SWEDISH DEFENCE
RESEARCH AGENCY

FOI-R--0822--SE
Mars 2003
ISSN 1650-1942
Technical report

Pär Thorén

Interworking of tactical ad hoc and static IP-network

Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping
Sweden

SWEDISH DEFENCE RESEARCH AGENCY

Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping
Sweden

FOI-R--0822--SE

Mars 2003

ISSN 1650-1942

Technical report

Pär Thorén

Interworking of tactical ad hoc and static IP-network

Issuing organization
FOI – Swedish Defence Research Agency
Command and Control Systems
P.O. Box 1165
SE-581 11 Linköping
Sweden

Report number, ISRN
FOI-R--0822--SE

Report type
Technical report

Research area code
4. C4ISR

Month year
Mars 2003

Project no.
E7755

Customers code
5. Commissioned Research

Sub area code
41. C4I

Author/s (editor/s)
Pär Thorén

Project manager
Peter Johansson

Approved by
Christian Jönsson

Sponsoring agency
FMV

Scientifically and technically responsible
Jan Nilsson

Report title
Interworking of tactical ad hoc and static IP network

Abstract (not more than 200 words)

In this report we investigate the relationship between host/network mobility and mobility within an ad hoc network to support seamless connectivity between a fixed core network infrastructure and an autonomous mobile tactical ad hoc network. There are several command and control systems within the Swedish defence to guide warfare operations and military efforts. By integrating these in the network centric warfare system, higher efficiency and information dominance can be achieved.

Mobile ad hoc network designs provide means for members to join and leave particular radio frequency subsystems as their position changes. The problem is that that the nodes (or sub-networks) should always be addressed with the same IP-address to be reachable. In this report we assume the protocol Mobile IPv6 to be used when meeting the goals of this integrated architecture.

Five tactical scenarios have been studied analytically and the problems and the effects on the network layer have been defined when the ad hoc network have been moving and changing access points to the fixed network. The conclusions were that using Mobile IPv6 together with Ad hoc On Demand Vector routing protocol is not enough to manage the access network in a tactical scenario. In this report we introduce a mobility management model that can provide seamless traffic management and connectivity to host applications in the network centric warfare system.

Keywords
Ad hoc network, Mobile IP, IPv6

Further bibliographic information

Language English

ISSN 1650-1942

Pages 59 p.

Price acc. to pricelist

Utgivare Totalförsvarets Forskningsinstitut - FOI Ledningssystem Box 1165 581 11 Linköping	**Rapportnummer, ISRN** FOI-R--0822--SE	**Klassificering** Teknisk rapport
	Forskningsområde 4. Spaning och ledning	
	Månad, år Mars 2003	**Projektnummer** E7755
	Verksamhetsgren 5. Uppdragsfinansierad forskning	
	Delområde 41. Ledning med samband och telekom och IT-system	
Författare/redaktör Pär Thorén	**Projektledare** Peter Johansson	
	Godkänd av Christian Jönsson	
	Uppdragsgivare/kundbeteckning FMV	
	Tekniskt och/eller vetenskapligt ansvarig Jan Nilsson	

Rapportens titel (i översättning)

Samverkan mellan taktiskt ad hoc-nät och fast IP-nät

Sammanfattning (högst 200 ord)

I den här rapporten har vi studerat förhållandet mellan nätverksmobilitet samt mobilitet inom ett ad hoc-nät för att stödja sömlös kommunikation mellan ett fast nät och ett autonomt rörligt taktiskt ad hoc-nät. Inom det svenska försvaret finns det flera olika ledningssystem för att leda operationer och övningar. Genom att integrera dessa i det nätverksbaserade försvaret kan högre effektivitet och bättre information uppnås.

I mobila ad hoc-nät kan noder tillkomma och försvinna när positioner förändras. Problemet är man vill att noderna (eller delnäten) alltid ska kunna nås på samma IP-adress. I den här rapporten har vi antagit att Mobile IPv6 används i i näten för att kunna uppnå målen.

Fem taktiska scenarier har studerats analytiskt och problemen och effekterna på nätverkslagret har identifierats då ad hoc-nätet rör sig och uppkopplingspunkterna till det fasta nätet ändras. Slutsatserna är att Mobil IPv6 tillsammans med routingprotokollet AODV (ad hoc on demand vector) inte är tillräckligt för att klara av samverkan mellan det fasta nätet och ad hoc-nätet. I rapporten introducerar vi en modell som hanterar mobilitet och kan ge sömlös kommunikation över en förbindelse mellan två applikationer i det nätverksbaserade försvaret.

Nyckelord

Ad hoc-nät, Mobil IP, IPv6

Övriga bibliografiska uppgifter	**Språk** Engelska
ISSN 1650-1942	**Antal sidor:** 59 s.
Distribution enligt missiv	**Pris: Enligt prislista**

1. Introduction

This master thesis will investigate the relationship between host/network mobility and mobility within an ad hoc network to support seamless connectivity between a fixed core network infrastructure and an autonomous mobile tactical ad hoc network. The focus is at global connectivity for nodes participating in a mobile tactical ad hoc network and not at a particular ad hoc routing protocol or core network routing protocol.

1.1 Background

There are several command and control systems within the Swedish defence to guide warfare operations and military efforts. They all have in common that they are adapted to different environments and requirements. The consequence is an overall segregated warfare command and control system divided into military areas of operation. Navy, Army and Air Force systems cannot interact with each other. The idea is that by integrating these different types of systems into one network centric warfare system, higher efficiency and information dominance can be achieved [1]. The different command and control systems should be able to support and interact with each other on one integrated centric level.

Utilisation of commercial off-the-shelf communications products to take advantage of existing economies of scale is important to make system design affordable. It is anticipated [2] that open standards and communication protocols, such as IP, will play a key role in meeting the goals of this integrated architecture. The next version of IP (IPv6) is currently being developed by the Internet community to support high performance networks, e.g. Gigabit Ethernet, Asynchronous Transfer Mode (ATM), etc, and at the same time still be efficient for low bandwidth networks, e.g. wireless networks [3]. In addition, the protocol standard provides a platform for new internet functionalities like autoconfiguration, security and mobility. This type of functionality and the built in support for extensions makes IPv6 a highly suitable and cost efficient standard to integrate different types of data links.

1.2 Problem overview

The definitions of most tactical information infrastructure include mobility in some form. Mobile ad hoc network designs provide means for members to join and leave particular radio frequency subsystems as their position changes. For example, as a platform moves out of the radio frequency line-of-sight range, it may switch from a typical line-of-sight radio frequency media such as the ultra-high frequency band to a long-haul radio frequency media such as high frequency, satellite communication or a civilian cellular based communication network such as the Universal Mobile Telecommunications System (UMTS).

It should be realised that mobility in the tactical setting is not limited to individual nodes moving about, but that, in some cases, entire sub-networks may change its point of attachment to an internet and thus its reachability in the topology, acting as a mobile network. This is the case with the tactical mobile ad hoc network described in chapter 2. This type of rapid movement should be seamless for upper layers and applications of all nodes in the ad hoc network. The nodes should always be addressable with the same IP-address from the internet by some mobility management scheme.

Given the scenarios in chapter 2 the mechanised battalion, acting as a mobile ad hoc network, may change access radio network as the battalion moves out of scope of a certain radio access network. An access network may also become unavailable due to hostile jamming and electronic warfare. This is a question of mobility management at the network layer even though the battalion maintains its geographical position. Redundant access networks may also be desirable. Having platforms, by some priority scheme, choosing the appropriate access network given a certain time and circumstance also require mobility management when it comes to addressing of the platforms.

When a platforms access network shifts access gateway also changes and the platform makes a movement in the network topology. Still the platform should always be addressable by the same address and be able to communicate with external nodes.

In some practical attempts made so far to visualise a tactical internet [4] (also referred to in chapter 1.4), mobility management is performed with routing protocols such as the Open Shortest Path First (OSPF) routing protocol. To solve the problem emerged from the tactical scenario described in chapter 2 a node mobility management scheme is approached in this master thesis. This approach could solve loss of aggregation efficiency [5] and addressing problems in the internet when very dynamic changes are made in the topology. In this master thesis different tactical scenarios alignment will be presented. The problems emerged from each scenario will be defined and solutions will be suggested.

