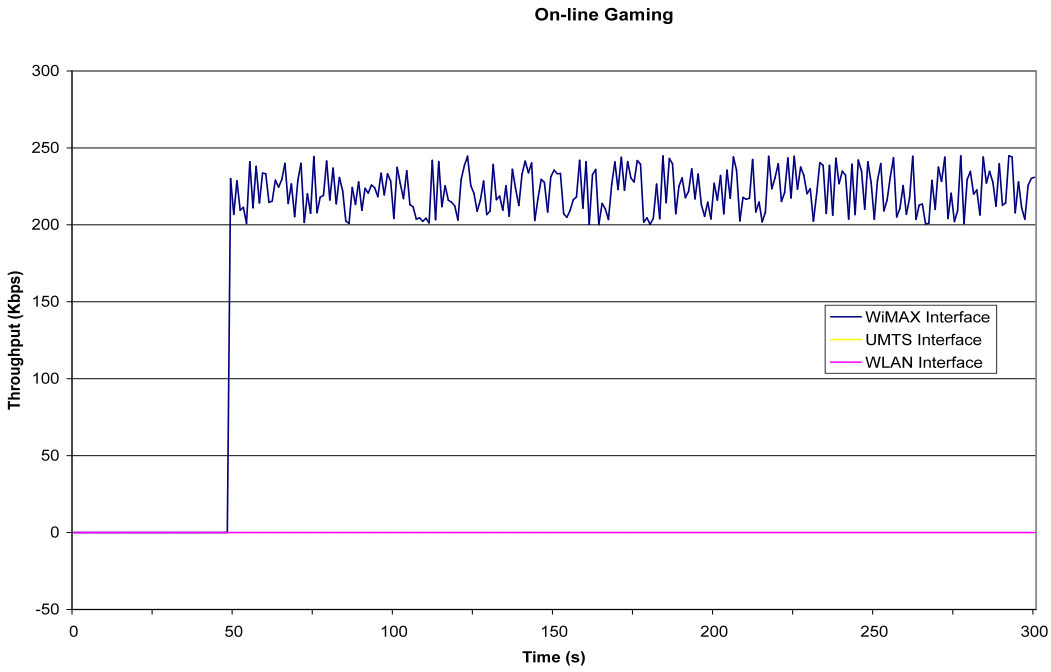

Figure 4-9: Online Gaming Traffic

From the plot, it can be observed that the online gaming traffic is going through the WiMAX interface. In PE we had set low latency as the preference for online gaming applications. For online gaming applications when all other application requirements are satisfied, the network having lowest latency should be chosen. Out of the three networks WiMAX is known to have the least latency. Figure 4-9 confirms this as application traffic is routed through WiMAX network.

Additional simulation was run where the three applications were simultaneously run from MN to CN. The resulting throughput plot on each interface is given in Figure 4-10. From the plot, it can be observed that the throughput on WiMAX interface is initially high. This shows that all three

applications are initially going through WiMAX interface. After a spike, the WiMAX interface throughput curve comes down. At about the same time, the throughput curves on WLAN and UMTS networks start ascending. This confirms that after some time, the video conferencing application traffic starts going through the WLAN interface while the voice application traffic starts going through the UMTS interface.

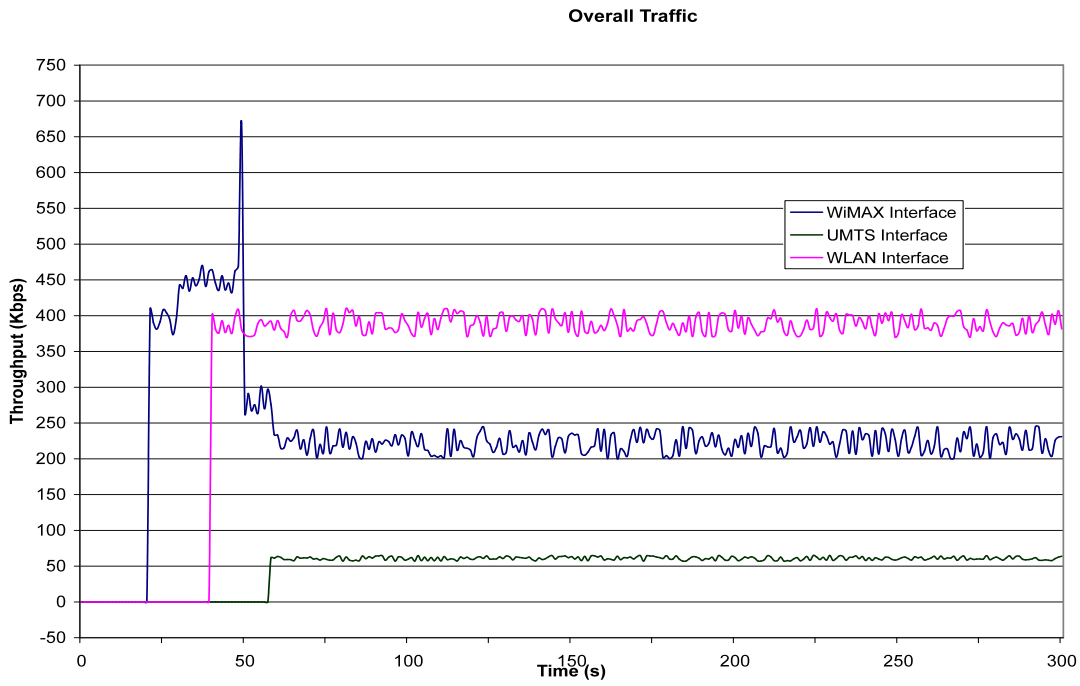

Figure 4-10: Overall Traffic

4.5 Chapter Summary

In this chapter, we proposed a new network selection mechanism for multi-homed MN in MIPv6 network. When MN is equipped with multiple active interfaces, it can choose the interface/network best suited for a particular application. To achieve this goal we designed a new Policy Engine.

Application requirements are defined in application profiles. Each network is analyzed against these requirements along with user preferences and a decision is taken by the Policy Engine on which network/interface to use for the particular application traffic. Network/interface switch is made through UR/UA message exchange.

Through this mechanism, it is ensured that best network/interface could be used for a particular traffic. We ran some simulations to test our proposal and observed the traffic switches a network/interface according to the policy defined in the Policy Engine. Moreover, switching delays are minimal.

Chapter 5

5 A New Seamless Mobility Mechanism for Multi-homed MIPv6 Enabled MN

In the previous chapters, it was highlighted that although MIPv6 is a widely accepted mobility solution for IPv6 based networks, it suffers from some flaws in heterogeneous network environment. One area of concern is handover management. For multi interfaced MN roaming in coverage area of multiple networks, it is desirable to perform handover between different networks/interfaces without causing traffic disruption.

Using current MIPv6 techniques this goal is impossible to achieve. In this chapter we build on the MNS-MIP6 idea presented in previous chapter and show that using the architecture, seamless handover is achieved between different networks/interfaces.

5.1 Introduction/Problem Statement

Providing mobility in an Internet environment has been a topic of much research over the past few years. The most important function of mobility is to keep ongoing communication alive when MN moves and changes its point of attachment to the Internet. MIPv6 has been accepted as a standard for supporting mobility in IPv6 based networks. However, MIPv6 suffers from some flaws. One such flaw is an unacceptable delay for many real-time applications caused by handover. Handovers can be divided into two categories: horizontal and vertical handovers. Handovers which occur within the same

access technology are horizontal handovers. On the other hand, vertical handovers take place when switch is made from one access technology to another [83]. Although high handover latency associated with MIPv6 has been identified as an important area of research and a lot of effort has been put to address the issue, there still doesn't exist a proposal which satisfies the vertical handover issue in real-time applications. Many ideas have been presented within IETF which focus on optimizing MIPv6 signaling to reduce handover delay. Out of these, Fast Mobile IPv6 (FMIPv6) [41], Hierarchical Mobile IPv6 (HMIPv6) [42], and most recently Proxy Mobile IPv6 (PMIPv6) [43] have gained much significance. Although these methods enhance MIPv6 handover performance, the disruption caused is still intolerable for many real-time traffic environments, i.e. handovers are not seamless. In today's heterogeneous network environment, this leaves much to be desired.

In the proposals mentioned above, much emphasis is on improving horizontal handover latency. Most MNs of today are equipped with multiple air interfaces. When such MN roams in an environment where it has access to multiple networks, it should be able to perform vertical handovers without much disruption.

In this chapter a seamless vertical handover mechanism is presented using MNS-MIPv6 architecture. It is shown that when multi-homed MN equipped with multiple interfaces is roaming in a heterogeneous network environment, handovers between the networks/interfaces are seamless. This results in minimal traffic disruption. The idea is supported by mathematical analysis and simulation results. The chapter is organized as follows: Section 5.2 constitutes related work. This is followed by explanation of proposed architecture in section

5.3. Section 5.4 gives the mathematical analysis simulation results followed by chapter summary in section 5.5.

5.2 Related Work

Handover process in MIPv6 is composed of three sub processes. These are movement detection, address configuration and address registration. MN registers its new CoA with either HA i.e. BT mode or with CN i.e. RO mode. Three major mechanisms to reduce handover delay in MIPv6 networks are FMIPv6, HMIPv6 and PMIPv6. These three use different approaches to reduce handover delay. FMIPv6 mechanism revolves around reducing movement detection and address configuration parts of handover delay whereas, in HMIPv6 and PMIPv6 the focus is on reducing address registration delay.

FAST HANDOVER FOR MIPv6

In FMIPv6 handover mechanism L2 triggers assist MN to quickly detect movement to a new subnet. MN can request new subnet information before or after getting disconnected from the current access point. As a result movement detection and address configuration times are reduced. FMIPv6 signaling is shown in Figure 5-1. A tunnel is established between MN's previous and new access routers. This gives rise to lower disruption time during handover.

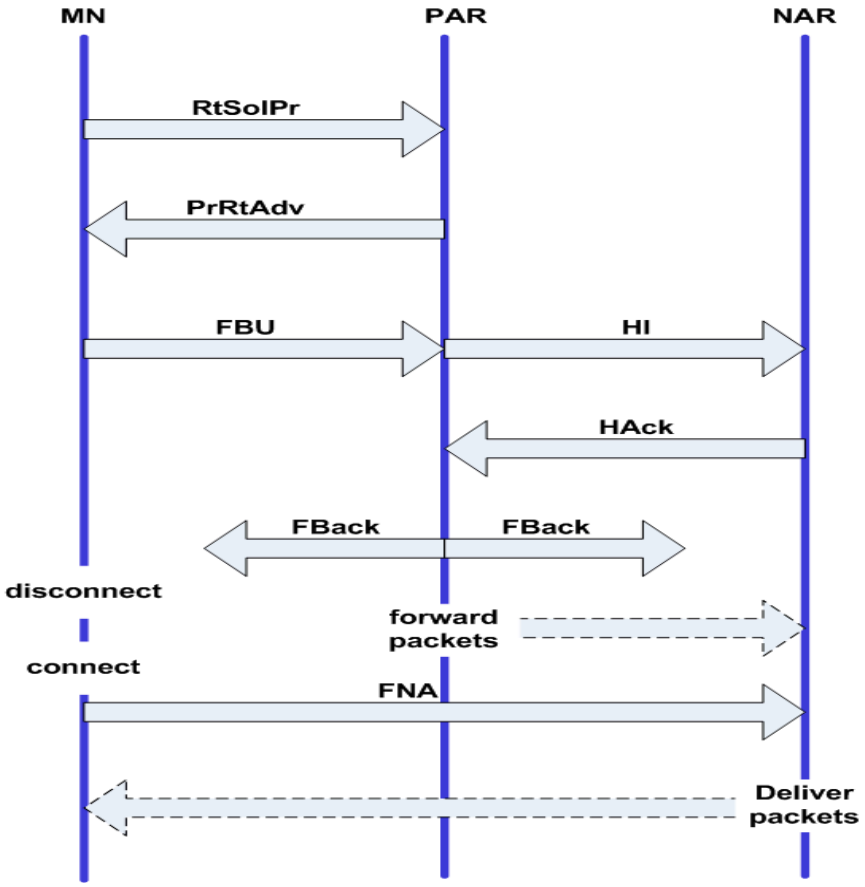

Figure 5-1: FMIPv6 Signaling

When an MN is moving to a new subnet a Link_GoingDown trigger is initiated which gives MN the available Access Points (APs). Consequently MN sends Router Solicitation for Proxy (RtSolPr) message to the Access Router (AR) it is attached to. This AR is known as PAR. This message tells PAR to resolve one or more AP Identifiers (AP-IDs) to subnet-specific information (AR-Info). The PAR sends back a Proxy Router Advertisement (PrRtAdv) message containing the [AP-ID, AR-Info] tuples. MN then configures a new CoA (NCoA). After configuring the NCoA, MN sends Fast Binding Update (FBU) message to PAR. PAR then sends a Handover Initiate (HI) message to New Access Router (NAR). The HI message contains MN's NCoA and previous CoA (PCoA). The NAR sends back a Handover Acknowledgement (HAck) indicating acceptance of

NCoA. A Fast Binding Acknowledgement (FBack) message is sent to MN from either the PAR or NAR. As a result a tunnel is established between previous CoA (PCoA) and NCoA. A LINK_UP trigger indicates new L2 connection. MN then sends a Fast Neighbor Advertisement (FNA) message to NAR. NAR then begins to deliver packets to the MN. Although FMIPv6 is the most promising MIPv6 enhancement to tackle handover latency, some studies [44][45][46][47] have concluded that the performance is not satisfactory for many real-time applications.

HIERARCHICAL MOBILE IPv6

HMIPv6 is another extension of MIPv6 which aims to improve handover performance. Mobility management is separated into inter-domain and intra-domain mobility management. A new entity called Mobility Anchor Point (MAP) is introduced to manage MN's mobility. MAP is a router or a set of routers which are normally placed at the edges of a network. It keeps a binding between itself and all the MNs visiting its domain. When MN enters a new network, it registers itself with the MAP serving that network. All packets destined for MN are intercepted by MAP and tunneled to MN's on-link CoA (LCoA). When MN moves but stays within the same MAP domain, it only needs to update binding in its local MAP. Hence, for micro mobility scenarios location update messages don't need to be sent to HA or CN. This results in lower address registration delay and signaling overhead.

When MN moves across a different MAP domain, it configures new Regional Care of Address (RCoA) in addition to LCoA. It then sends a BU to its MAP to bind the RCoA to LCoA. MAP would then return binding acknowledgement (BAck) to MN. In

addition, MN also sends BU to HA or CN in order to bind its RCoA with HoA. Basic HMIPv6 structure is shown in

Figure 5-2.

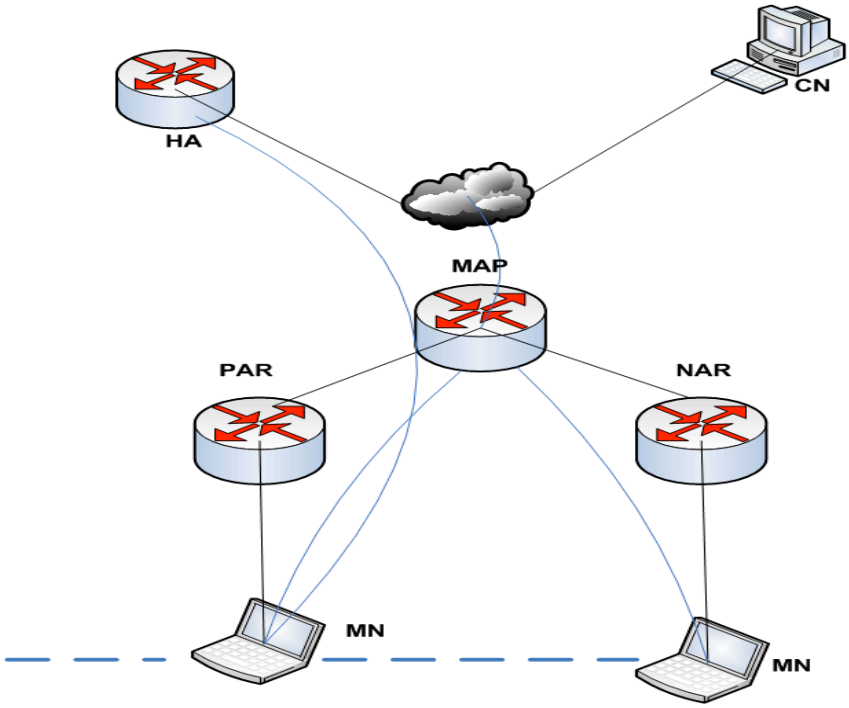

Figure 5-2: HMIPv6 Structure

PROXY MOBILE IPv6

Another IETF proposal that has gained much importance recently is PMIPv6. It is a network based mobility management extension of MIPv6. PMIPv6 introduces two new network entities: Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). Basic PMIPv6 structure is shown in Figure 5-3. MAG handles all the mobility related signaling on behalf of MN. This frees MN from any involvement in MIPv6 signaling and thus eliminates tunneling overhead over air interface. Binding between prefix assigned to MN and its local Proxy-CoA is kept in LMA. Thus LMA has the same functionality within PMIPv6 domain as HA in MIPv6.