1.3 Assumptions

Some assumptions need to be made in order to focus on the problems. In this master thesis it is assumed that a core network based on IPv6 exists. The core network is envisioned to be a high performance network. A more detailed description of the core network is given in chapter 2 when describing the main scenario. All nodes participating in the network are implementing an IPv6 standard. To this day the IPv6 final standard is not defined so some assumptions are being made in this master thesis when it comes to some parts of IPv6 concerning mobility.

The protocol architecture used in this core network is based on IP to form a homogenous network based on various heterogeneous networks. The end-user and application is not aware of the underlying architecture.

Figure 1.1 tries to envision the functions of different layers and the relationship between them. Each layer is transparent for the above layer. The application layer is a flat layer concerned about the end-to-end communication between applications. The Mobile IP layer handles mobility. The IP layer is concerned with routing. In Figure 1.1 below there are two domains on the IP layer; the ad hoc domain with its flat routing infrastructure and the core network with a hierarchical routing structure with route aggregation. On the data link layer a third domain is illustrated. This domain is the access network technology in use when the ad hoc network interworks with the core network. A description of ad hoc networks, IP and routing is given in chapter 3.

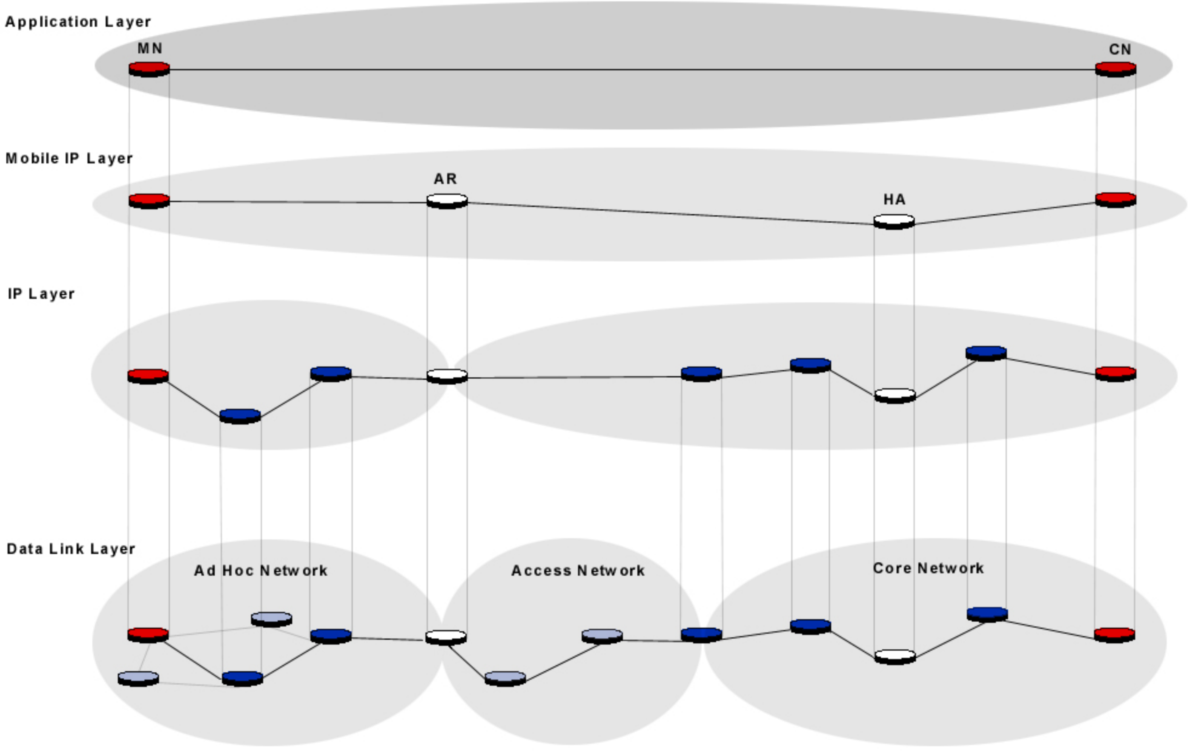


Figure 1.1: conceptional interlayer model

1.4 Related Work

Not much work has been done in the field of interworking between a tactical ad hoc network, such as a battalion and a fixed IP infrastructure. The sources of information for this master thesis in regards to related work can be divided into two categories, military and civilian source of information.

An example of a military model of a tactical internet (in this document referred to as the core network) has been illustrated in "Struktur Taktiskt internet" [4]. In this and other visions of a tactical internet the focus has been to describe a conceptional model of a homogenous network centric warfare system and the function that is provided by the system. The models often, more or less indirectly, include mobility management, ad hoc networks, advanced routing procedures and seamless connectivity. The goal is situations awareness and information dominance. But little work has been done on describing the interworking procedures necessary from a technical point of view. What is in reality required to achieve these goals?

The civilian sources of information used in this master thesis are mainly working drafts and request for comments published by Internet Engineering Task Force (IETF) groups. Some master thesis projects have been done in this area. In regards to related work, several publications ([6], [7]) that describe interworking between an ad hoc network and the Internet, have been found. These publications have in common that they are all focusing on a commercial implementation of the technology. Often an ad hoc network is described as a Personal Area Network where different hand held devices interworks with the global Internet through 3G or Wireless Local Area Network (WLAN) access technology.

1.5 Report Structure

This thesis consists of 8 chapters. A summary of the contents of the chapters and the appendixes is given below:

Chapter 2 This chapter gives an introduction to the overall alignment in a network centric warfare communication system. It should be realised that the scenario given, in relation to the assumptions made, is fictive and in some cases based on personal opinions. Further, the chapter describes five different specific tactical scenarios with events that affect the network topology and result in outlined problems related to interworking and seamless connectivity.

Chapter 3 In chapter 3 an introduction to the technology used in the tactical scenarios in chapter 2 is given. This chapter is intended to identify and only briefly introduce the reader of the general functions of the technology in use. For a more detailed description of each technology the reader is referred to the reference list.

Chapter 4 The chapter tries to give the reader a clear picture of the outlined problems related to interworking described in the five scenarios in chapter 2.

Chapter 5 In chapter 5, solutions to the defined problems are given. This chapter discusses various approaches to solution. The goal is to use the technology described in chapter 3 in the tactical scenario described in chapter 2 with modification to solve the problems outlined in chapter 4.

Chapter 6 In this chapter an evaluation is given to chapter 5, concerning the choice of technology and the tactical scenarios. Also other parameters such as security and traffic management are discussed.

Chapter 7 Various issues that elicited from this report are given in this chapter. This chapter intends to be a guideline for the future research that needs to be done in this area.

Chapter 8 Concludes the thesis.

References References to the source material used in this master thesis. The reader is referred to this appendix in the master thesis for a more detail description of the technology in use.

Glossary In the master thesis several jargons are used. This appendix is intended to be a dictionary for the technical language used and to clarify the meaning of the terminology.

2. Tactical scenarios

The core network in a network centric warfare system provides a backbone service for military platforms and personnel in order to exchange information. The core network is based on a high performance low cost fixed infrastructure where traditional routing mechanisms provides a hierarchical relationship between networks, forming an internet. Military platforms and personnel can attach to this core network in order to interact with the information available in the network. Military ad hoc networks attached to this core network are considered to act as stub networks from IP-layer point of view, i.e. no data is transported through the network, only to and from. This relationship is seen in Figure 2.1. The core network can be attached to the main global Internet and is then regarded as a stub network in relation to the Internet.

A military mobile platform that wishes to interoperate with the core network may desire to do so by any means available under a specific period of time. In the scenarios presented in this chapter a mechanised battalion [15] is forming an ad hoc network. Platforms in this autonomous wireless domain want to distribute situation awareness or any other kind of information to nodes on the core network. Warfare control platforms may also desire to send command information message to all or specific platforms in the battalion from anywhere in the core network.

All units in the battalion have communication interfaces to interact with each other and form an autonomous ad hoc network. Communication from one platform to another within this autonomous network is provided by a hop-by-hop scheme in an ad hoc fashion. There are several types of radio interfaces available in the battalion to use when interworking with the core network centric warfare system. There are also several access networks available (seen in Figure 2.1.).

The access networks available can vary depending on the current location and effort of the battalion. In urban areas civilian commercial and emergency infrastructures as the UMTS and TErrestrial Trunked RAdio (TETRA) communication system can be used. In other situations there may also be military on-demand access networks like TeleSystem9000 (TS9000) or Unmanned Aerial Vehicles (UAV) communication systems. The battalion may also be able to use North Atlantic Treaty Organization (NATO) infrastructures with satellite interfaces.

Since all platforms in the ad hoc network can interact with each other the platform that currently supply external access to the core network, for example using the TS9000 radio system, performs access router functionality to all other platforms. Platforms that desire to communicate with nodes on the core network use this access router as default. Data from nodes on the core network designated to platforms within the battalion is also delivered to the access router, which forwards the data to the ad hoc network.

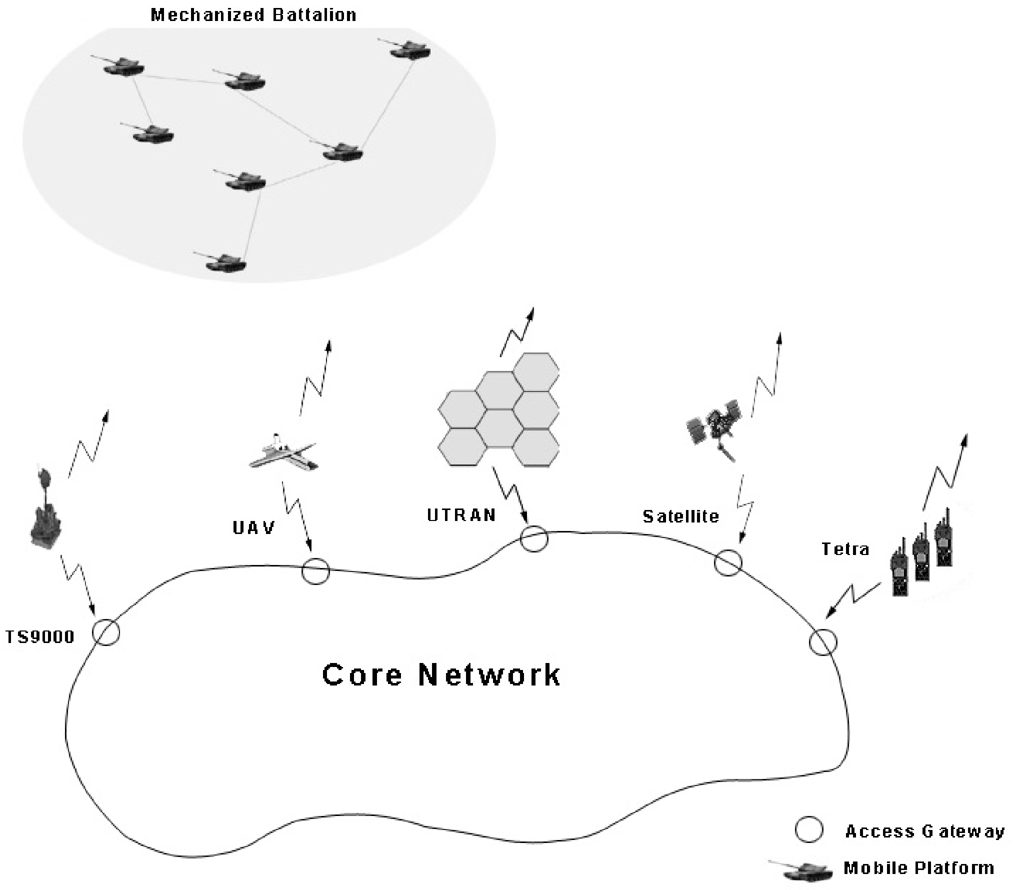


Figure 2.1: Mechanised battalion and access network availability

There can also be several platforms in the battalion acting as default access routers to the core network. The use of different types of available access networks is seamless for platforms and applications in the ad hoc network.

If the current default gateway platform is destroyed or the access network becomes unavailable due to enemy warfare or geographical position of the platform another platform with available interoperating interface can start to interwork with the core network. This platform takes over the default gateway service for the ad hoc network. The access network can be of any kind available, for instance an UAV.

All platforms in the battalion have one Domain Name Service (DNS) entry bound to an IP-address to uniquely identify itself in the network. A unit in a tank company can for instance have the following DNS entry:

tank_3.5th_comp.1st_bat.army.mil.se -> 3ffe:501:8:0:260:97ff:fe40

This tank is always, regardless current attachment to the core network or geographical position, addressable by this unique name and IP-address. Changes in the network topology are seamless for platforms in the battalion. All current data sessions between corresponding nodes in the core network and platforms in the battalion maintain active.

Below are five different scenario alignments. Each of the alignments results in changes in the network topology. The problems common for all alignments are defined in chapter 4. A more detailed problem description of the effect at the network layer and suggestions for solution to each scenario are described in chapter 5.

2.1 Scenario 1. Access network variation

The platform acting as default router for the rest of the battalion has two communication interfaces to interoperate with the core network. For example one UTRAN and one satellite interface. In this scenario it is assumed that the access network current in use is the UTRAN system.

The UTRAN system becomes unavailable due to enemy warfare. The default router uses the satellite interface to take over the communication to the core network.

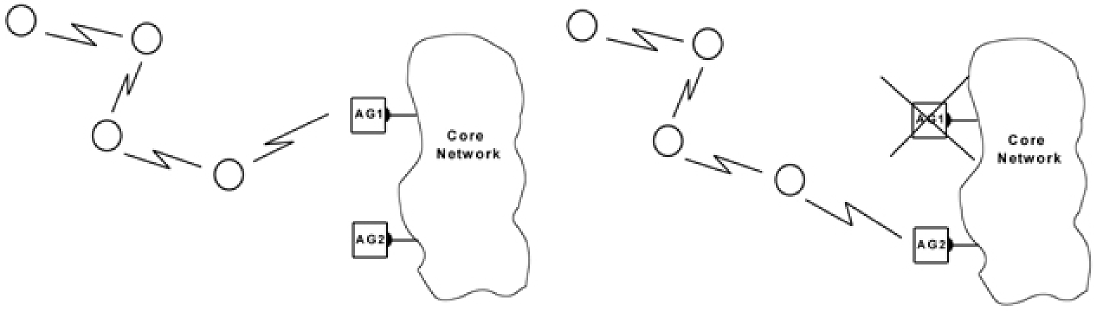


Figure 2.2: Change of access network

These changes in both network address topology and data link layer are seamless for platforms in the battalion. Ongoing data sessions between the core network and platforms in the ad hoc network maintain active.

2.2 Scenario 2. Access router variation

There are several platforms in the battalion capable of interoperating with the core network with different types of available radio interfaces on each platform.

The platform that current interoperates with the core network is destroyed and a new default router is needed for nodes in the battalion to communicate with the core network.

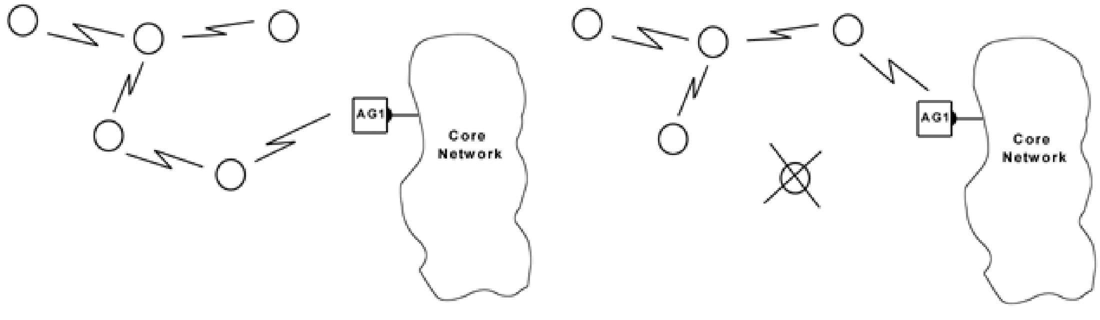


Figure 2.3: Change of access router

A platform establishes a new link and is selected as the new default router in the battalion. Platforms in the battalion update their routing tables with the new default router information.