When MN moves from one MAG to another, LMA receives a Proxy Binding Update (PBU) from MAG. This is followed by LMA sending a Proxy Binding Acknowledgement (PBA) back to MAG. A tunnel is then setup between MAG and LMA. LMA forwards any packet it receives on behalf of MN to its currently attached MAG.

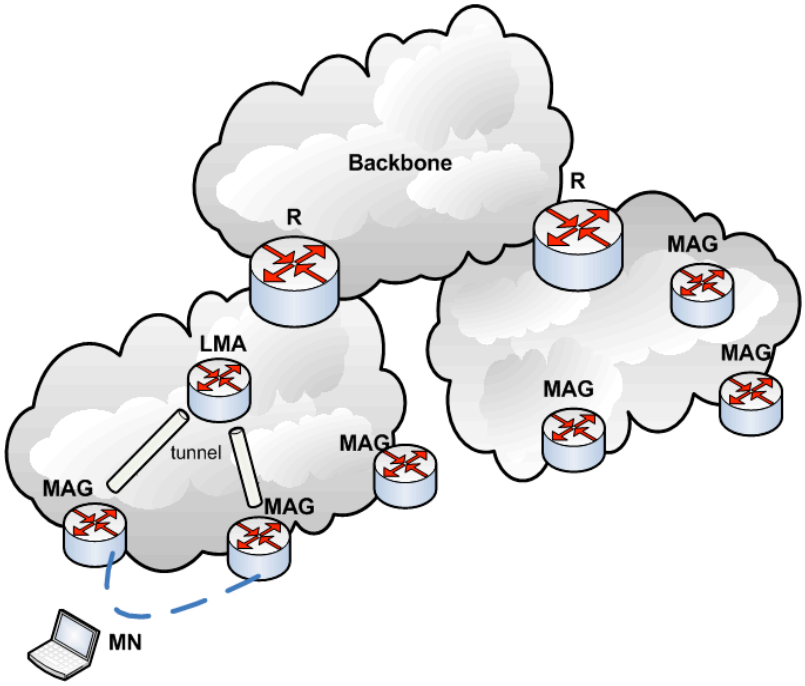

Figure 5-3: PMIPv6 Structure

Although these enhancements reduce the MIPv6 handover latency, they are still not seamless [48] [49] [50]. There is also a question mark about the scalability and complexity of these enhancements [70][81].

In addition to MIPv6 and its enhancements, there are some proposals whose primary focus is not mobility management but have nonetheless gained significance in this area. The most significant of these are HIP, mSCTP and Location Independent Network Architecture for IPv6 (LIN6). In these proposals mobility is tackled differently from MIPv6. Before

discussing these proposals, it is important to identify some of the requirements that need to be fulfilled in order for them to be deployed on large scale. These requirements are:

- **Transparency to upper layers**. Handovers should be transparent to layers above IP layer. There should be minimal changes to existing applications.
- **Avoid adding entities in the Internet**. Introducing third party entities in the Internet should be avoided as much as possible.
- **Smooth integration into Internet**. Solution should be easily integrated into existing Internet infrastructure.

In addition to handover management, these proposals are analyzed in view of the requirements.

HOST IDENTITY PROTOCOL

HIP has been described in chapter 1. Here, an overview is given of how HIP supports mobility management in IPv6 networks. HIP sub layer is introduced between network and transport layers of a host's protocol stack. A new namespace known as Host Identifier (HI) is introduced. HI is a public key. It is to this HI, instead of IP address, that transport layer connections are bound. Hence IP address is solely used for routing. HI is dynamically bound to one or more IP addresses in the HIP sub layer. In order to represent HI in 128 bit format, Host Identity Tags (HITs) are used. The Host Identifier Tag (HIT) is a 128 bit hash value of the HI that can be used in IPv6-sized address structures.

HIP operations are explained in Figure 5-4 [51]. HIP introduces Rendezvious Server (RVS) for location management. During initiation phase, the initiator of communication retrieves RVS IP address by looking up the domain name of peer from DNS through HIP RVS Resource Record (RR). After this, the initiator sends I1 message to RVS having HIT as the destination. RVS forwards the packet to the peer's current location. Rest of HIP initiation is carried out directly between the two communicating hosts without involving RVS. For updating its location, MN sends HIP update message with readdress parameter (REA) to the CN. CN responds to this by ACK message.

Although HIP provides a mobility management mechanism for IPv6 networks, its deployment costs are very high. By introducing a new entity namely RVS and a new namespace, HIP introduces added complexity to network infrastructure. As extensive efforts have been made in laying out the current Internet infrastructure, feasibility of employing a solution which requires huge changes is a big question mark. In addition, many applications which follow traditional layered structure have to be modified [51].

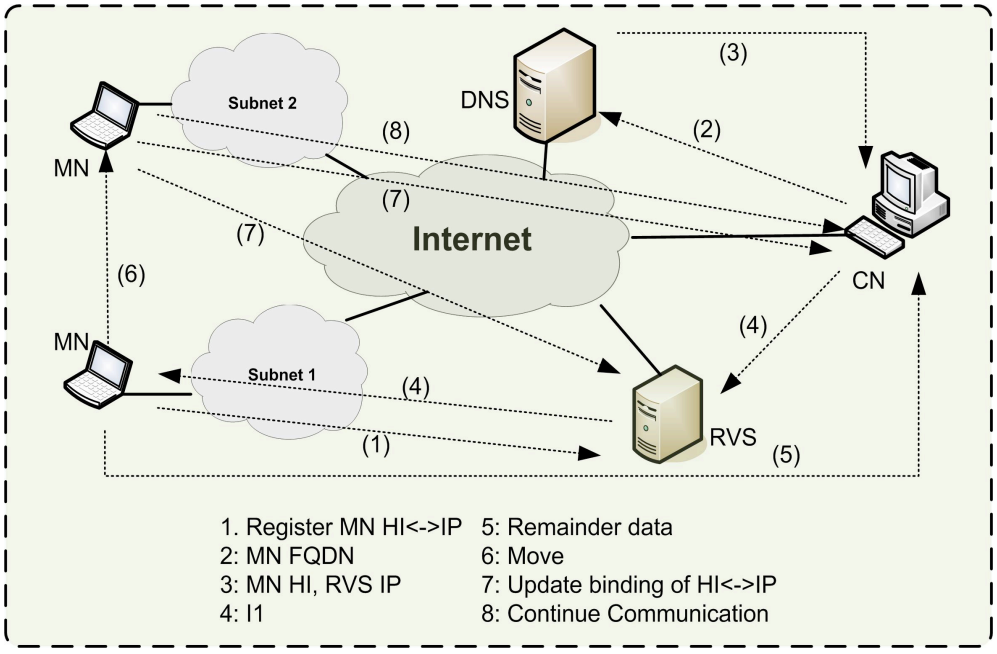

Figure 5-4: HIP Operations

MOBILE STREAM CONTROL TRANSMISSION PROTOCOL

SCTP is an alternative transport layer protocol to TCP and UDP. A mobility extension of SCTP called Mobile SCTP (mSCTP) is briefly described in chapter 1. In addition to having the same main features as TCP and UDP, it provides support for multi-homing, association concept and dynamic address configuration. An mSCTP association is initiated when MN negotiates a list of IP addresses with CN. One of these addresses is chosen as the primary path for communication. The other addresses are active IP addresses. When MN moves to a new network and obtains a new IP address, it sends Address Configuration Change (ASCONF) with Add IP Address parameter to CN. CN adds the new IP address to the list of association addresses and returns the ASCONF-ACK message back to MN. A moving MN can change the primary path to the new IP address through path management function [52]. An existing IP address can also be removed from the association.

This is done through MN sending a ASCONF message with Delete IP address parameter.

Although mSCTP has some promising features, it cannot be a stand alone mobility solution. There is no location management support function in mSCTP. Also, the proposal doesn't provide any details on how when the primary path should change. Hence, it cannot be employed as a mobility solution on its own. In heterogeneous network environment, the IP address change is not transparent to layers above IP.

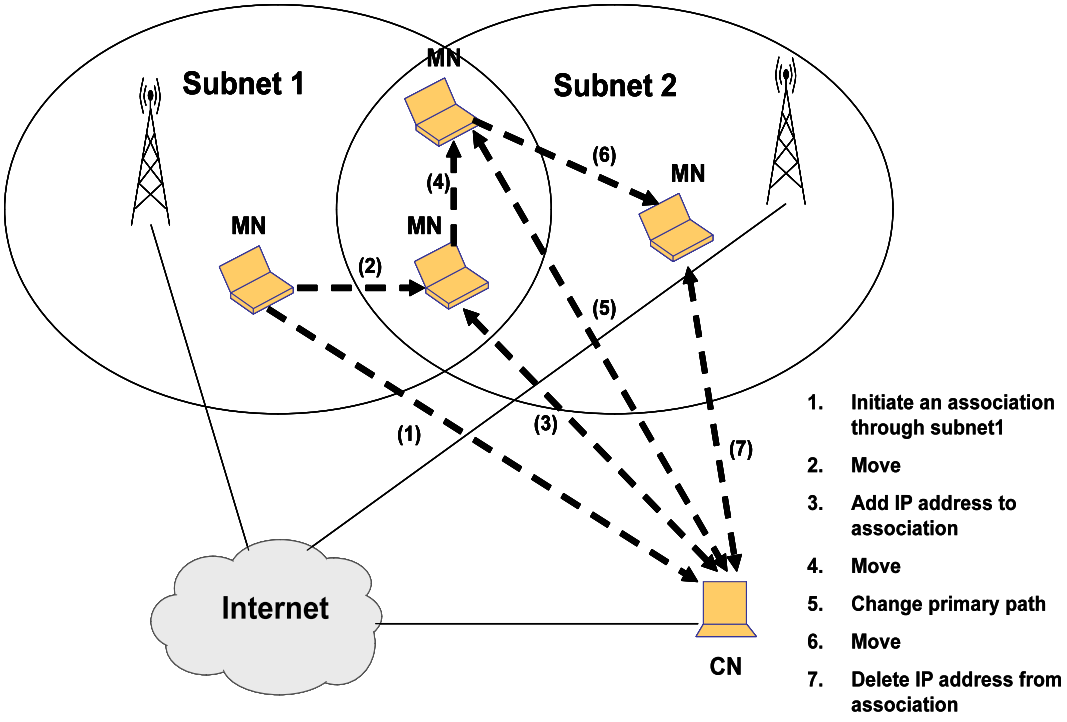

Figure 5-5: mSCTP Signaling

LOCATION INDEPENDENT NETWORK ARCHITECTURE FOR IPv6

LIN6 [53] aims to tackle mobility by separating the identifier and locator parts of an IP address. A network node is identified by LIN6 ID. Two types of IP addresses are defined: the LIN6 generalized ID and LIN6 address. LIN6 generalized ID

used to identify the connection in transport layer. LIN6 address is used to route packets over network layer. LIN6 generalized ID is formed by concatenating a constant value called LIN6 prefix before LIN6 ID. LIN6 address is formed by concatenating network prefix with LIN6 ID.

LIN6 employs Mobility Agents (MAs) for location management. Mapping of LIN6 ID and network prefix is kept at MA. Each MA is assigned a 64-bit value called MA Interface Identifier (IFID). During bootstrapping phase MN registers its current location with its MAs. For initial communications CN sends a query to DNS server and obtains the network prefix of MA and LIN6 ID of MN. The CN then forms the IPv6 address of MA by concatenating upper 64-bits of AAAA record and MA IFID. CN then queries for MN's network prefix from its MA and gets its IP address. When MN moves to a new network, it registers its new network prefix with MA and CN by sending Mapping Update message or Mapping Refresh message. LIN6 mobility mechanism is shown in Figure 5-6.

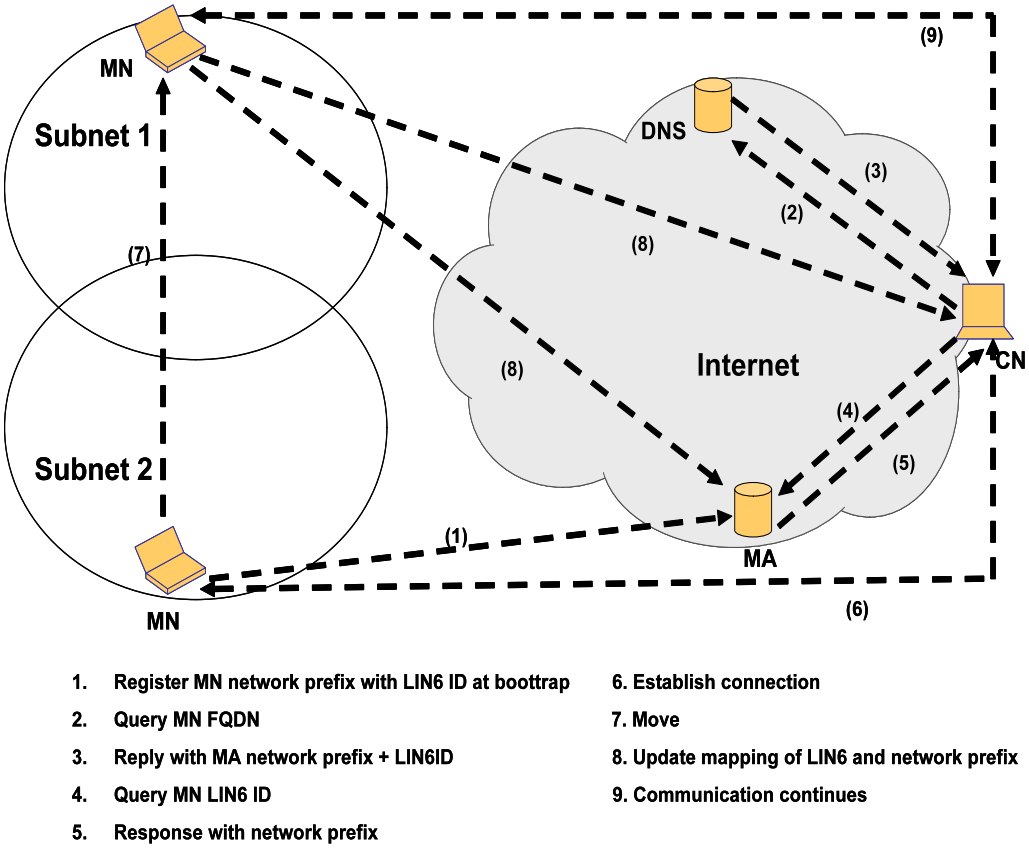

Figure 5-6: LIN6 Signaling

All the proposals listed have limitations which prevent them from providing seamless mobility support in heterogeneous network environment [54]. A multi interfaced MN having access to multiple technologies should be able to roam without loss of connectivity [55].