2.3 Scenario 3. Ad hoc split

The battalion has one active default router to the core network. The router is using TS9000 as an access network.

A platform in the battalion acting as an intermediate node in the ad hoc network moves out of scope and loses connectivity to one of its two available neighbours. This results in an ad hoc network split.

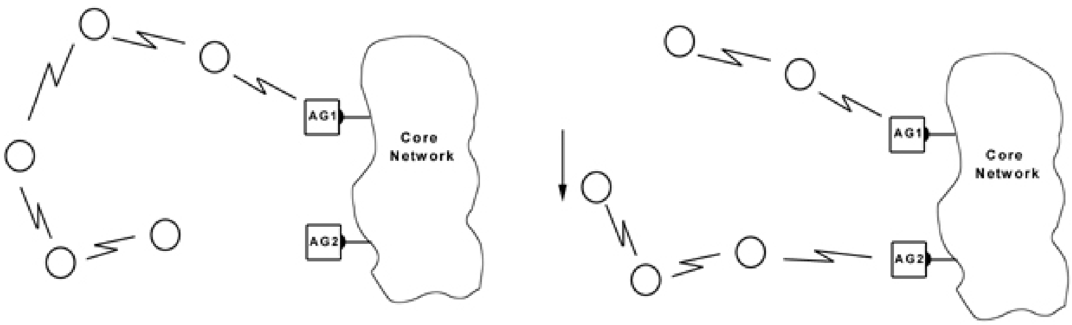


Figure 2.4: Ad hoc network split

A platform in the new autonomous ad hoc network uses a satellite radio interface to communicate with the core network. All other platforms within ad hoc range use this platform as the new default route to communicate with the core network and the other ad hoc network.

2.4 Scenario 4. Multihoming

There are several platforms in the battalion capable of acting as default routers. There are also several available types of radio interfaces available. The platform current acting as the default router for the battalion is using a satellite interface. An UAV access network becomes temporary available. This access network provides a higher bandwidth to nodes that temporary needs a high bandwidth link.

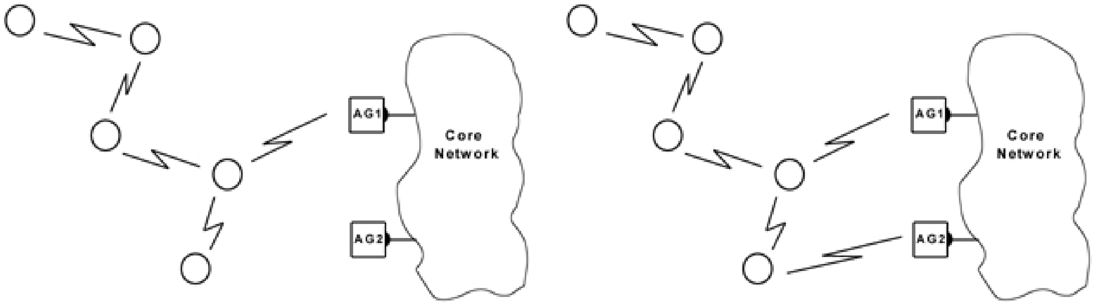


Figure 2.5: Ad hoc network with multiple access routers

Nodes that wish to communicate with the core network through one of the available access networks can choose between default routes. Platforms in the battalion are capable of choosing the appropriate default route to the core network depending on some priority scheme.

2.5 Scenario 5. Node Roaming

A mobile platform participating in an ad hoc network has one default route. The platform acting as the default router interoperates with the core network with a UAV interface.

The mobile platform moves out of scope from the ad hoc network and into scope of another ad hoc network with an additional access router interoperating with another access gateway.

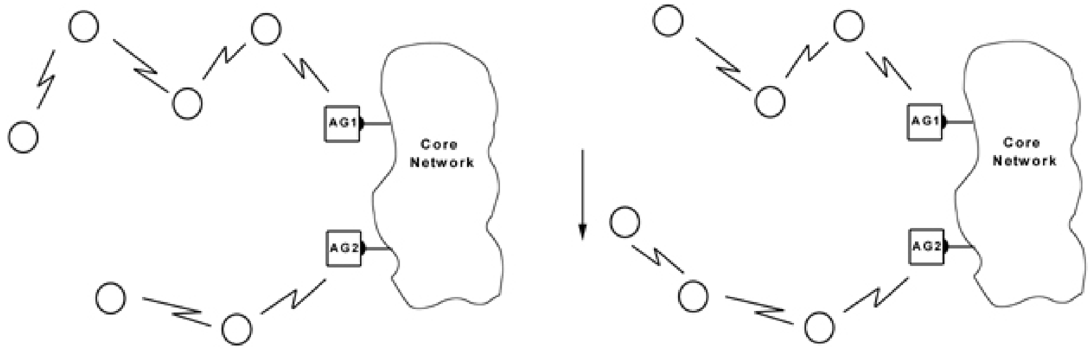


Figure 2.6: A platform moves from one ad hoc network to another

The platform can interact with the new ad hoc network and can be reached by platforms in its home ad hoc network through the core network. This platform can also become the default router for the visited ad hoc network.

3 Introduction to Interworking

3.1 Internet Protocol version 6

Internet protocol version 6 (IPv6) [3] was recommended in 1994 to be an evolutionary step from the internet protocol version 4. The IP address size has been increased from 32 bits to 128 bits to support more levels of addressing hierarchy, greater number of addressable nodes and a stateless auto-configuration method. To keep the common-case processing cost of packet handling and to limit the bandwidth cost the header format has been simplified. Features that are in work in IPv4 are kept in IPv6 and features that is not in use where removed. In addition new features like security capabilities and improved support for options are integrated as extension headers in the main header design. Also, an additional Mobility Header is proposed to manage mobility at the network layer.

3.1.1 Address Architecture

An IP-address is an identifier for a node's attachment and sets of attachments to a link. The attachment to a link is referred as an interface to that link. In IPv6 there are three types of addresses. The Unicast address is an identifier for a single interface. A packet sent to a Unicast address is delivered to the interface identified by that address. An Anycast address is an identifier for at set of interfaces. A packet sent to an Anycast address is delivered to the nearest interfaces identified by that address according to the routing protocols measure of distance. A Multicast address is an identifier for a set of interfaces. A packet sent to a multicast address is delivered to all interfaces identified by that address. The IPv6 Multicast address replaces the IPv4 broadcast address.

The text representation of an IPv6 address can be formatted in different ways. The preferred form is x:x:x:x:x:x:x:x, where the eight 'x's are hexadecimal values of 16-bit pieces of the address. It is not necessary to write all zeros in an individual field, but there must be at least one numeral in every field.
Example:

1080:0:0:50:8:800:200C:417A

It is common for addresses to contain long strings of zeros due to certain styles of address allocation. A special syntax is available on order to make writing of such addresses easier. The use of "::" indicates multiple 16-bits groups containing zeros. The "::" can only appear once in an address.
Example:

1080::50:8:800:200C:417A

The text representation of the IPv6 address prefix is:

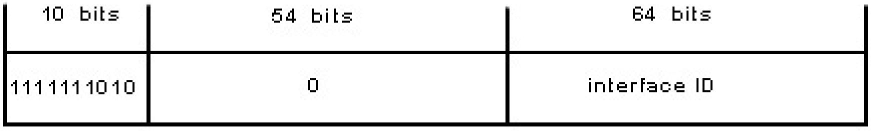
```
ipv6-address/prefix-length
```

Where the prefix length is an integer value specifying how many of the leftmost contiguous bits of the address comprise the prefix.
Example:

1080:0:0:50:8:800:200C:417A/64

In the above 1080:0:0:50:: is the network prefix

There are three main types of Unicast addresses in IPv6; link-local, site-local and global. The link-local is used for addressing on a single link for purposes such as automatic address configuration, neighbourhood discovery or when no routers are present on the link. Routers do not forward any packets with link-local source or destination address to other links. Link-local addresses have the following format:

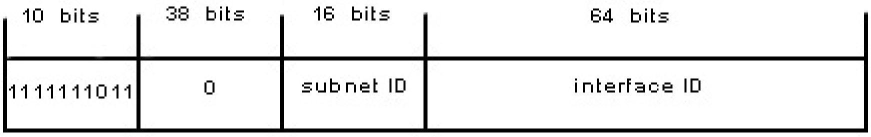


10 bits	54 bits	64 bits
1111111010	0	interface ID

Figure 3.1: Link-local address layout

The first 10 bits identifies the link-local address. The 64 interface ID bits are required to be unique on the link.

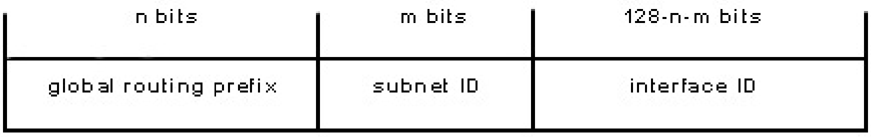
Site-local addresses are used to uniquely identify interfaces within a single site. A site is not very well defined but is typically expected to cover a region of topology that belongs to a single group and is located within a single geographical location. Routers do not forward any packets with site-local source or destination addresses outside the site. Site-local addresses have the following format:



10 bits	38 bits	16 bits	64 bits
1111111011	0	subnet ID	interface ID

Figure 3.2: Site-local address layout

The first 10 bits identifies the site-local address and the 16 bits subnet ID identifies the site scope. The 64 interface ID bits are required to be unique on the site. Global addresses are for uniquely identifying interfaces anywhere in an internet. The general format for global Internet addresses is as following:



n bits	m bits	128-n-m bits
global routing prefix	subnet ID	interface ID

Figure 3.3: Global address layout

The global routing prefix is a hierarchically structured value assigned to a cluster of subnets. The subnet ID is and identifier of a site within the subnets and the interface ID is unique value on the link and site.

3.1.2 Protocol Headers

In IPv6 the main header is kept as simple as possible. Optional network-layer features are encoded in separate extension headers placed between the IPv6 header and the transport-layer header in a packet. Each extension header is identified by a distinct Next Header value. The full implementation of IPv6 includes the following extension headers:

- Hop-by-Hop Options
- Destination Options
- Routing
- Fragment
- Authentication
- Encapsulating Security Payload

In addition a Mobility Header (MH) is proposed in an Internet draft [9] to carry mobility information messages.

An IPv6 packet may carry zero or more extension headers each identified by the Next Header field of the preceding header.
Example:

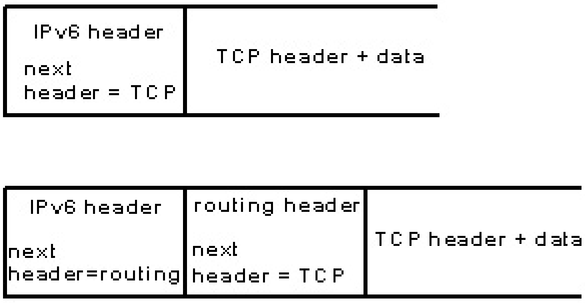


Figure 3.4: Header layout example

Except for the Hop-By Hop option header, extension headers are not examined or processed by any node along a packet's delivery path until the packet reaches the node, or each of the set of nodes in the case of multicast, identified in the destination address field of the IPv6 header.

There are two possible ways to encode optional destination information in an IPv6 packet: either as an option in the Destination Options header, or as a separate extension header. Mobile IPv6 described in 3.2 and 3.3 uses a separate extension header. If a packet contains multiple extension headers the Mobility header is the last one. The Mobility Header is identified by a unique value in the immediately preceding header and has the following format:

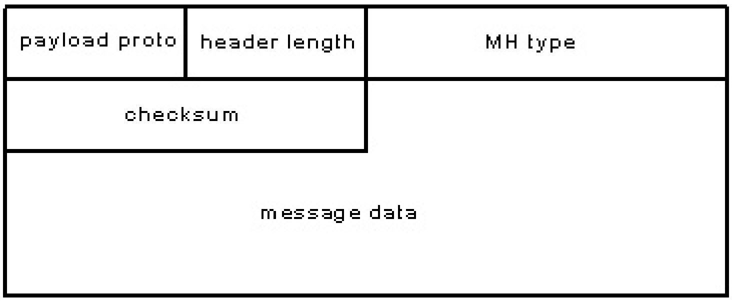


Figure 3.5: The mobility extension header

Payload Proto is an 8-bit selector and identifies the type of header immediately following the Mobility Header. The first 8-bits in an extension header is usually identified as Next Header Field but since the Mobility header is the last extension header in a packet the Payload Proto is identifying upper-layer protocol header such as TCP. The Header Length field is an 8-bit unsigned integer and identifies the length of the total header in 8-octets units. The Mobility Header Type field is a selector that identifies the particular mobility message in question, described in chapter 3.2.2. The value in the checksum field is calculated on the entire Mobility Header starting with the Payload Proto field. Message Data can be of variable length and contains data specific to the type of message.

3.1.3 Native Neighbour Discovery

The Neighbour Discovery Protocol (NDP) is a part of the IPv6 architecture and solves a set of problems related to the interaction between nodes attached to the same link. Nodes use NDP for three purposes; to determine the link-layer addresses for neighbours known to reside on attached links and to quickly update cached values, to find neighbouring routers, and to actively keep track of which neighbours are reachable and which are not, and to detect changed link-layer addresses. NDP is a network-layer protocol and is by that independent on the type of link-layer. However, because NDP uses multicast for some services, it is relaying on the link-layer to support multicast function. Multicast for the Ad Hoc On Demand Distance Vector is described in chapter 3.5.1.

Neighbour discovery uses five different Internet Control Message Protocol (ICMP) messages [8] to serve its purpose. The ICMP types are:

- Router Advertisement
- Router Solicitation
- Neighbour Solicitation
- Neighbour Advertisement
- Redirect

The Router Advertisement message is used by routers to advertise their presence together with various link and internet parameters. The message can either be multicast periodically or sent in response to a Router Solicitation message. Router Advertisements contain prefixes that are used for the stateless address configuration procedure [8]. The Router Solicitation message is sent by hosts that request routers to generate Router Advertisements immediately rather than their predefined next scheduled time. Neighbour Advertisement is sent in response to a Neighbour Solicitation message. A node may also send unsolicited advertisement to announce a link-layer address change. Nodes usually use the Neighbour Solicitation message to verify that a neighbour on the link is still reachable via a cached link-layer address. It can also be used in the Duplicate Address Detection procedure [8]. The fifth NDP message is the Redirect message. Routers to inform hosts of a better first hop for a destination use this message.

Hosts on a link receive Router Advertisements from all available routers on that link and build a list of default routers. The advertisements are usually generated frequently enough for hosts to learn their presence within a few minutes. But the advertisements are not sent frequently enough to detect router failure. For that, a separate Neighbour Unreachability Detection procedure is provided. The procedure is depending on confirmation that packets sent to a node on the link are actually reaching that node and being processed properly. The confirmation is provided by two sources. When possible, upper-layer protocols provide a positive confirmation that a connection is successfully ongoing, that is, previously sent data is known to have been delivered correctly. When this approach is not available by upper-layers a node sends Unicast Neighbour Solicitation message as probes to the next hop node to ensure that a confirmation, in the form of a Neighbour Advertisement, is received.

The Router Advertisement ICMP has the following layout:

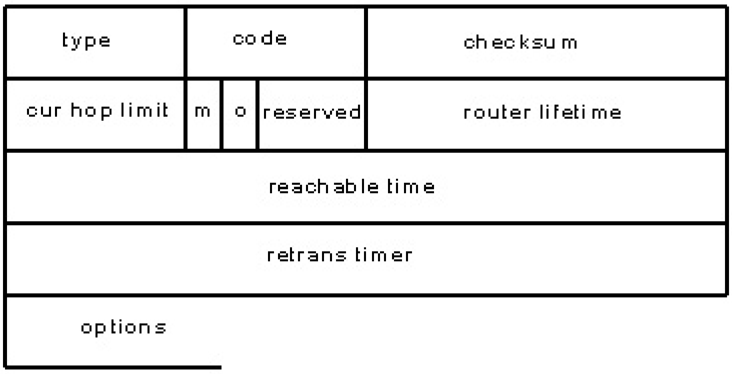


Figure 3.6: Router Advertisement message

The options field is used to carry additional information. This field is referred in chapter 3.2.3 relevant to mobility management.