5.3 Proposed Architecture

During MIPv6 bootstrapping phase MN is allocated HA in its HN [72] [73]. Permanent address of this MN is its HoA. When this MN moves away from its HN into a visited network, it configures another address known as its CoA. MN sends a BU message with this CoA to HA. HA updates its cache binding entry and sends BA message back to MN. All the packets sent to MN's HoA are now intercepted by HA and tunneled to MN's

CoA. The packets from MN can be sent directly to CN. This mode of communication is known as BT mode. BT is the traditional mode of MIPv6 communication. This mode gives rise to a problem commonly referred to as triangular routing. The traffic from CN to MN has to go through HA while traffic in opposite direction doesn't. This gives rise to unnecessary delays. A more robust mode of MIPv6 communication is RO mode. In this mode, in addition to HA, CN also keeps the binding between MN's HoA and CoA. When MN changes its CoA, it sends BU both to CN and HA. CN can communicate directly with MN without going through HA. This is done by including home address option in destination options header and a new type 2 routing header to the packets. The semantics of these messages can be found in MIPv6 standard.

MN which is equipped with multiple active interfaces can at a time be configured with more than one IPv6 address. In this section it is shown how this MN can seamlessly roam through heterogeneous network environment.

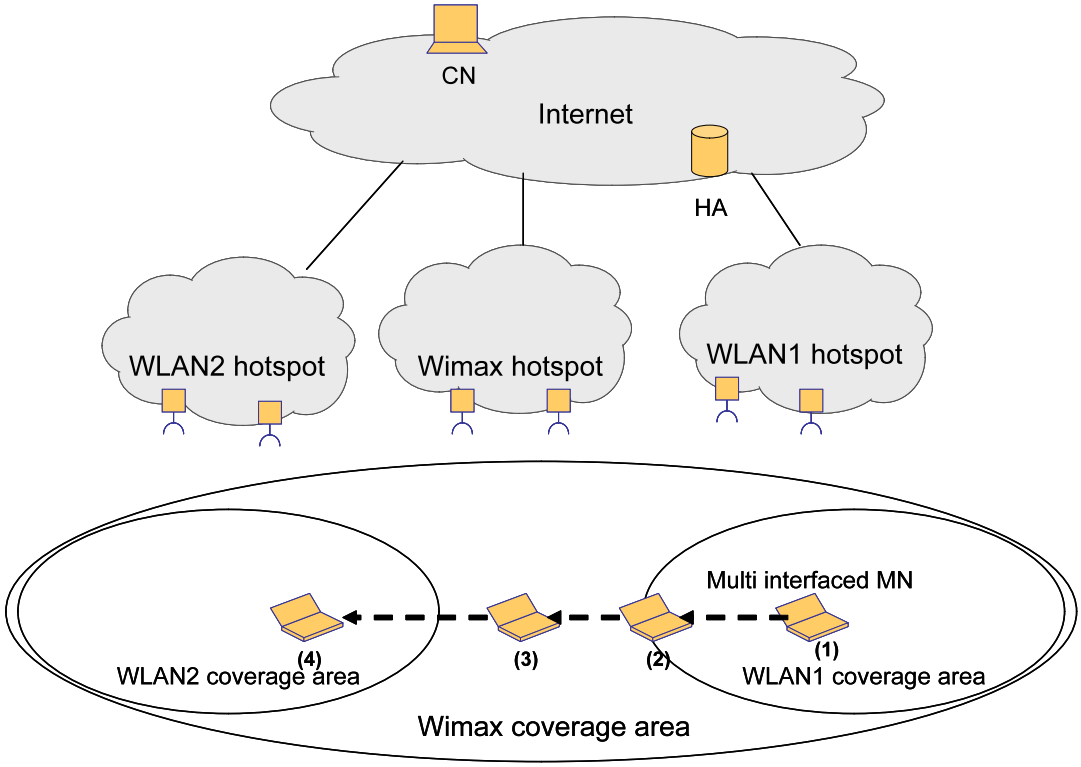

Figure 5-7: MNS-MIP6 Seamless Handover Network Scenario

Building on the MNS-MIP6 idea presented in chapter 2, a handover procedure is defined to enable multi interfaced MN to switch from one access technology to another without breaking communication sessions.

The idea is explained with help of network scenario of Figure 5-7. The route optimization mode of MIPv6 is considered as it is the common mode in IPv6 communications. A multi interfaced MN is initially at location 1 where it is in the coverage area of two access networks. In the context of mobility, MN can either be in its HN or in a visited network. It is assumed that MN is in a visited network. IPv6 address configured on the WLAN interface is the CoA for MIPv6 session. The other WiMAX interface is also active and an IPv6 address is configured on it. MN is communicating with CN and

after some packets are exchanged a context is established between the two. ULID for MN is the HoA while the locator set consists of all the addresses on interfaces including the CoA. In Figure 5-7 locator set consists of addresses on WiMAX and WLAN interfaces. At this stage of communication the MNS sub layer is by passed as HoA is mapped to CoA in MIPv6 sub layer. However, changes to any of the addresses are communicated to MNS sub layer so that locator set can accordingly be updated. When MN moves to location 2 where it is at the edge of WLAN1 and WiMAX coverage areas, WLAN1 network signal strength starts deteriorating. A Link_GoingDown trigger is generated. The MNS sub layers in MN and CN exchange UR and Update UA messages. The Change_loc_pref flag in UR message is set to indicate that communication should switch to the other locator (IPv6 address on WiMAX interface). Upon receiving the UR message, MNS sub layer in CN changes the locator preference for communication and acknowledges by sending UA message back to MN. All the packets now travel through the second interface. HoA is mapped to the WiMAX network IPv6 address at MNS sub layer. All the packets now travel with MNS extension header. The IPv6 address on WiMAX interface is the new CoA for MIPv6 session. A MIPv6 BU message is sent to HA and CN. The Return Routability (RR) test is run for the new CoA [56]. HA and CN change binding cache entry with the new CoA and send BA message back to MN. Upon receiving the BA message MN returns to normal MIPv6 procedures and HoA is now mapped to CoA at MIPv6 sub layer.

This mechanism involves using L2 triggers to anticipate a L3 handover and switch the session to a different interface. The triggering mechanism is similar to FMIPv6. SNR on each

interface is periodically checked through scanning procedures. When the value of SNR on an active interface used for communication approaches a low threshold value, Link_GoingDown trigger is generated. Switch is made to a different network/interface through MNS sub layer. The result is that handovers remain seamless and sessions are not broken. Hence, when MN moves out of the coverage area of the previously active network, it doesn't lose connectivity with CN.

When MN moves out of WLAN1 network coverage area, Link_Down trigger is generated. MNS sub layer on MN sends UR message to CN with Remove_loc flag set. MNS sub layer on CN removes the address associated with WLAN1 from locator set and sends back a UA message.

When MN moves to a coverage area of a new network WLAN2, Link_Up trigger is generated and a new IPv6 address is configured on the WLAN interface. MNS sub layer on MN adds the address to the locator set and sends UR message to CN with Add_loc flag set. CN adds the new address to MN's locator set and replies with a UA message.

5.3.1 Building Blocks

In order to deploy the seamless handover mechanism, some building blocks have to be defined. This section describes building blocks required to implement the seamless handover procedure of S-MIPv6.

Context Establishment:

When multi interfaced MN and CN are communicating with each other a context can be established between the two. The procedures are the same as explained in Chapter 2. HoA

assigned to MN is ULID for the context. Locator set contains all the additional addresses including the current CoA. Sender and Receiver context tags are randomly generated 47 bit numbers. As explained in the previous chapter, I1, R1, I2, and R2 messages are exchanged between MN and CN. When any of these addresses changes or becomes obsolete, MNS sub layer is informed and locator set is accordingly updated.

Updating Locator Set due to Mobility:

When any of these addresses changes or becomes obsolete, MNS sub layer updates the locator set. When signal strength on an active interface has deteriorated, a Link_GoingDown trigger is generated. If the address going down is the CoA for MIPv6 instance, MNS sub layer chooses a different locator/IPv6 address for communication and sends a UR message with Change_loc_pref flag set to CN. The context is accordingly changed and UA message is sent back from CN to MN. ULID is mapped to the new locator at MNS sub layer and packets are sent with MNS header. .

Deletion of Address from Locator Set:

When signal strength on one of the MN interfaces becomes too low, a Link_Down trigger is generated. The locator associated with the down interface is removed from the locator set. A UR message with Remove_loc flag set is sent to the CN. MNS sub layer on CN removes the locator from the list and sends back a UA message to MN. Hence the obsolete address is removed from locator list.

Addition of Address to Locator Set:

When signal on a previously down interface becomes significant, a Link_Up trigger is generated. A new IPv6 address

is configured on this interface. This address is added to the locator set and an UR message with Add_loc flag set is sent to CN. The locator is added to the context running on CN. MNS sub layer in CN sends back a UA message to MN. Hence a new address is added to the locator set.

Link Layer Triggers:

The seamless mobility mechanism uses link layer triggers to assist in switching from one IP address to another or to remove an IP address from locator set. There are three triggers used: Link_GoingDown, Link_Down, and Link_Up triggers. When signal on any interface starts deteriorating the Link_GoingDown trigger is generated. This trigger anticipates a handover and to switch the communication from the currently used interface/IP address to a different IP address. A BU message is also sent to HA and CN to update their binding cache entries with a new CoA. A Link_Down trigger is generated when MN moves out of coverage area of a network and signal on the associated interface becomes too low. MNS sub layer removes IP address/locator associated with the interface from locator list. A Link_Up trigger is generated when signal on an interface becomes significant and a new IPv6 address is configured on it. MNS sub layer on MN adds the IPv6 address on associated interface to the locator set. It sends a UR message to CN with Add_loc flag set. The CN responds with UA message.

Binding Procedures with HA and CN:

In MIPv6 when MN is away from its HN, it is configured with a CoA. Every time MN moves into a new subnet, handover procedure is initiated. A new CoA is configured and registered with HA and CN through BU/BA message exchange. Until a

new CoA is configured, all communication between MN and CN seizes. Therefore, it is called break before make handover.

In the MNS-MIP6 seamless handover mechanism, communication switches to a different IPv6 address/locater before link actually goes down. Hence, it is a make before break handover. When the Link_GoingDown trigger is generated, MNS sub layer switches communication to the second interface. A BU message is sent to HA and CN. HA and CN reply with a BA message. During this registration time, communication continues via a second interface bypassing MIPv6 sub layer. Upon reception of BA message, communication is switched back to MIPv6 with the new CoA.

5.3.2 General Workflow

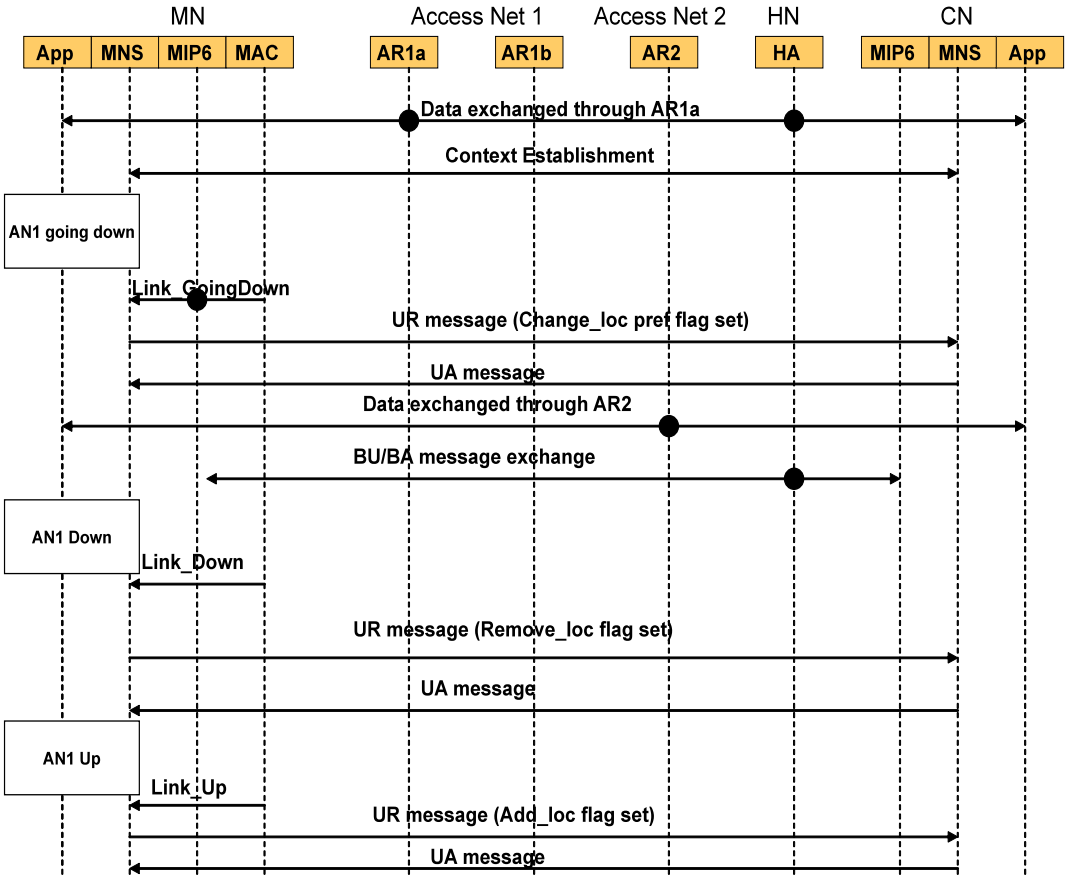

Figure 5-8: MNS-MIP6 Seamless Handover Signaling Diagram

The mechanism is further explained with help of a signaling diagram of Figure 5-8. MN has two active interfaces connected to Access networks 1 and 2 respectively. Initially, communication with CN is through Access network 1 (AR1a). A context is established between MN and CN where ULID is the HoA and locator set contains the IPv6 addresses on both interfaces.

When signal on interface 1 becomes low, a Link_GoingDown trigger is generated. Consequently, MNS sub layer on MN sends a UR message with Change_loc pref flag set to MNS sub layer on CN. The MNS sub layer on CN replies with a UA

message. The communication between MN and CN now takes place via Access network 2 (AR2). MIPv6 sub layer is bypassed.

A BU message is sent from MN to HA and CN to update the binding cache entry with new CoA. After running the Return Routability procedure, a BA message is sent back to MN. Communication reverts back to normal MIPv6 procedures and HoA is now mapped to the CoA at MIPv6 sub layer. MNS sub layer is by passed.

When MN moves away from AR1a such that signal strength on the associated interface becomes too low, a Link_Down trigger is generated. MNS sub layer on MN sends a UR message with Remove_loc flag set to CN. The MNS sub layer on CN removes the locator and sends a UA message back to MN.

Finally when MN moves back into the coverage area of Access Network 1 (AR1b), a Link_Up trigger is generated. The locator set is updated with the addition of the new address.

We compare our MNS-MIP6 handover signaling with FMIPv6. FMIPv6 handover signaling is given in Figure 5-9. In FMIPv6, communication session between MN and CN is broken when AN1 goes down and is not restored until AN2 becomes active. Hence, the handover disruption time in FMIPv6 is much more than our proposed solution.