3.1.4 Internet Routing Hierarchy

IPv6 introduces some new routing functionality, like the Router Extension header which contains a lists one or more intermediate nodes that must be visited on the way to a packet's destination. But general routing is almost identical to IPv4 routing under Classless Internet Domain Routing (CIDR) [5]. It is very important to understand that routing in IPv6 network must be in the form of CIDR. CIDR defines address assignment and aggregation strategies designed to facilitate scalable internet routing. Without an address hierarchy, routers would be forced to store routing table information on the reachability of every network on the internet. In a large internet it is not feasible to manage routing tables and updates for so many routers.

In IPv4 CIDR and IPv6 networks the routing system makes forwarding decisions based on the longest prefix match. The IPv6 aggregatable global unicast address, used by nodes global addressable on the Internet, has the following format:

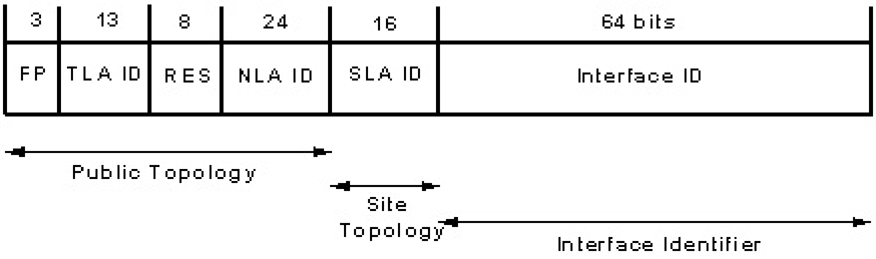


Figure 3.7: The global unicast address layout

The first three bits, the Format Prefix (FP), is set to 001 and identifies Internet aggregatable global unicast addresses. The next field, the Top-Level Aggregation Identifier (TLA-ID) is the top level in the routing hierarchy. Every router on the internet, not including routers with a default route entry as described in chapter 5, must have a routing table entry for every active TLA ID. The Reserved (RES) field is reserved for future growth of the TLA field. The current maximum number of TLA-ID's is 8,192 (2^13).

The Next-Level Aggregation Identifier's (NLA-ID) is the next level in the address hierarchy. The 24 NLA-ID bits can be used in an arbitrary manner to create an under-laying level of addressing hierarchy appropriate to the network topology. This is shown as follows:

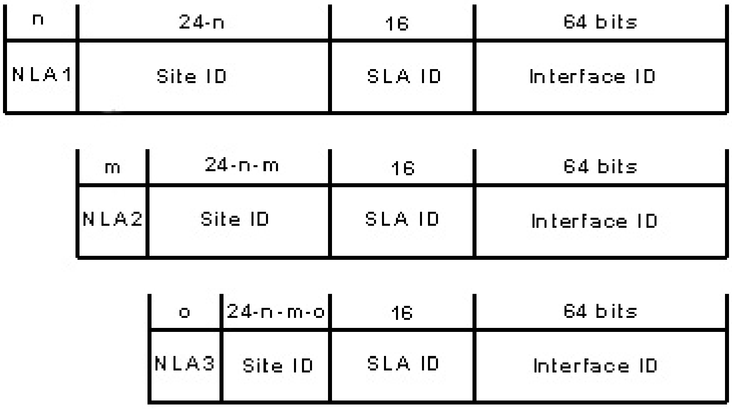
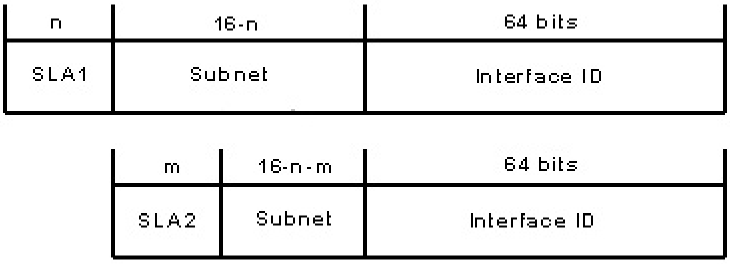


Figure 3.8: NLA level of addressing hierarchy

The design of an NLA-ID hierarchy is a trade-off between routing aggregation efficiency and flexibility. The use of hierarchies allows for greater amount of

aggregation and results in smaller routing tables. A flat NLA-ID structure provides more attachment flexibility but results in larger routing tables.
The Site-Level Aggregation Identifier (SLA-ID) is the level below the NLA-ID in the global hierarchy structure. The SLA-ID is also used to identify subnets, in analogue to IPv4 subnets. As in the case of NLA-ID the design of the SLA-ID bits is a trade-off between routing aggregation efficiency and flexibility. The design of the SLA-ID bits can be shown as follows:



n	16-n	64 bits
SLA1	Subnet	Interface ID

m	16-n-m	64 bits
SLA2	Subnet	Interface ID

Figure 3.9: SLA level of addressing hierarchy

An example of hierarchical relationship in order to accommodate route aggregation can be shown as follows:

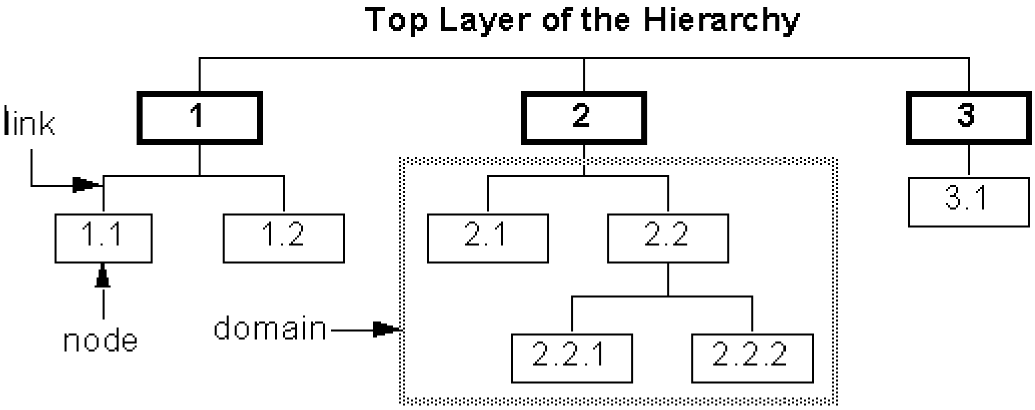


Figure 3.10: Routing Hierarchy

3.2 Mobile IPv6

If a node disconnects from its home network and connects elsewhere on the internet, the node would not be able to continue communication until it configures the network interface with a new topologically correct IP address, netmask and default router. The node would then not be addressable by its home address. Mobile IPv6 [9] introduces a mobility management scheme at the network layer providing seamless mobility to higher-layers including applications across heterogeneous media. A brief introduction to Mobile IPv6 is given in this chapter relevant to the Master Thesis. For a more detailed description on specific node operations the reader is referred to the Mobil IPv6 specification [9].

3.2.1 General Operation

The basic idea with Mobile IPv6 is that a node is always, independent on its current hierarchical attachment to an internet, addressable at its home address. Packets addressed to this home address are routed through the internet hierarchy using conventional routing mechanisms. If the destination node is away from home, attached to a foreign link, it is also addressable at one or more care-of addresses. A care-of address is a topologically correct IP address associated with a mobile node (MN) while visiting a foreign network. The subnets prefix of a mobile node's care-of address is the subnet prefix belonging to the foreign link. The mobile node acquires its care-of address through address autoconfiguration, according to the method of Neighbour Discovery described in chapter 3.1.3 with some modification described in chapter 3.2.3. The association between a mobile node's home address and care-of address is known as a binding for the mobile node.