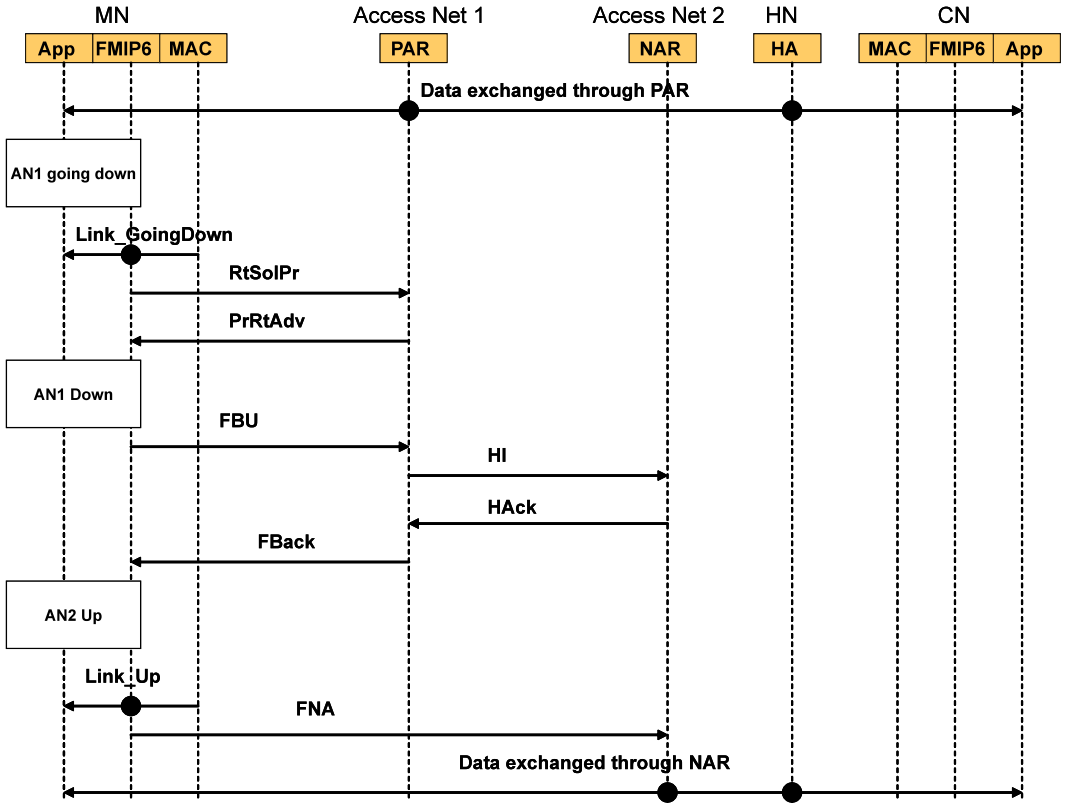

Figure 5-9: FMIPv6 handover signaling

5.4 Performance Analysis

In this section we evaluate the performance of our proposed seamless handover mechanism by comparing it with the most promising MIPv6 extension to reduce handover latency i.e. FMIPv6. First we compare handover delay through mathematical analysis and then we run some simulations.

5.4.1 Mathematical Analysis

Handover Latency in FMIPv6

We consider the more faster predictive mode of FMIPv6. In predictive mode of operations movement detection and new CoA configuration is done prior to the actual Layer 2 handover. This phase is known as Handover Initiation (HI)

phase. The four messages involved in HI phase are RtSolPr, PrRtAdv), FBU, and FBAck. The total delay involved is thus

$$D_{HI} = D_{RtSolPr} + D_{PrRtAdv} + D_{FBU} + D_{FBAck}$$

If we assume that Layer 2 delay is D_{L2} and once MN attaches to the nAR, it sends Fast Neighbour Advertisement (FNA) to it. Assuming the single trip time from MN to nAR is $D_{MN\text{-}nAR}$. The total handover delay becomes:

$$D_{HO\text{-}FMIPV6} = D_{HI} + D_{L2} + D_{MN\text{-}nAR} \quad (a)$$

Handover Latency in MNS-MIP6 mechanism

Now considering our proposed mechanism, the handover delay doesn't include HI time as there doesn't exist a need to form a new CoA or send FBU to HA. Hence the handover initiates with L2 triggers. If $D_{MN\text{-}CN}$ denotes the single trip time between MN and CN, the total handover delay is given by:

$$D_{HO\text{-}MNS\text{-}MIP6} = D_{L2} + 2\, D_{MN\text{-}CN} \quad (b)$$

From equations (a) and (b) we can observe that in the MNS-MIP6 assisted handover, the handover initiation time is zero. The reason is that the context already contain valid IP addresses for the MN/CN. Hence, when handover is detected in layer 2, a switch is made through UR/UA message exchange. This is quicker than first forming the new CoA and then registering it with HA through FBU/FBAck message exchange.

5.4.2 Simulation Results

We test the proposed seamless mobility procedures by running simulations using OPNET 14. We compare our proposal with FMIPv6. For this, OPNET MIPv6 module is modified to support

FMIPv6 (control messages). A multi interfaced MN is created using OPNET's custom node facility. MN has WiMAX 802.16e and WLAN 802.11b interfaces. In addition, the MNS process model is incorporated in MN and CN. The link layer triggers, Link_Down, Link_GoingDown and Link_UP are also defined.

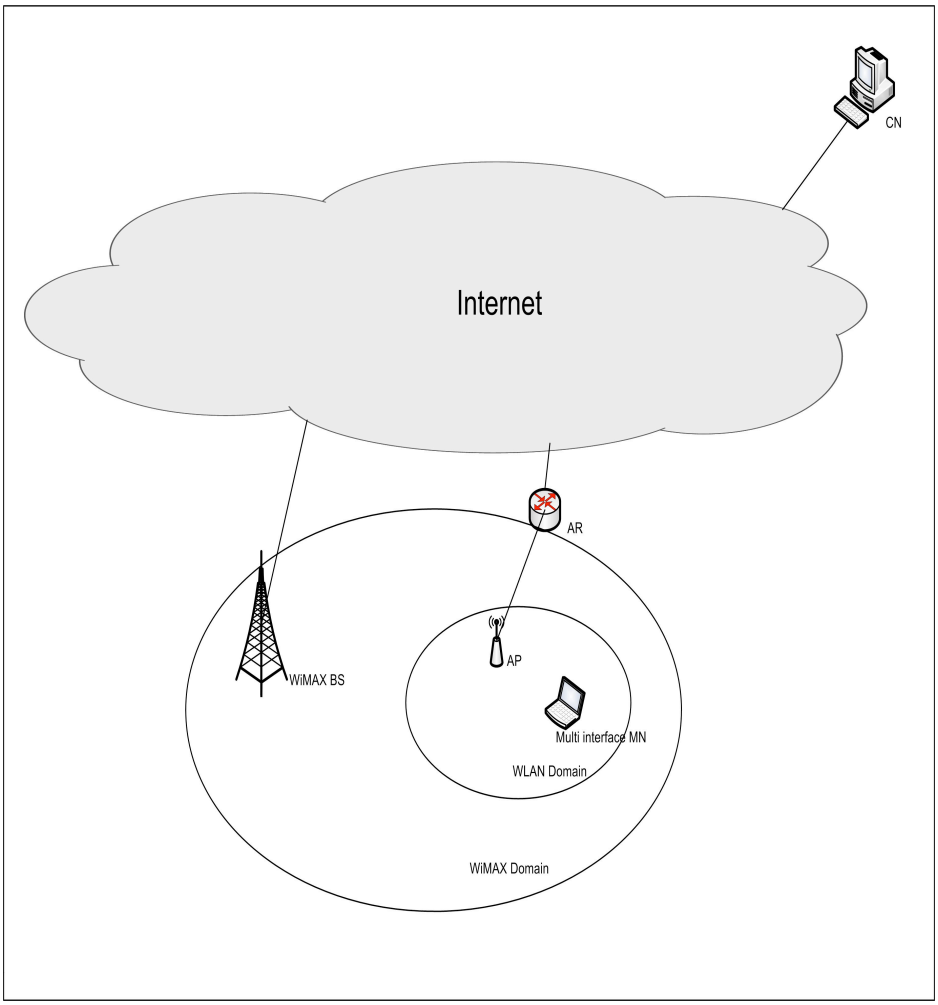

Figure 5-10: MNS-MIP6 Seamless Handover Simulation Setup

Simulation network scenario is shown in Figure 5-10. Simulation area is 3 kilometers by 3 kilometers where a WiMAX cell with radius of 1.5 kilometers and a WLAN Basic Service Set (BSS) with coverage area of 60 meters are located. WLAN BSS is located within the WiMAX cell. We assume the

mobility is managed by a single Mobility Service Provider. WLAN is the home domain where HA is located. CN is connected to the Internet through a 100Mbps Ethernet connection. MN moves in the area with speed of 10 meters/second while communicating with CN.

We evaluate the handover performance based on handover latency, handover signaling, and packet loss.

Handover Latency

Handover latency is defined as the time elapsed between last packet received on the old link and the arrival of new packet on the new link. It is the time period during which MN can neither send nor receive any traffic.

Handover Signaling Load

The signaling traffic during handover procedure.

Packet Loss

The number of packets lost during handover procedure.

Two traffic profiles are defined to run between MN and CN. A video streaming traffic with packet size of 182 bytes and rate of 150 packets/second and an audio stream with packet size of 185 bytes and rate of 30 packets/second. The simulation time was set at 600 seconds. There were 10 runs each for FMIPv6 enabled handover and our proposed MNS-MIP6 handover procedure. We plot the comparison between two mechanisms in terms of handover latency, handover signaling load, and packet loss in Figures 5-11, 5-12 and 5-13 respectively.

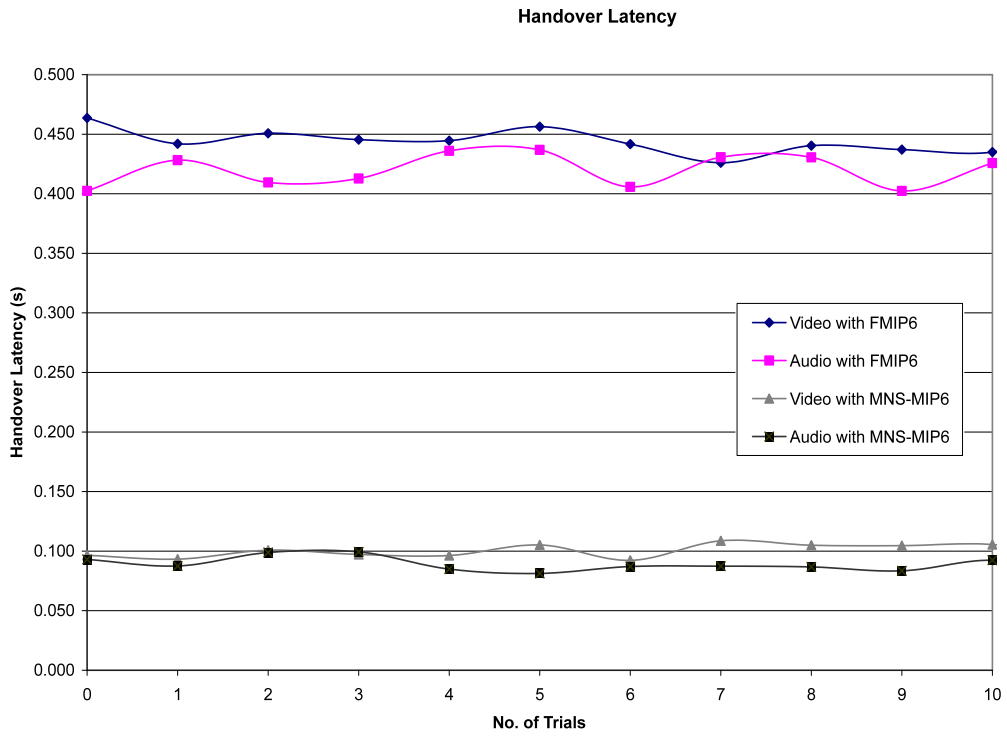

Figure 5-11: FMIPv6 and MNS-MIP6 Handover Latency Comparison

From Figure 5-11 it is evident that handover latency for both types of traffic is significantly reduced when using the MNS-MIP6 enabled mechanism. The main reason for this is that in MNS-MIP6 mechanism, the moment handover is anticipated through Link_GoingDown trigger, UR/UA messages are exchanged between MN and CN and a switch is made to new locator set. Hence, in comparison to FMIPV6, the handover procedure is completed in much shorter time. In fact, handover latency is reduced by approximately one fourth.

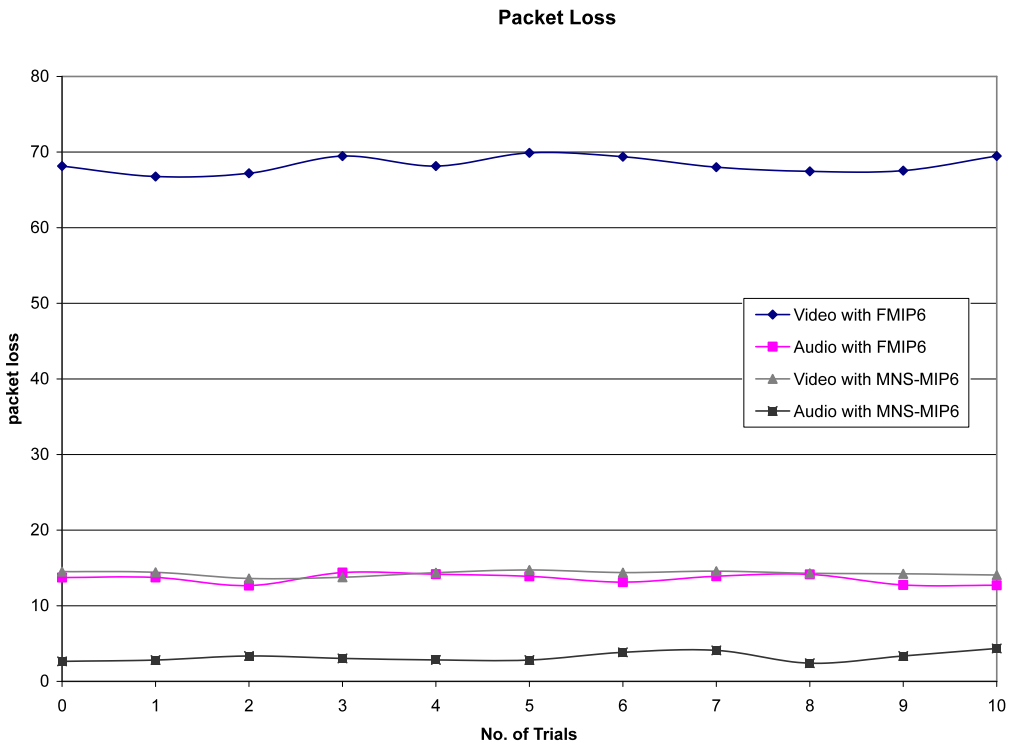

Figure 5-12: FMIPv6 and MNS-MIP6 Packet Loss Comparison

Low handover latency results in low packet loss. Packet loss due to handover is given in Figure 5-12. Note that there is a big difference in packet loss between video and audio traffic. This is due to the difference in number of packets sent per second for both the traffics. In video streaming 150 packets are sent in a second whereas in audio streaming only 30 packets are sent per second. Again there is a dramatic reduction in number of packets lost when using MNS-MIP6.

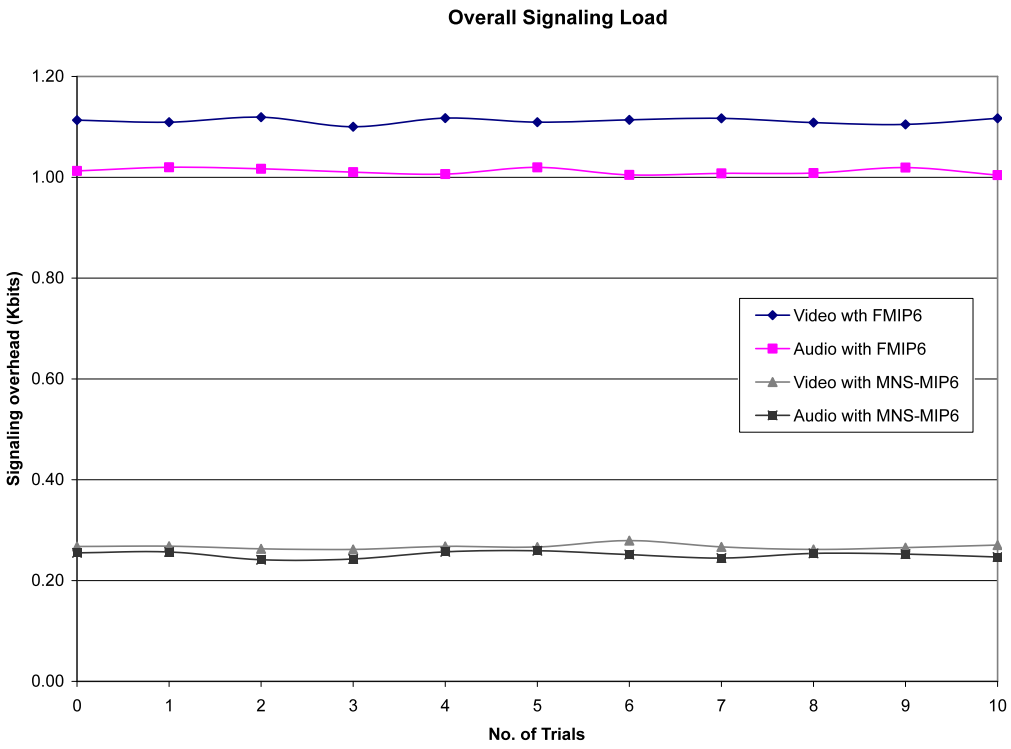

Figure 5-13: FMIPv6 and MNS-MIP6 Overall Signaling Load Comparison

Figure 5-13 gives the handover signaling overhead. Note again that the signaling overhead is considerably less in MNS-MIP6 mechanism compared to FMIPV6. This is because in MNS-MIP6 handover mechanism, only two signaling messages UR and UA are involved where as in FMIPV6 there are seven signaling messages. Hence, the overall handover signaling overhead is much less for MNS-MIP6 enabled handovers.

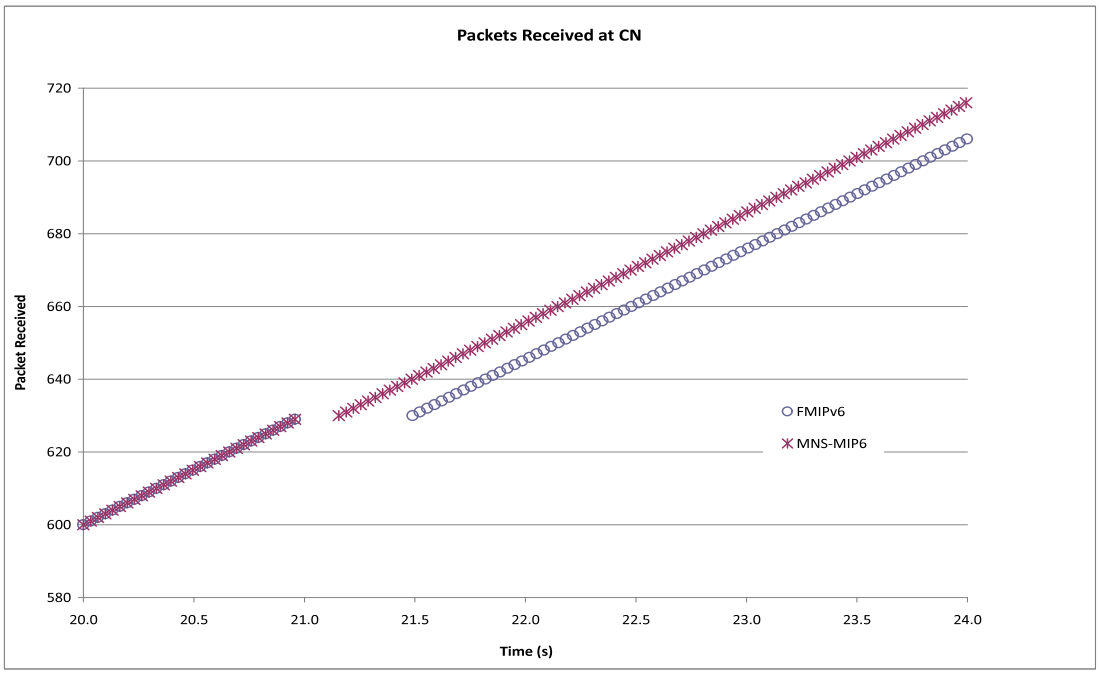

Figure 5-14: Packets Received Comparison between FMIPv6 and MNS-MIP6

In Figure 5-14, the comparison of FMIPv6 and MNS-MIP6 handoff mechanism in terms of packets received is given. We only use audio traffic stream for the simulation run. The handoff initiates at 21 seconds mark. It can be seen that the disruption caused by MNS-MIP6 handoff is much less than FMIPv6 handoff.

5.5 Chapter Summary

In this chapter, we proposed a seamless handover procedure using MNS-MIP6. A multi interfaced MN roaming in heterogeneous network environment can switch from one active network/interface to another without much traffic disruption. The mechanism is assisted by Layer 2 triggers.

A context is established between MN and CN and once signal strength on the communicating interface becomes low, a

Link_GoingDown trigger is generated. UR/UA messages are exchanged between MN and CN and the context is used to switch communication to a different locator pair. The new source locator becomes CoA for MIPv6 instance.

MIPv6 layer sends BU message containing the new CoA to HA and CN. Hence, while normal MIPv6 handover procedure is followed, the switching takes place through MNS signaling. This greatly enhances MIPv6 handover performance. This is especially significant for delay-sensitive applications such as VoIP and video streaming. We showed through simulations that our proposed mechanism greatly reduces handover latency, packet loss, and overall handover overhead when compared to the most widely accepted MIPv6 enhancement, namely FMIPv6.

Moreover, only minor modifications are required to MIPv6 individual nodes i.e. MN, HA, and CN to run our proposed mechanism. MNS sub layer is introduced within IP layer in node's protocol stack. In addition, three link layer triggers are defined to assist the handover procedure. Hence, our proposed mechanism does not add any new entities or major complexity to the existing MIPv6 system.

When MNS-MIP6 enabled MN is communicating with CN which does not support MNS signaling, normal MIPv6 protocol can be used to support mobility. Hence, our proposed mechanism I compatible with base MIPv6.

Chapter 6

6 Proxy MNS-MIP6 Support for Legacy Non MNS-MIPv6 Enabled CN

Our work has been based on supporting multi-homing in MIPv6 networks by introducing a new sub layer in MN's protocol stack. We have shown in the previous chapters that by employing our proposed MNS-MIP6 mechanism, main benefits of multi-homing i.e. reliability, load sharing and seamless mobility are obtained for MN located in a heterogeneous network environment. In all our work, the main assumption has been that CN with which MN is communicating supports MNS signaling. However, in current Internet environment hosts protocol stacks don't contain MNS sub layer.

An MNS-MIP6 enabled MN cannot establish a context with such hosts. Thus, in order to gain true multi-homing benefits, a mechanism needs to be defined through which MNS capable MN can communicate with non MNS capable CNs and gain multi-homing benefit.

In this chapter we propose a mechanism through which MNS-MIP6 system is supported in situations where an MN communicates with non MNS capable CN. Middleboxes known as Proxy MNS-MIP6 or PMNS boxes are introduced in non MNS capable host's or CN's network. Through those boxes context is established between MN and CN.

6.1 Introduction/Problem Statement

In the previous chapters it was shown that through MNS-MIP6, MN running MIPv6 can take advantages of multi-homing. The advantage include reliability, and load sharing capabilities. In addition, in heterogeneous network environments, seamless handovers can be supported through MNS-MIP6.

An MNS-MIP6 system requires both ends of communication to have MNS sub layer. MNS sub layer resides above MIPv6 sub layer in MN. The other end of communication i.e. CN can either be static or mobile. For static CN, MNS sub layer resides within IP layer. For mobile CN, MNS sub layer resides within IP layer above MIPv6 sub layer.

Legacy nodes on the Internet do not contain MNS sub layer in their protocol stacks. Hence, the benefits of MNS-MIP6 can not be envisaged when one or both ends of communication are such legacy nodes.

When both MN and CN are MNS capable, the multi-homing mechanism is supported. However, when MNS-MIP6 supported MN is communicating with non MNS CN, multi-homing cannot be supported. Additional mechanisms/procedures are required to enable MNS to run on such legacy nodes.

A mechanism is introduced in this chapter which allows MNS-MIP6 supported MN to communicate with CN not containing MNS sub layer and obtain the multi-homing benefits listed in the previous chapters. Middle boxes known as proxy-MNS-MIP6 or PMNS boxes are introduced in non MNS CN's network.

6.2 Related Work

In our proposed MNS-MIP6 mechanism some of the signaling is same as in SHIM6 protocol. However, base SHIM6 is a site wise multi-homing solution rather than end host based. In the original SHIM6 architecture multiple ISPs advertise their prefixes on the site. This results in configuration of multiple IP addresses for each host located in the site. The additional addresses can be used as locators and when failure takes place, communication can switch to using a different locator pair for routing traffic.

When SHIM6 architecture was presented a need was felt to define a mechanism which would allow legacy non SHIM6 hosts on the Internet to be able to establish SHIM6 context with SHIM6 hosts and enjoy multi-homing benefits. In this regard a draft Proxy Shim6 or P-Shim6 [57] was presented.

Proxy Shim6:

In the SHIM6 architecture, peers exchange their multiple IP addresses so that in case failure is detected in the communication path, the switch can be made to a different address. For hosts which don't support SHIM6 signaling, proxy shim6 middle box/boxes are introduced in the host's network. Hence, context management is off loaded from the actual end hosts to these middle boxes. This scheme consists of the following two main features:

- Introduction of Centrally Managed Unique Local Addresses (CMULA's) as ULIDs.
- A new DNS Resource Record (RR) is defined for storing ULIDs.

- Use reverse DNS to retrieve locator information for the ULIDs.

A multi-homed site obtains a Provider Aggregatable (PA) prefix from each of its ISPs and a non-routable Provider Independent prefix from a central registry (CMULA). Hosts within this site are configured with a single address containing the CMULA prefix. A new RR is created in DNS for ULID. CMULAs are published in this RR.

Each multi-homed site contains one or more p-shim6 boxes. When a non SHIM6 host located within a multi-homed site initiates communication with a peer host, it will perform a DNS query sending the peer's FQDN. A DNS Application Level Gateway (DNS ALG) [58] is defined in the p-shim6 box which processes the query and both AAA RR and ULID RR are queried for. When DNS replies to the query, the DNS ALG on the p-shim6 box only forwards the CMULA to the host. P-shim6 box stores the PA address information returned in the DNS reply message. When the host sends packet addressed to CMULA of peer, it is intercepted by p-shim6 box. The packet is retained by p-shim6 box which in turn attempts to establish a context with the peer. The peer can either be a host supporting SHIM6 or it could be behind another p-shim6 box. The PA addresses are set as locators while CMULAs are the ULIDs. Once the context is established between local p-shim6 box and the peer, the data packet is forwarded to the peer containing shim6 payload extension header. This process is continued until there is communication between host and peer. When the communication stops the p-shim6 box discards the associated shim6 state.

The hosts only have provider independent (non routable) ULIDs (CMULAs). Hence, an end site obtains CMULA block that is independent of its ISPs and will use these CMULAs as ULIDs for SHIM6 context. The CMULAs are globally unique and are independent of location of the network to which they are assigned. They are permanently allocated to the end site. In order to prevent an external peer from using CMULAs as routable addresses for non SHIM6 host in a multi-homed site, it is necessary to store CMULAs in a different DNS Resource Record (RR). Hence, a new DNS RR is to be defined for storing ULIDs. So, the DNS of a multi-homed site contains routable addresses in AAA RR and CMULAs in the new ULID RR.

When there is no locator information, a reverse tree of DNS is used to obtain locator set associated with a particular CMULA. When a reverse DNS query is performed for a CMULA, the locator information is added in the additional information field of DNS reply. P-SHIM6 process flow is explained with the help of network architecture of Figure 6.1.

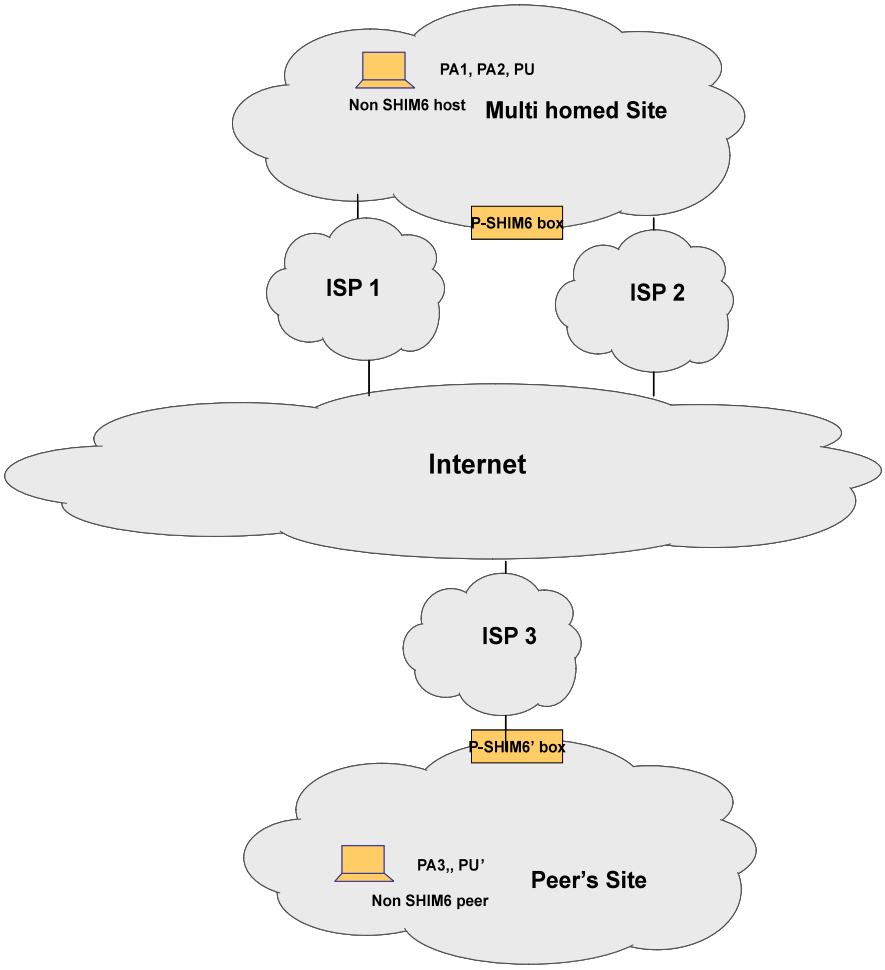

Figure 6-1: p-shim6 Network Architecture

In the Figure a multi-homed site containing a non SHIM6 host is served by ISPs 1 and 2. Each of these ISPs delegates a PA address block to the multi-homed site with prefixes PA1 and PA2 respectively. A CMULA block (prefix PU) is also delegated to the multi-homed site so that they can be used as ULIDs for shim6 communications. Similarly a non SHIM6 peer is located in another site which is served by ISP3. The PA address block allocated has prefix PA3. The CMULA block prefix allocated to the peer's site is PU'. The host within the multi-homed site has p-shim6 box as the DNS server. Hence, all the DNS queries are forwarded to it.

When the host in multi-homed site wants to communicate with a peer, it sends a DNS query to its server (p-shim6 box) containing peer's FQDN. The p-shim6 box performs DNS query for peer's FQDN. If the query returns a ULID RR along with AAA records, the p-shim6 box stores information about ULID and any additional locators that the peer has. It forwards a single AAA RR containing peer's CMULA in the reply message to host. P-shim6 box in the multi-homed can now initiates a four-way handshake to establish shim6 context with p-shim6 box serving the peer. The host then sends packets to the peer with destination address as peer's CMULA. The packets will be routed to p-shim6 box serving the multi-homed site. Once p-shim6 box receives such packets, it will check if a context exists for ULID pair in the packet. If there is an existing context, p-shim6 will use the context to process the packets. If no shim6 context exists, p-shim6 box would perform a DNS reverse lookup on the destination CMULA. Once the locator information corresponding to the destination CMULA is obtained a shim6 context establishment is performed. When the context is established, it is used to process packets. At the destination the p-shim6 box at peer site would receive the packets and check if there is an existing context. If the context exists, it will replace the locators with the associated identifiers and forward packets to the peer. If a shim6 context doesn't exist for the packets received, it will initiate context recovery procedure be sending R1bis message back to the source p-shim6 box. As long as host and peer keep communicating, p-shim6 boxes translate between ULIDs and locator pairs. When communication is finished, p-shim6 boxes will discard the shim6 context.