If the node is away from home it registers its current care-of address with a router on its home link as a binding. The home link router is by that requested to function as the home agent (HA) for the mobile node. The home agent uses Neighbour Discovery to intercept any IP packets addressed to the mobile node's home address on the home link. The packet is then tunnelled to the mobile node's care-of address. Tunnelling is performed using IP encapsulation. The packet is routed to the care-of address by intermediate routers using conventional routing mechanisms. The mobile node uses the encapsulated source address and sends any packet directly to the corresponding node (CN). The mobile node sets the source address of this packet to the care-of address and includes the Home Address destination option. This allows every correspondent node the transparent use of the care-of address for layers above Mobile IPv6. The routing procedure is called triangular routing and can be shown as follows:

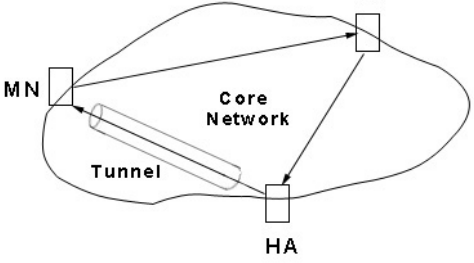


Figure 3.11: Mobile IPv6 triangular routing

When a node visiting a foreign network receives tunnelled packets it can use this as an indication that the corresponding node has no binding with the mobile node. The node can inform the corresponding node of its current location to avoid triangular routing. Sending a binding update to the corresponding node does this. It is usually expected that corresponding nodes will route packets directly to the mobile node's care-of address so that the home agent is rarely involved with packet transmission to the mobile node.

An alternative to triangular routing and route optimisation is reverse tunnelling. The mobile node then uses a reverse tunnel to the home agent when sending packets to the corresponding node. The home agent de-capsulate the packet and forward it to the corresponding node. These two alternatives in regard to a tactical scenario will be discussed further in chapter 5.

3.2.2 Message Types

To serve its purpose Mobile IPv6 uses the Mobility Extension Header to carry the following messages:

- Binding Update
- Binding Acknowledgement
- Binding Refresh Request
- Binding Error
- Home Test Init
    - Home Test
- Care-of Test Init
    - Care-of Test

The Binding Update message is used to notify a corresponding node or the mobile node's home agent of its current care-of address. The recipient of the Binding Update message sends a Binding Acknowledgement in return if the binding cache update was successfully performed. Every entry in a corresponding node's binding cache has a lifetime. If the lifetime is close to expire the corresponding node can send a Binding Refresh Request to update the lifetime of the binding. The Binding Error message is sent by corresponding nodes to signal an error. The four Test messages are used in the procedure to avoid triangular routing.

Mobile IPv6 also uses four new ICMP message types for home agent discovery and home address configuration on a foreign link:

- Home Agent Address Discovery Request and Reply
- Mobile Prefix Solicitation and Advertisement

The two Home Agent Address Discovery Request and Reply message allows a mobile node to dynamically discover the IP address of a home agent on its home link. The mobile node visiting a foreign network sends a Request to the Home Agent anycast address for its own home subnet prefix and reaches any available home agent on its home link. The available home agent returns a Reply message to the mobile node including a list of home agents on the home link. The Mobile Prefix Solicitation and Advertisement messages are similar to the Router Solicitation and Advertisement used in Neighbour Discovery. The difference is that these messages are routed through the internet between the home agent and visited link. The mobile node can use these messages to reconfigure or autoconfigure its home address on a foreign link.

An IPv6 Destination Option extension header is also a part of the Mobile IPv6 specification. It is used to inform the recipient of the mobile node's home address so that higher layers do not notice the care-of address.

3.2.3 Neighbour Discovery in Mobile IPv6

The Neighbour Discovery Protocol NDP [10] is modified in Mobile IPv6. Relevant changes are briefly described in this chapter.

In the Router Advertisement Message a bit in the header is added to indicate that the router sending the advertisement message is serving as a home agent on this link. The Prefix Information option used in Router Advertisement message is also modified to carry the sending routers global address, in addition to the link-local address. The routers global address is needed for the dynamic home agent address discovery mechanism and to allow a mobile node to send a binding update to a router on a previous visited link to establish forwarding to the new link.

As described in chapter 3.1.3 routers generate advertisement frequently enough that hosts will learn their presence within a few minutes. This is not enough to provide movement detection for mobile nodes. A mobile node detects a movement by learning the presence of new routers and their prefixes and by learning that previous routers are no longer reachable. To provide seamless mobility to higher-layers the rate which routers send out advertisement is increased. Recommended values [9] are between 0.05 and 1.5 seconds to supply seamless connectivity without interrupting above layer procedures. Mobile nodes may also send router solicitation message more frequently than originally intended in NDP.

Two more option is added to the router advertisement message. The Interval option is added to advertise the interval at which the sending router sends unsolicited multicast router advertisements. A mobile node could use this option in its movement detection algorithm by assuming the router is out of reach if the advertisements no longer are received in the earlier stated interval. The second option added is the Home Agent Information option. This option is used by home agents to advertise information specific to this router's functionality as a home agent. The greater value the more preferable home agent. This can be dynamically based depending on the number of nodes the home agent serves or predefined by some management.

3.3 Mobile IPv6 Mobile Router Extension

The purpose of traditional mobility support on the network-layer is to provide continuous and seamless internet connectivity to mobile hosts (host mobility support). In contrast, network mobility support is concerned with situations where an entire network dynamically changes its point of attachment to an internet and thus its reachability in the topology (network mobility support). Mobile IPv6 is unable to support an entire network that changes its point of attachment. But there are some efforts within the Internet community to extend the Mobile IPv6 standard to support mobile networks. The goal is to provide continuous seamless internet connectivity for both the mobile router and nodes behind it in a transparent way.

There are two proposed solutions to the network mobility problem following different set of requirements [11], [12]. [11] has a more straightforward solution to the problem described in chapter 4 and is relevant to ad hoc operation described in chapter 3.4. [12] is considering a more advanced topology where the mobile network is not a stub network and where nested level of mobile routers is possible. These types of topologies are not relevant in this master thesis. In chapter 3.3.2 the general operation of [11] is briefly described.

3.3.1 Extensions

To support mobile routers some extensions to Mobile IPv6 are proposed. In the Binding Update message header an extra flag is added. If the flag is set it indicates that a Prefix Sub-Option is carried in the Binding Update message. A Prefix Scope Binding Update is an enhanced Mobile IPv6 Binding Update message, which associates a care-of address with a prefix instead of a single address. This binding establishes a many-to-one relationship between the set of nodes that share the same mobile network prefix and a care-of address instead of the usual Mobile IPv6 one-to-one relationship between a home address and a care-of address. The receiving node processes the Prefix Sub-Option and re-routes packets with a destination address that corresponds to the care-of prefix.

3.3.2 General Operation

When a mobile router detects a foreign link it sends a Prefix Scope Binding Update with the foreign link network prefix to its Home Agent. If triangular routing wishes to be avoided, Prefix Scope Binding Updates is sent to all the corresponding nodes communicating with the mobile router itself or any nodes within the mobile network. The Prefix Scope Binding Update instructs its recipients to use the mobile network prefix as a netmask in the binding cache. This allows binding independently of the number of nodes in the mobile network and also transparent to them. Datagrams sent by corresponding nodes to the home IP address of a node in the mobile network are routed to the home link of the mobile router where the home agent intercepts them. The home agent examines its Binding Cache for an entry corresponding to the destination address. If a care-of-address is returned, the packet is tunnelled to this address as specified in MIPv6. If the end node in the tunnel is a mobile router it forwards the packet to the de-capsulated destination address within the mobile network.

3.4 Ad Hoc Networks

A mobile ad hoc network consists of a wireless multi-hop topology, which is dynamic, random, and sometimes rapidly changing. To support robust and efficient operation in such networks, nodes forming an ad hoc network perform network functions that are normally the job of routers within an internet infrastructure. The mobility of an ad hoc network is defined within an autonomous, mobile, wireless domain, where a set of nodes using various radio technologies, themselves form a flat network routing infrastructure. The network may operate isolated or may have gateways to a fixed network. In the latter case the ad hoc network operate as a stub network. Stub network carries traffic originating at and destined for internal nodes, but do not permit traffic to transit through the network.