P-shim6 mechanism is an extension to the base SHIM6 protocol. Hence, it only deals with cases where site is multi-homed through multiple ISPs advertising their prefixes. Need for address switch is much less frequent in such situations. Contrary to this, in multi-homed host mobility environments need for address change is much more frequent. Hence, a mechanism needs to be defined which tackles the problem of supporting legacy hosts in such multi-homed mobile environments.

6.3 Proposed Mechanism

In the previous Chapters we proposed an idea MNS-MIP6 which enables MIPv6 capable MN to use MNS signaling to gain multi-homing benefits i.e. better reliability and load sharing. In addition, it was shown that MNS-MIP6 could be used in heterogeneous network scenarios to provide seamless handover among different network. MNS sub layer is added within host's protocol stack.

In MNS-MIP6 systems, both ends of communication need to support MNS signaling. As MNS-MIP6 would be seen as an optional service available to Internet users, not all the users would be expected to support it especially in early stages of deployment. Hence, a mechanism is needed to allow an MNS-MIP6 capable MN to communicate with legacy hosts not supporting MNS. In this section, a mechanism is introduced through which such communication is possible.

Middle box known as Proxy MNS box is introduced in legacy node's network. MNS signaling takes place between this PMNS box and MNS-MIP6 supported MN.

When MNS-MIP6 supported MN initiates communication with a non-MNS CN, it performs a DNS query and receives the globally routable IP address of CN. MN then attempts to establish context with CN by sending I1 message. When CN is a legacy node not supporting MNS, it will discard the I1 message from MN. MN then makes a second DNS query to know if CN is behind a PMNS box. For this purpose a new Resource Record (RR) is created in DNS. If CN is in fact behind a PMNS box, DNS sends the IP address of PMNS box. MN then establishes context with PMNS box. CN's IP address is set as ULID for the context. Context establishment messages are exchanged between MN and PMNS box. The address used is of PMNS box rather than of CN for the context establishment. After context is established, all communication to and from CN is carried out through PMNS box. Routing Header is used to send packets to CN's address via PMNS box [75]. We further explain this mechanism in later sections. After the context establishment, PMNS box sends msenable message to CN which indicates that all packets sent to MN have to pass through PMNS box.

When a non MNS CN initiates communication, it sends a DNS query for MN's IP address. DNS replies to the request and communication is started. However, when MN wants to establish a context with CN, it first sends an I1 message to CN. As CN would discard the message, MN sends a second DNS query to check whether CN is behind a PMNS box. If MN receives the IP address of PMNS box, a context is established. Otherwise, normal communication takes place between MN and CN without MNS-MIP6 support.

Through this mechanism multiple communication paths exist between multi-homed MNS-MIP6 capable MN and a non MNS

CN. When there is failure on the primary path, communication can be switched to a different path without disrupting traffic. Failures are detected and overcome by using the M-REAP protocol explained in the Chapter 3. Load can also be shared according to application profiles or user preferences among MN's different interfaces. Hence, by introducing PMNS box in non MNS CN's network all the benefits of MNS-MIP6 detailed in the previous chapters are realized.

6.3.1 Components

In order to run PMNS-MIP6 system, following components are required:

Psb-address:

When MN performs a DNS query for PMNS box in CN's network, the address of PMNS box is returned. This address is called Psb-address. After performing the DNS lookup, MNS-MIP6 enabled MN establishes a context with PMNS box. The context establishment messages are sent to and received from PMNS box through the Psb-address.

msenable-message:

When context is established between MNS-MIP6 enabled MN and PMNS box, msenable message is sent to CN. Purpose of this message is to inform CN that all the communication with MN has to be carried out via PMNS box. After receiving msenable message, CN sends data packets to MN via PMNS box by using routing header.

PMNS box:

PMNS box is introduced at the edge of a network where non MNS CN is located. Its main purpose is to act as a proxy for CN when communicating with MNS-MIP6 enabled MN. PMNS-

MIP6 functionality could be obtained by introducing a stand alone box at the edge of a network or could be embedded within an edge router. If CN is also a mobile device supporting MIPv6, the PMNS-MIP6 functionality could be embedded in CN's HA. After context is established between MN and PMNS box, all communication between MN and CN is carried via PMNS box.

DNS Component:

The mechanism requires a new Resource Record (RR) to be defined in DNS. Semantics of a DNS RR is given in Figure 6-2 [59]. A new TYPE field has to be defined for PMNS box. As type field has to be represented by two octet value, we define a field PSX with octet value 19. The name of this resource record is PSB. The class is defined as Internet (IN). The TTL is set to 0 value. RDLENGTH field is set to 128. And RDATA field contains the IP address of PMNS box which is 128 bits long. The DNS procedure is further explained in a later section.

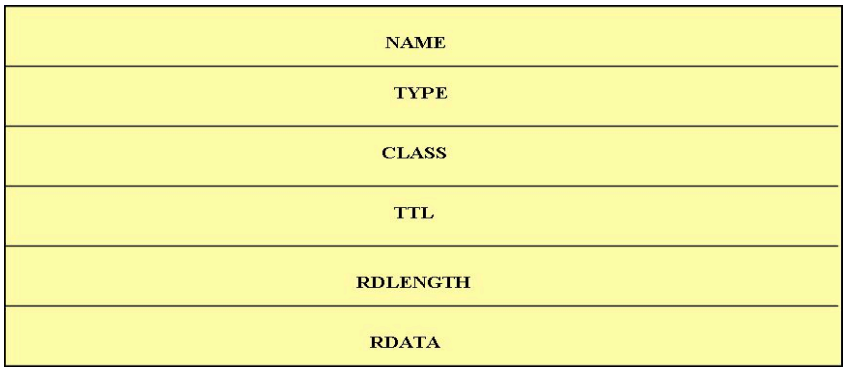

Figure 6-2: DNS RR Format

Routing header is used by IPv6 source to indicate a list of intermediate nodes that a packet has to go through to get to its destination. Once a context is established between MNS-

MIP6 enabled MN and PMNS box, all the data traffic between MN and CN has to go through PMNS box. PMNS box sends msenable message to CN after which CN appends a routing header to all the packets destined for MN. In the reverse direction, MN appends routing header to all the packets destined for CN.

The format for routing header is given in Figure 6-3. The Next Header value is set to 59 indicating no next header. The Message type is 0. The 8-bit Hdr Ext Len field contains the length of the routing header in 8-octet units not including the first 8 octets. In our case, the Hdr Ext Len field is set to 2 as there is only one intermediate node i.e. PS-MIP6 box. Segment left option is to indicate how many intermediate nodes the packet has to traverse. At source, the segment left value is set to 1. When the packet arrives at PMNS box, the segment left value is decremented to 0. The reserved field is set to 0. The 24-bit strict/loose map field is a mask which indicates how each intermediate address in the packet is to be treated. If the bit for a particular address is set to 0, it indicates that an address has to be treated loosely, if its 1 the address has to be treated strictly. In order to treat an address in a strict way, a node which receives the packet checks that the address belongs to an adjacent node and delivers the packet on the interface associated with that adjacent node. If the node is not adjacent, the packet is discarded. If the field indicates that an address must be treated in a loose way, the node examines its routing tables and routes the packet to the address. We set the field as 0 to indicate a loose treatment.

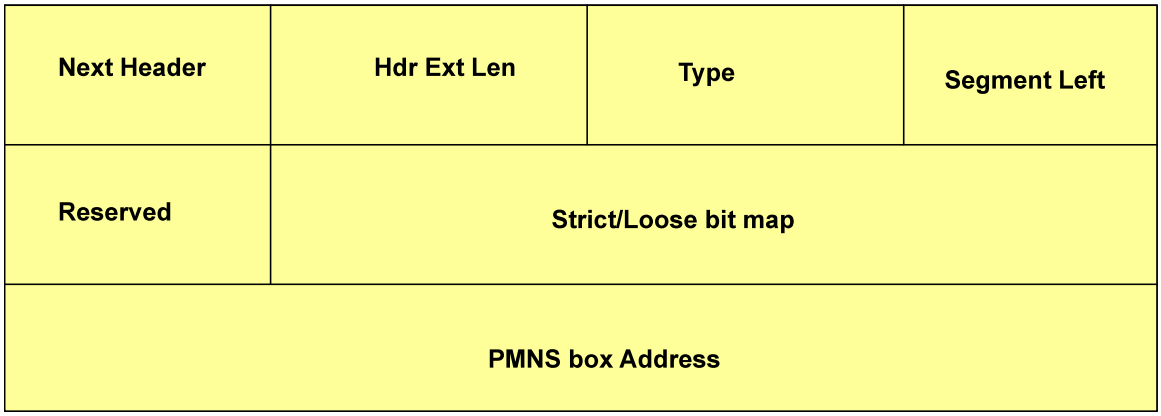

Figure 6-3: Routing Header Format

6.3.2 Packet Format

The mechanism introduces a msenable message. The message format is given in Figure 6-4.

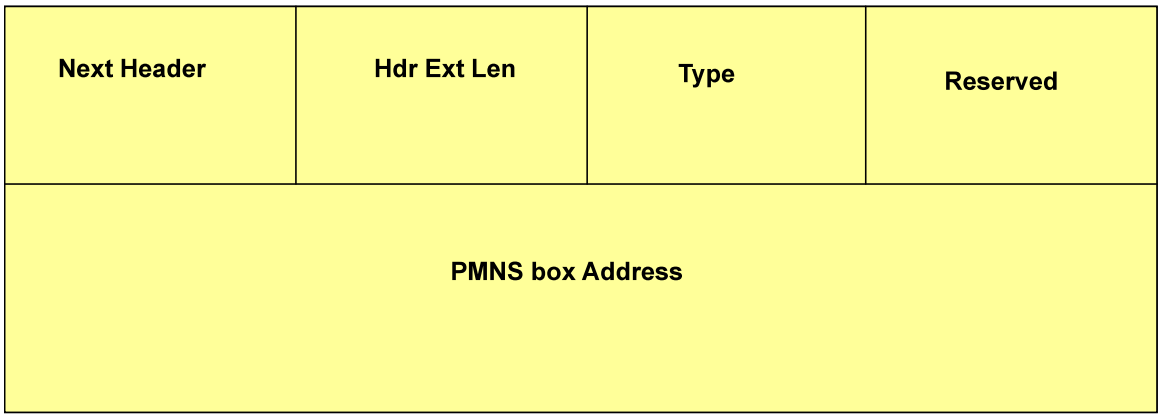

Figure 6-4: msenable packet format

Next Header value is set to 59 indicating no next header. The Hdr Ext Len is 2. Type is set to 0 and reserved field is also 0. msenable message contains the 128-bit IPv6 address of PMNS box.

6.3.3 Message Flow

Figure 6-5 gives the message flow for MNS-MIP6 locator switch when PMNS box exists in CN's network.

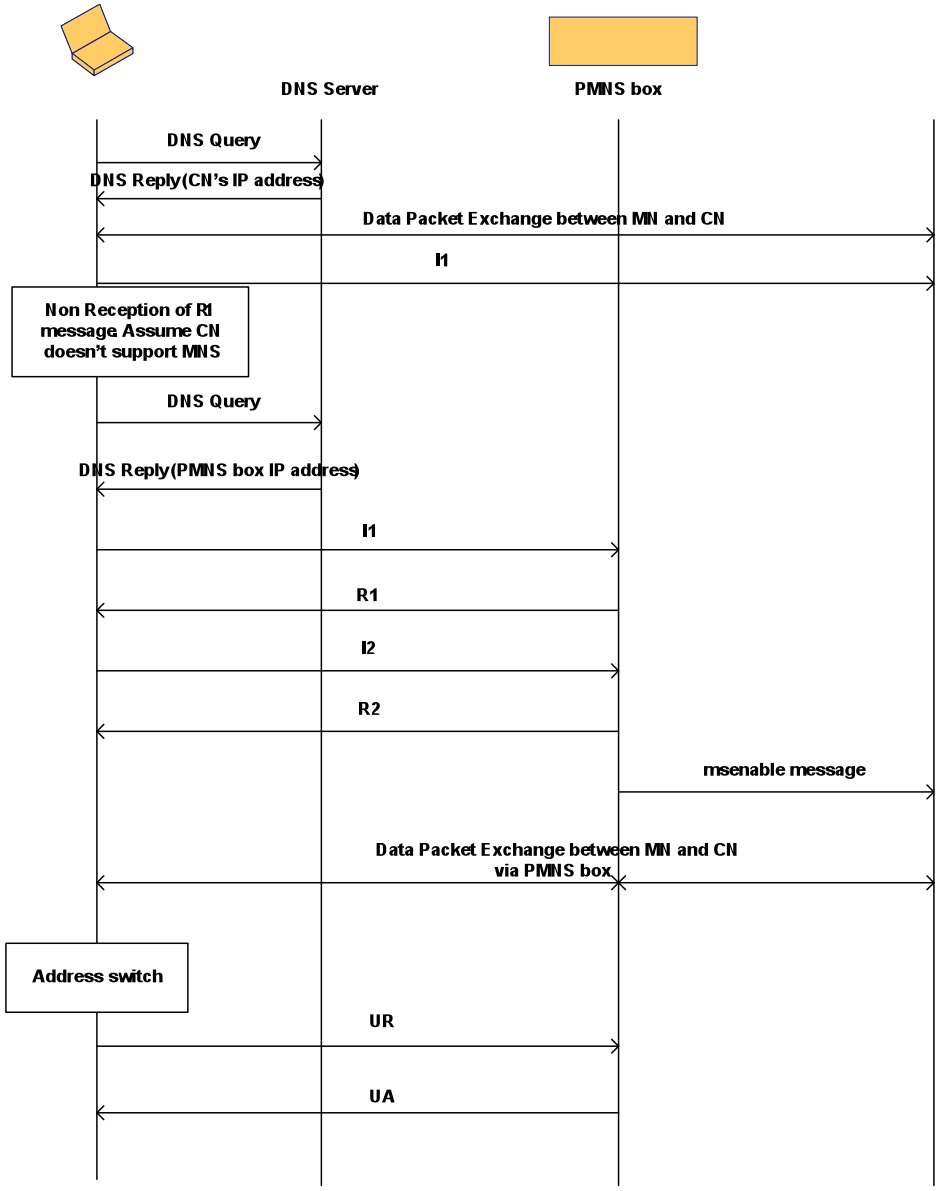

Figure 6-5: PMNS-MIP6 Signaling

Initially, MN establishes communication with CN using CN's IP address. As mentioned in the previous section, when MNS-MIP6 enabled MN makes a DNS query for CN it receives its IP address. After the initial communication, MN attempts to establish context with CN. MN sends I1 message to CN. However, non MNS CN doesn't recognize the message and discards it. MN waits for R1 message until the time out expires. MN then performs a DNS lookup for whether CN is

behind a PMNS box. This DNS lookup is different from normal host lookup on the Internet. The PMNS box DNS lookup procedure is explained in a later section. Only when MN gets the IP address of PMNS box in reply to DNS query, it knows that CN is behind a PMNS box. MN establishes a context with PMNS box. The context establishment messages are exchanged with PMNS box using psb_address. This procedure is different from the one explained in Chapter 2 where context establishment messages were sent using source and destination ULIDs. ULID for CN is its IP address and is sent in the ULID option of I2 message. When PMNS box receives I2 message with ULID option set, it reads the IP address in ULID option and marks it as ULID for the context.

Context establishment messages have the same format as explained in Chapter 2. Once context is established between MN and PMNS box, msenable message is sent to CN. All subsequent communication between MN and CN takes place through PMNS box by using routing header option. However, no MNS payload extension header is appended on packets until there is a need to make locator switch.

In the context establishment phase, locator set consists of all the additional IP addresses of multi-homed MN. Switch can be made from the primary IP address to any of the locators. As explained in the previous chapters, reason for the switch could be reliability, load sharing, or mobility. The switch is made through UR/UA message exchange between MN and PMNS box

After the switch, all subsequent data packets exchanged between MN and PMNS box contain payload extension header. When receiving data packets from MN, PMNS box strips the MNS header, checks the context and forwards packets to CN.

In the reverse direction PMNS box receives packets from CN, appends the payload extension header and sends it to MN. The locators switch remains transparent to transport and upper layers.

6.3.4 Application Scenario and Workflow

A typical network scenario where PMNS box is used is given in Figure 6-6.

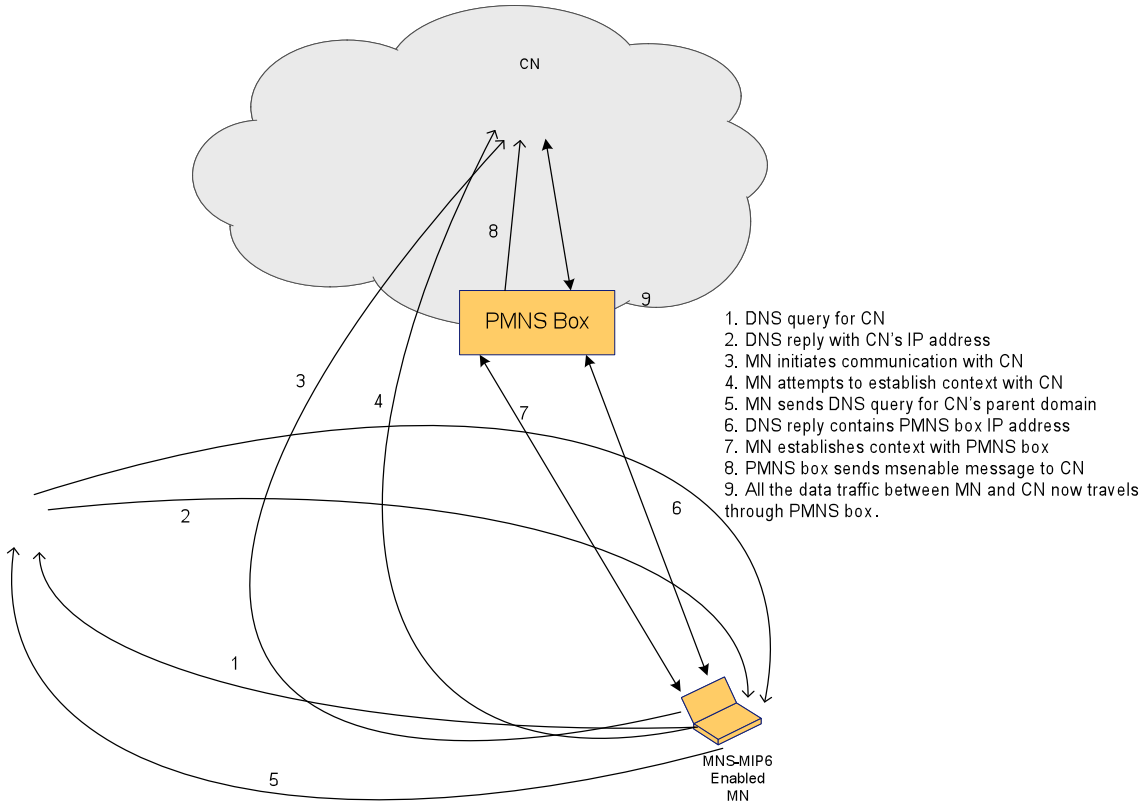

Figure 6-6: PMNS-MIP6 Application Scenario

When an MNS-MIP6 enabled MN communicates with a non MNS CN behind a PMNS box. The procedure flow is as follows:

- MN performs a DNS query for CN and gets the IP address.
- DNS replies with CN's IP address

- After MN initiates communication with CN, it attempts to establish a context with CN by sending I1 message.
- CN which doesn't support MNS signaling will discard the message.
- When MN doesn't receive R1 message back from CN, it sends a DNS query for any PMNS boxes in CN's parent domain.
- If CN is behind a PMNS box, IP address of the box is sent in DNS reply message. Otherwise, MN assumes that MNS is not supported in CN's network.
- MN establishes context with PMNS box in CN's network. The ULID pair for context is MN's HoA and CN's IP address.
- After context is established and PMNS box becomes aware of MN's additional locators, it sends msenable message to CN.
- The msenable message informs CN that all the traffic to and from MN has to pass through PMNS box.
- All the traffic between MN and CN now passes through PMNS box. This is done through routing header option.
- Switch is made from MN's one active IP address/locator to another through UR/UA message exchange between MN and PMNS box.
- Consequently all the data packets traveling from MN to CN contain MNS payload extension header.
- PMNS box receives packets from MN, strips MNS payload extension header and forwards the data packet to CN.

- In reverse direction, PMNS box intercepts data packets from CN destined for MN, appends MNS payload extension header, and sends them to MN.
- The context remains established between MN and PMNS box until communication between MN and CN continues.

As explained earlier, a new DNS RR is defined for PMNS box's IP address. .

PMNS box behaves as a MNS proxy for CN when communicating with MN. This way, all the benefits of MNS-MIP6 system mentioned in the previous Chapters namely, reliability, load sharing, and seamless mobility are realized.

MNS-MIP6 enabled MN could be communicating with a non MNS CN which is either mobile or stationary. In cases where CN is a mobile device supporting MIPv6, PMNS box can exist in CN's HN. It is reasonable to have MNS functionality in HA. Signaling is the same as shown in Figure 6-5.

There are thus two scenarios where PMNS box could be used.

Scenario I: Context is established between MNS-MIP6 enabled MN and PMNS box on the stationary CN's network.

Scenario II: Context is established between MNS-MIP6 enabled MN and HA/PMNS box on CN's HN.

The two scenarios are illustrated in Figure 6-7.

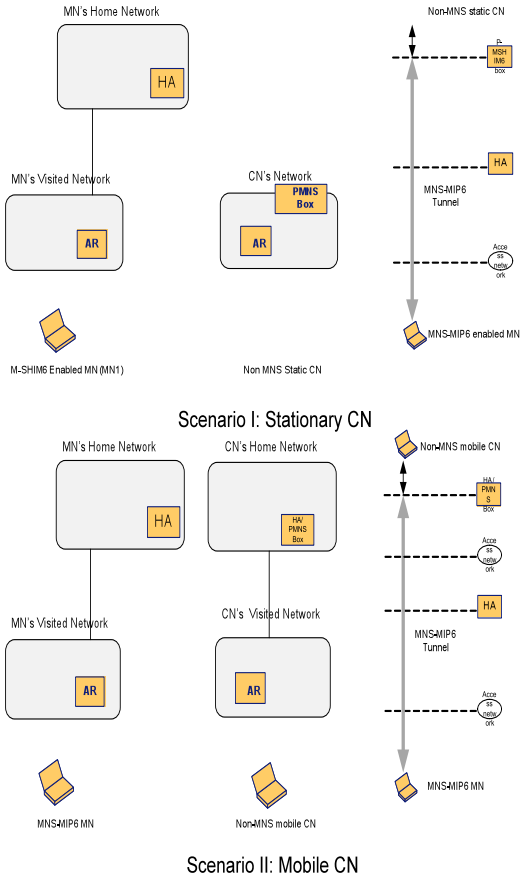

Figure 6-7: PMNS Coexistence Scenarios

In scenario I, CN is a stationary host on the Internet. The PMNS box is present in its network. The second scenario is a situation where CN is a mobile device. The PMNS functionality is present in HA of CN. During the context establishment phase, ULID pair is set as HoAs for MN and mobile CN. Mobile CN can be in one of two MIPv6 modes: BT or RO mode. In BT mode of operation the co-location of HA and PMNS box implies that not only traffic to CN has to go through HA/PMNS box but also traffic from CN to MN. In RO mode of operations, traffic between MN and CN has to again go through the HA/PMNS

box. This is done through routing header option. This can result in greater signaling delays. Hence, when RO mode of MIPv6 is running, there is a trade off between gaining multi-homing benefits and experiencing lower signaling delays.

6.3.5 DNS Lookup for PMNS Box

When MNS-MIP6 enabled MN wants to establish a context with non MNS CN, it sends an I1 message to CN. When CN receives the message it discards it as there is no MNS sub layer.

MN then performs a DNS query [60] to check whether CN is behind a PMNS box. As we explained earlier a new RR is defined in the DNS. The new type field is defined as PSX.

In order to explain the procedure we consider an example. In normal DNS procedure when a host wants to make DNS query for a peer's IP address on the Internet it sends the FQDN of peer. For example to make a query for peer "x" on a network "brunel.ac.uk" the FQDN would be "x.brunel.ac.uk". The DNS would check the IP address associated with this FQDN and send it in the DNS reply. Here, the parent network for peer "x" is "brunel.ac.uk".

In case MN is making a DNS query for PMNS boxes on the host "x's" network, it will send the FQDN "psx.brunel.ac.uk" in DNS query. DNS would check if any PMNS boxes exist in the network "brunel.ac.uk". If there is a PMNS box in the network, DNS would send IP address of it in reply message.

6.3.6 Receiving control messages at PMNS Box

When a context is established between MN and PMNS box, a MNS state is created both in MN and PMNS box. When a packet containing MNS payload extension header arrives at PMNS box, the extension header is stripped. The context tag is

checked for any existing context. When context tag matches with an existing context, the source and destination locators are replaced by source and destination ULIDs. The packet is consequently forwarded to CN.

6.3.7 Sending control messages from PMNS Box

After context is established between MN and PMNS box, all the data packets from CN to MN have to go through the PMNS box. After locator switch is made through UR/UA message exchange between MN and PMNS box, the packets traveling from CN to MN have to go through the PMNS box. MNS sub layer on PMNS box appends MNS payload extension header on packets it receives from CN for MN.

6.3.8 Location of PMNS Box

Location of PMNS Box in CN's network is of great importance. PMNS box has to communicate with both CN and MN. Being far away from the CN, the packet transmission delays could be very high and can cause significant disruption. We propose that PMNS box be located at the edge of CN's network. In our view this is the best possible location. When there is presence of multiple CNs simultaneously communicating with MN, the PMNS box would be ideally located.

6.4 Multi-homing Benefits through PMNS-MIP6

In the previous chapters we explained how, through MNS-MIP6 mechanism benefits of reliability, load sharing and seamless mobility can be obtained by MN equipped with multiple active interfaces when communicating with MNS enabled CN. Here, we analyze how the same benefits can be obtained when MN is communicating with a non MNS CN behind a PMNS box.

Reliability

When CN is behind a PMNS box, reliability is provided by M-REAP protocol explained in Chapter 3. Values for Keep-alive interval, Send timeout, Initial probe timeout, and maximum probe timeout are the same. However the M-REAP procedure is now run between MN and PMNS box rather than between MN and CN.

After the context is established between MN and PMNS box, failure can be detected through M-REAP. After failure is detected, probe messages are sent using different source/destination locator pairs until a new working pair is found.

Load sharing

Again the procedure is similar to what is explained in Chapter 4. A Policy Engine is defined within MNS sub layer in MN. The Policy Engine takes inputs from different networks and based on application requirements and user preference a decision is made on which network/interface to use for communication. Note that since CN is behind a PMNS box, the UR is sent to PMNS box.

Seamless mobility

Seamless mobility is supported for multi-homed MN through link layer triggers as explained in Chapter 5. When MN is communicating with a CN behind PMNS box, the UR is sent to PMNS box rather than to CN itself. Rest of the procedure is the same except all the MNS signaling is between MN and PMNS box.

6.5 Chapter Summary

In this chapter we have presented a mechanism through which an MNS-MIP6 enabled MN can establish context with legacy CN not containing MNS sub layer. In the research community there has been a lot of mention of the need for a mechanism to provide multi-homing support to legacy hosts [61][62][63][64]. A PMNS box is introduced in CN's network. All the MNS signaling takes place between MN and the PMNS box. Once context is established between MN and PMNS box, msenable message is sent to CN and all the subsequent data packets between MN and CN have to travel through the box.

By introducing the PMNS box, all benefits of MNS-MIP6 system described in earlier chapters are obtained. There is no added complexity to the Internet infrastructure. Only some modification is required at edge routers or HAs.

The M-REAP mechanism is used to detect any failures in the path between MN and PMNS box. Also, Policy Engine described in Chapter 4 can be used to share load between MN's different interfaces. Seamless mobility is also supported in the same way explained in Chapter 5.

Chapter 7

7 Conclusion and Future Works

This chapter describes the main conclusion of this thesis. Future work in this area is also described towards the end of this chapter.

7.1 Concluding Remarks

This thesis studies the multi-homing techniques in mobility networks. Keeping in view the various benefits that multi-homing can provide in mobile environments, the existing techniques/mechanisms are analyzed. It is concluded that, although the existing techniques have some desirable features, they fall short in many important aspects.

A new mechanism to support multi-homing in mobility networks is proposed. The mechanism is called Multi Network Switching in MIPv6 or MNS-MIP6. A clean architecture which separates multi-homing from mobility is presented where MN having multiple communication paths between itself and CN can use them to gain multi-homing benefits. Communication between MN and CN is initiated through normal DHCP procedures [65]. The switching from one interface/communication path to another is done through MNS signaling described in the thesis. This ensures transparency to layers above IP. Hence, the existing Internet applications do not require any modifications.

A new technique is proposed to improve reliability in multi-homed mobile environments. The technique uses MNS-MIP6

architecture to switch from one interface/communication path to another in case of failures. The basis of this mechanism is a quick failure detection and recovery procedure. We call the procedure M-REAP. Reliability of communication between MN and CN depends on how quickly failures can be detected and recovered from. A performance analysis is conducted which compares our proposed M-REAP mechanism with the existing MIPv6 failure detection and recovery techniques. Through both mathematical and simulation analysis, it is concluded that our proposed mechanism outperforms MIPv6.

A multi-homed MN should be able to use multiple communication paths to share the traffic load. We proposed a new network selection mechanism in heterogeneous networks environment. A Policy Engine is defined which chooses a particular network according to the application profile and user preference. The decision of which network to choose for a particular application traffic is taken by comparing the parameters of cost, available bandwidth, latency and SNR from the available networks. The switch is made through MNS signaling. The proposed load sharing mechanism is tested by running simulations using different application traffic.

Another contribution of this thesis is that a new mechanism is proposed to ensure seamless mobility in heterogeneous network environment where MN is multi-homed. Layer 2 triggers are used to anticipate a handover and MNS signaling is used to make the actual switch. This results in minimum disruption to on-going communication during handovers. The proposed seamless handover mechanism is compared with the most promising mobility enhancement of MIPv6, namely FMIPV6. The results conclude that our proposed mechanism gives better performance than FMIPV6 [66].

Thesis also tackles scenarios where CN does not support MNS signaling. In such scenarios it is proposed to introduce middle boxes at the edge of CN networks. These boxes are called PMNS boxes. They act as proxies for CN when communicating with MN. This way, benefits of multi-homing can be attained in scenarios where legacy non MNS hosts exist.

7.2 Future Works

Further research can be pursued building on the work presented in this thesis. Following are some of the areas where future work can be carried out:

- To further analyze the MNS-MIP6 architecture by building a test bed and running different scenarios.
- The work on multi-homing support in mobile environments needs to be standardized. Standardization bodies should be consulted to evaluate the MNS-MIP6 architecture. IETF is a good forum for that.
- M-REAP mechanism can work as a stand alone failure detection and recovery procedure. There is a scope of employing the procedure in non-multi-homed environments and testing its performance.
- Various network load sharing algorithms have been presented in the research community. These algorithms can work along with MNS switching mechanism to provide load sharing capabilities. An analysis can be carried out to compare these algorithms.
- Our proposed seamless mobility mechanism is supported by layer 2 triggers. These triggers indicate SNR on a particular interface. It is useful to add other triggers to

assist in handover procedures. One such trigger can be congestion related i.e. indicate the congestion on a particular network/interface.

Bibliography

[1] N. Montavont, R. Wakikawa, T. Ernst, C. Ng, K. Kuladinithi,"Analysisof Multi-homing in Mobile IPv6", Internet Draft (work in progress), IETF, October 2005.

[2] Jon. Postel et al, "Internet Protocol Version 4 Specification", RFC791, IETF, September 1981.

[3] S. Deering et al, "Internet Protocol Version 6 Specification", RFC 2460, IETF, December 1998.

[4] D. Johnson et al, "Mobility Support in IPv6",RFC 3775,IETF,June'04

[5] IETF: http://www.ietf.org/multi6/

[6] IETF: http://www.ietf.org/html.charters/hip-charter.html

[7] IETF: http://www.ietf.org/html.charters/tsvwg-charter.html

[8] IETF: http://www.ietf.org/html.charters/mext-charter.html

[9] IETF: http://www.ietf.org/html.charters/shim6-charter.html

[10] R. Moskowitz, P. Nikander, "Host Identity Protocol (HIP) Architecture", RFC 4423, IETF, May 2006.

[11] P. Nikander, T. Henderson, C. Vogt, J. Arko, "End-Host Mobility and Multihoming with the Host Identity Protocol", RFC 5206, IETF, April 2008.

[12] P. Paakkonen,P. Salmela, et al, "Performance Analysis of HIP-based mobility and triggering", Proceedings of the World of Wireless, Mobile,and Multimedia Networks, WoWMoM June 2008, Pages 1-9.

[13] R. Stewart, "Stream Control Transmission Protocol", RFC 4960, IETF, September 2007.

[14] Vinton. Cerf, Yogen. Dalal, Carl. Sunshine "Specification of Internet Transmission Control Protocol", RFC 675, IETF, December1974

[15] J. Postel, "User Datagram Protocol", RFC 768, IETF, August 1980.

[16] Ma. Li, F.R. Yu, V.C.M. Leung, "Performance Improvement of

Mobile SCTP in Integrated Heterogeneous Wireless Networks", IEEE Transaction of Wireless Communications, Issue 10. October 2007, Pages 3567-3577.

[17] S. J. Vaughan-Nichols, "Mobile IPv6 and the future of Wireless Internet Access", IEEE Comp., Volume 36, no. 2, February 2003, pp. 18-20.

[18] R. Wakikawa, V. Devarapalli, G. Tsirtsis, et al, "Multiple Care-of Addresses Registration", Internet draft (work in progress), IETF, May 2009.

[19] J. Palet, M. Diaz, C. Olvera et al, "Analysis of IPv6 Multihoming Scenarios", IETF Internet Draft (work in progress), July 2004.

[20] E. Nordmark, "Shim6: Level 3 Multihoming Shim Protocol for IPv6",IETF Internet Draft (work in progress), February 2009.

[21] P. Savola, "IPv6 Site Multihoming Using a Host Based Shim Layer", Proceedings of International Conference on Networking, International Conference on Systems, and International Conference on Mobile Communications and Learning Technologies, ICNICONSMCL, Morne, Mauritius, April 2006.

[22] M. Bugnulo, "Hash Based Addresses (HBA)", Internet Draft (work in progress), IETF, December 2007.

[23] T. Aura, "Cryptographically Generated Addresses (CGA)", RFC 3972, IETF, March 2005.

[24] Bagnulo, M, Garcia-Martinez A., Azcorra A., "IPv6 Multihoming Support In the Mobile Internet", IEEE Wireless Communications Journal, Volume 14, Issue 5. October 2007. pp. 92-98.

[25] Le. Deguang, Lei Jun, Fu. Xiaoming, "A New Decentralized Mobility Management Service Architecture for IPv6-based Networks", Proceedings of Third ACM International Workshop on Wireless Multimedia Networking and Performance Modeling WMuNeP'07, Crete Island Greece. October 2007.

[26] IST Project ENABLE, http://www.ist-enable.org/

[27] W. Dave, E. Philip, B. Louise, "IP for 3G", Addison-Wesley, 2002.

[28] T. Ernst, N. Montavont, R. Wakikawa, et al, "Motivations and Scenarios for Using Multiple Interfaces and Global Addresses", Internet Draft (work in progress), IETF, May 2008.

[29] H. Soliman, "Mobile IPv6: Mobility in Wireless Internet", Addison Wesley, 2004.

[30] J. Arko, I. van Beijnum, “Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming”, Internet draft (work in progress), IETF, June 2008.

[31] R. Caceres, L. Iftode, “Improving the performance of reliable transport protocols in mobile computing environments”, IEEE Journal on Selected Areas in Communications, 1995, pp. 850-857.

[32] X. Fu, H. Tschofenig, S. Thiruvengadam, Yao. Wenbing, “Enabling Mobile IPC6 in Operational Environments”, Proceedings of the 10th IFIP International Conference on Personal Wireless Communications (PWC 2005), Colmar, France, Aug 2005.

[33] Bjorn Chambless, Jim Binkley, “HARP-Home Agent Redundancy Protocol”, Internet draft (work in progress), IETF, October 2007.

[34] Yin-Fu Huang, Min-Hsiu Chuang, “Fault tolerance for home agent in mobile IP”, The International Journal of Computer and Telecommunications Networking, Volume 50, Issue 18, Pages 3686-3700, December 2006.

[35] J. Faizan, H. El-Rewini, M. Khalil, “VHARP: Virtual Home Agent Reliability Protocol for Mobile IPv6 based Networks”, Proceedings of IEEE International Conference on Wireless Networks, Communications and Mobile Computing, Maui, June 2005, pp. 1295-1300.

[36] Adnan K. Kiani, Shoaib Khan, Wenbing Yao, “SHIM6 Based Failure Detection and Recovery Mechanism in Multi-homed MIPv6 Networks”, Proceedings of Wireless World Research Forum, WWRF 17, Heildelberg Germany, November 2006.

[37] Prashant K. Wali, Pallapa Venkataram, “An Effective Seamless Connectivity Scheme for Ubiquitous Applications”, Proceedings of the 6th International Conference on Advances in Mobile Computing and Multimedia (MoMM’08), Linz, Austria, November 2008. pp. 307-312.

[38] Chen. Wen-Tsuen, Shu. Yen-Yuan, “Active Application Oriented Vertical Handover in Next-Generation Wireless Networks”, Proceedings of IEEE Wireless Communications and Networking Conference, New Orleans. LA, March 2005, pp. 1383-1388.

[39] Kang. Tae-Hoon, Hong. Chung-Pyo, et al, “A Context-aware Handover Management for Seamless Connectivity in Ubiquitous Computing Environment”, Proceedings of The 2006 World Congress in Computer Science Computer Engineering, and Applied Computing”, Las Vegas, Nevada, June 2006.

[40] Lassoued. Imed, Bonnin. Jean-Marie, Hamouda. Zied Ben, Belghith.

Abdelfettah, “A Methodology for Evaluating Vertical Handover Decision Mechanisms”, Proceedings of IEEE Seventh International Conference on Networking ICN 2008”, Cancun, Mexico, April 2008, pp. 377-384.

[41] Koodli, et al, “Fast Handovers for Mobile IPv6”, RFC 4608, IETF, April 2006.

[42] H. Soliman et al, “Hierarchical Mobile IPv6 Mobility Management”, RFC 5380, IETF, October 2008.

[43] Ed. S Gundavelli, Lueng K. et al, “Proxy Mobile IPv6”, RFC 5213, IETF, August 2008.

[44] Q.B. Mussabbir, W.B. Yao, Zeyun Niu and X.M. Fu, “Optimized FMIPv6 using IEEE 802.21 MIH Services in Vehicular Networks”, Vehicular Technology, IEEE Transactions on Volume 56, Issue 6, Nov, 2007. pp. 3397-3407.

[45] Fu, Shaojian, M. Atiquzzaman, “Handover latency comparison of SIGMA, FMIPv6, HMIPv6, FHMIPv6”, Proceedings of IEEE Global Telecommunications Conference Globecom’05, St. Louis, MO. December 2005, pp. 3809-3813.

[46] R. Chakravoty, P. Vidales, L. Patanapongpibul, K. Subramanian, “On Inter-network Handover Performance using Mobile IPv6”, http://www.cl.cam.ac.uk/users/rc277/handovers.pdf.

[47] T. Pagtzis, R. Chkravorty, J. Crowcroft, et al, “Proactive mobile IPv6 for context-aware all-IP wireless access networks”, Proceedings of International Conference on Wireless Networks, Communications and Mobile Computing, Maui, June 2005. pp. 1017-1022.

[48] Dong. Ping, Zhang. Hongke, et al, “A network-based mobility management scheme for future Internet”, Elsevier Journal in Computer and Electrical Engineering, May 2009.

[49] C. Prehofer, N. Nafisi, Q. Wei, “A framework for Context-Aware Handover Decision”, Proceedings of IEEE PIMRC 2003, Beijing, China, September 2003.

[50] S. Balasubramaniam, J. Indulska, “Vertical Handover supporting Pervasive Computing in Future Wireless Networks”, Computer Communications, 27, 2004, pp. 708-719.

[51] Pekka. Nikander, “The Host Identity Protocol (HIP): Bringing mobility, multi-homing, and baseline security together”, Third International Conference on Security and Privacy in Communications Networks and the Workshops SecureComm 2007, Nice, France. Sept 2007, pp. 518-519.

[52] Andrei Gurtov, “Host Identity protocol (HIP): Towards the Secure Mobile Internet”, Wiley Series in Communications Networking & Distributed Systems, June 2008.

[53] F. Teraoka, M. Ishiyama, M. Kunshi, A. Shionozaki, “LIN6: A Solution to Mobility and Multi-Homing in IPv6”, Internet draft (work in progress), IETF, August 2001.

[54] J. Ronan, S. Balasubramaniam, Kiani, Adnan K. Yao. Wenbing, “On the use of SHIM6 for mobility support in IMS networks”, Proceedings of the 4th International Conference on Test beds and research infrastructure for development of networks & communities, TRIDENTCOM 2008, Innsbruck Austria.

[55] Adnan K.Kiani, Khan. S. Yao. Wenbing, “A Novel Mechanism to Support Session Survivability in Heterogeneous MIPv6 Environment”, 2nd International Conference on Emerging Technologies, IEEE-ICET, Peshawar Pakistan, November 2006.

[56] G. Bajko, H. Tschofenig, “Firewall friendly Return-Routability Test (RRT) for Mobile IPv6”, Internet draft (work in progress), August 2008.

[57] M.Bagnulo, “Proxy Shim6 (P-Shim6)”, Internet draft (work in progress), IETF, February 2008.

[58] Fred Halsall, “Multimedia Communications-Applications, Networks, Protocols and Standards”, Addison-Wesley Press, 2001.

[59] C. Everhart, L. Mamakos, R. Ullmann, P. Mockapetris, “New DNS RR Definitions“, RFC 1183, IETF, October 1990.

[60] J. Klensin, “Role of the Domain Name System (DNS)”, RFC 3467, IETF, February 2003.

[61] Bates, T. Rekhter, Y., “Scalable Support for Multihomed Multi-provider Connectivity”, RFC 2260, IETF, January 1998.

[62] Ohta, M. “The Architecture of End to End Multihoming”, IETF Internet Draft (work in progress), July 2001.

[63] Huitema, C. Draves, R. “Host-Centric IPv6 Multihoming”, IETF Internet Draft (work in progress), June 2002.

[64] Narten, T., Nordmark, E., and W. Simpson, “Neighbour Discovery for IP Version 6 (IPv6)”, RFC 2461, December 1998.

[65] Droms, R., “Dynamic Host Configuration Protocol for IPv6 (DHCPv6)”, IETF Internet Draft (work in progress), November 2002.

[66] Ivov, E., Noel, T., "An Experimental Performance Evaluation of the IETF FMIPv6 Protocol over IEEE 802.11 WLANs", Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'06), pp. 568-574.

[67] OPNET Modeler Documentation.

[68] OPNET Support Center, www.opnet.com/support

[69] OPNET FAQs http://enterprise16.opnet.com/4dcgi/FAQ_SEARCH

[70] Montavont, N. and T. Noei, "Handover Management for Mobile Nodes In IPv6 Networks", IEEE Communication Magazine, 40(8): pp38-43, 2002.

[71] J. D. Solomon, "Mobile IP, The Internet Unplugged", Prentice Hall Series, 1998.

[72] Roe, M., Aura, T., O'Shea, G. and J. Arkko, "Authentication of Mobile IPv6 Binding Updates and Acknowledgements", IETF Internet Draft (work in progress), March 2002.

[73] Patel, A. Leung, K., Khalil, M., et al "Authentication Protocol for Mobile IPv6", RFC 4285, IETF, January 2006.

[74] E. Nordmark, "Securing MIPv6 BUs using return routability", IETF Internet Draft (work in progress), November 2001.

[75] Conta, A., S. Deering, "Generic Packet Tunnelling in IPv6 Specification", RFC 2473, December 1998.

[76] Thomson, S., T. Narten, "IPv6 Stateless Address Autoconfiguration", IETF RFC 2462, December 1998.

[77] Narten, T., Nordmark, E., W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", IETF RFC 2461, December 1998.

[78] Faizan, J., El-Rewini, H., Khalil, M., "Efficient Dynamic Load Balancing for Multiple Home Agents in Mobile IPv6 based Networks", in Proceedings of IEEE Int'l Conference on Pervasive Services (ICPS 2005), Santorini Greece, July 11-14, 2005.

[79] Faizan, J., El-Rewini, H., Khalil, M., "Problem Statement: HA Reliability", IETF Internet Draft (work in progress), November 2003.

[80] Andrew S. Tanenbaum, "Computer Networks", Prentice Hall, 2003.

[81] T. Ernst, "Network Mobility Support Goals and Requirements", IETF Internet Draft (work in progress), November 2006.

[82] Quoitin, B., lannone, L., et al, “Evaluating the Benefits of Locator/Identifier Separation”, Proceedings of MobiARch(ACM Workshop), Kyoto Japan, August 2007.

[83] Iv, J., Ma, Y., Yoshizawa, S. “Intelligent Seamless Vertical Handover Algorithm for the next generation wireless networks”, Proceedings of the 1st International Conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications, Innsbruck Austria, 2008.

[84] Wei. Guozhi, Wei. Anne, Xu. Ke, Dupeyrat. Gerard. “Optimization of Mobile IPv6 Handover Performance Using E-HCF Method”, Proceedings of the Internation Conference on Computational Science, Beijing China, 2007.pp. 506-513.

Appendix

Publications

Following is the list of publications:

- Adnan K. Kiani, Qiang Ni, Wenbing Yao, "MNS-MIP6: A New Multi Network Switching Architecture for Future Heterogeneous Networks", To be submitted to Elsevier Journal, Computer Networks.

- Adnan K. Kiani, Shoaib Khan, Wenbing Yao, "SHIM6 Based Failure Detection and Recovery Mechanism in Multi homed MIPv6 Networks", Wireless World Research Forum, WWRF 17, November 2006, Heidelberg, Germany.

- Adnan K. Kiani, Shoaib Khan, Wenbing Yao, "A Novel Mechanism to Support Session Survivability in Heterogeneous MIPv6 Environment", 2nd International Conference on Emerging Technologies, IEEE-ICET, November, 2006, Peshawar Pakistan.

- Adnan K. Kiani, S.R. Chaudhry, Wenbing Yao, "An Analysis of Network Level Solutions for Mobile Multi homed Host", 11th National Aeronautical Conference, May 2005, Risalpur, Pakistan.

- John Ronan, Sasitharan Balasubramaniam, Adnan K. Kiani, Wenbing Yao, " On the use of SHIM6 for mobility support in IMS networks", Proceedings of the 4th International Conference on Test beds and research infrastructure for

development of networks & communities, TRIDENTCOM 2008, Innsbruck, Austria.

- S. Khan, Loo. J., Adnan. K. Kiani., Yao. W. "Home Agent management based on autonomic Computing" Submitted to Elsevier Journal, Computer Networks.

- S. Khan, Loo. J, Adnan. K. Kiani., Yao. W. "Testbed implementation of Secure FMIPv6" submitted to Elsevier Journal, Network Security

- S. Khan, Adnan K. Kiani, Cecelia. F, and Yao W. "Home Agent Load Balancing in Mobile IPv6 with Efficient Home Agent Failure Detection and Recovery", 2nd International Conference on Emerging Technologies, IEEE-ICET, November, 2006, Peshawar, Pakistan.