The original motivation of an ad hoc network is the military need to move about freely without any of the restriction imposed by a wired communication infrastructure. Also, the military cannot rely on an existing fixed communication infrastructure in battlefield environments such as in forests or urban areas, but need to rapidly deploy a self-organised survivable mobile communication infrastructure. Nodes beyond radio media line of sight may also need to communicate with each other by a multi-hop scheme. The primary goal of ad hoc networking is to provide connectivity between participants. But there are also tactical occasions where global connectivity is required by ad hoc nodes to be able to communicate with remote nodes or ad hoc networks through a long-range communication media such as satellite.

Ad hoc Routing is usually performed at the IP-level to provide network-level consistency for networks composed of nodes using various physical-layer media. One single ad hoc routing protocol will likely not be able to efficiently operate across the entire spectrum of possible designs and operating conditions of ad hoc networks. Therefore there are several proposed protocols available [13]. Routing protocols used within an ad hoc network may generally be categorised as either table-driven or source-initiated. These categories can also be referred to as proactive or reactive routing protocols. The proactive approach keeps track of routes to all destinations in the ad hoc network and has the advantage that communication with any node within the ad hoc network experience minimal initial delay viewed from upper-layers. The disadvantage of proactive routing protocols is the additional control traffic that is needed to continually update routing tables. If the ad hoc environment is very dynamic and rapidly changing the control messages can result in congested network points since the bandwidth in an ad hoc network are generally very scarce. The reactive approach however, acquires routing information only when it is needed. This results in less bandwidth usage but increased latency for upper-layers since the route is requested on demand.

In this master thesis the ad hoc network is seen as a very dynamic network where nodes are free to move about arbitrarily, described in chapter 1. The number of nodes is relatively large, as described in chapter 2, and bandwidth resources are generally very low for nodes participating in the ad hoc network. Therefore a reactive routing protocol is assumed. In chapter 3.5 the On Demand Distance Vector (AODV) and functionality relevant to the routing protocol itself and interworking procedures are briefly introduced.

AODV is chosen as the ad hoc routing protocol in this master thesis for its adaptation to IPv6, suitableness in regards to the tactical scenarios described in chapter 2, its interworking operations, and for the amount of research that is currently being done regarding security issues [14].

3.5 Ad Hoc On-Demand Distance Vector Routing (AODV)

The Ad Hoc On-Demand Distance Vector algorithm [14] was designed specifically for wireless ad hoc networks and does not depend on a particular physical medium except that the link provided by the medium must be symmetric, which means that data can traverse in both directions. It tries to provide communication between mobile nodes with minimal control overhead and minimal route acquisition latency to upper-layers. AODV discovers routes paths on an on-demand basis and these routes are maintained only as long as they are necessary. With the use of destination sequence numbers loop freedom is accomplished. Every node maintains its own individual sequence number, which it increases each time it learns of a change in the topology of its neighbourhood. Given the choice between two routes to a destination, a requesting node always selects the one with the greatest sequence number. This ensures that the most recent route is selected during route discovery. The routing table in ad hoc nodes maintained by AODV has the following layout:

Destination IP Address	Destination Seq. Nr.	Valid Destination Seq. Nr.	Interface	Hop Count	Next Hop	List of Precursors	Lifetime	Routing Flags	State

Table 3.1: AODV node routing table

The Destination IP Address field contains the route entry in question, and is a unique row identifier in the table. The Destination Sequence Number field contains a number created by the destination for any route information it sends back to a requesting node. Other nodes to determine the freshness of the information contained from the originating node use this. Interface field is an identifier for the physical interface to the media, through which the destination node can be reached. The Hop Count field is the number of hops to the destination and the Next Hop field is the next hop in the routing path to reach the destination. The List of Precursors field is a list of nodes that route through the node in question in order to reach their destination. The node uses this field if the link breaks to inform precursor nodes about changes in their route path. The expiration or deletion time of the route entry is given in the Lifetime field. The routing Flags field is used in multicast procedures beyond the scope in this master thesis. In the State field it is indicated whether the entry is valid or invalid. An invalid route entry is used to store the previously valid route information for an extended period of time. An invalid route may not be used to forward data packets.

In chapter 3.5.1 a description of the three message types used in AODV is given and the layouts of the messages are shown. Chapter 3.5.2 briefly describes the routing operations performed by AODV and chapter 3.6 gives an introduction to interworking procedures.

3.5.1 Message Types

There are three control messages defined in AODV. These messages are sent using the transport layer protocol UDP via port identifier 659. The message types are:

- Route Request (RREQ)
- Route Replies (RREP)
- Route Errors (RERR)

A node sends a RREQ message when a route to a new destination is needed. The node multicasts the message to find the route. When either the destination itself or any intermediate node with a fresh enough route to the destination is reached a RREP message is unicast back to the origination of the RREQ message. The RERR message is sent when a link breakage is detected in an active route. The message indicates those destinations that are unreachable due to the loss of the link. The message is sent from the node that detects its link breakage to all the nodes in its precursor list.

Below are the layouts of the three AODV messages. These figures, and the contents of the headers, are referred to further on in this master thesis.

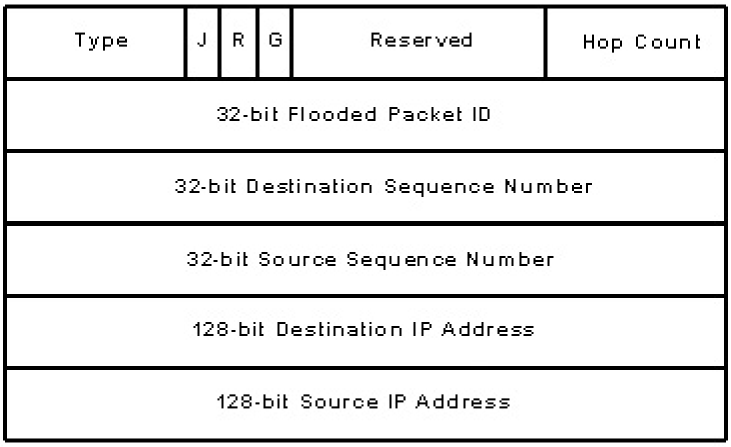

Type
J
R
G
Reserved
Hop Count
32-bit Flooded Packet ID
32-bit Destination Sequence Number
32-bit Source Sequence Number
128-bit Destination IP Address
128-bit Source IP Address

Figure 3.12: Route Request (RREQ) message format

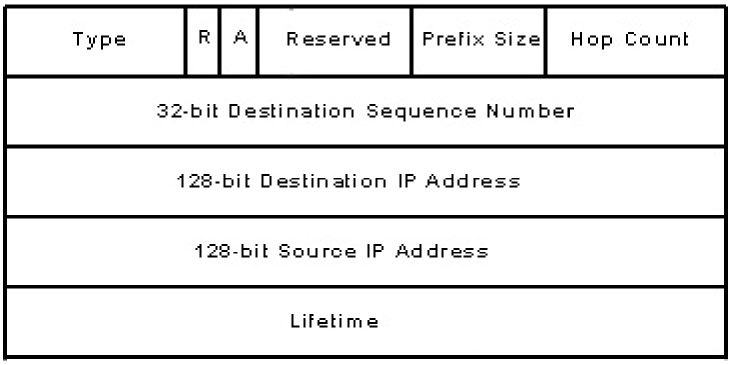

Type
R
A
Reserved
Prefix Size
Hop Count
32-bit Destination Sequence Number
128-bit Destination IP Address
128-bit Source IP Address
Lifetime

Figure 3.13: Route Reply (RREP) message format

<table>
<tr><td>Type</td><td>N</td><td>Reserved</td><td>DestCount</td></tr>
<tr><td colspan="4">Unreachable Destination Sequence Number</td></tr>
<tr><td colspan="4">Unreachable Destination IP Address</td></tr>
<tr><td colspan="4">Additional Unreachable Destination Sequence Numbers</td></tr>
<tr><td colspan="4">Additional Unreachable Destination IP Addresses</td></tr>
</table>

Figure 3.14: Route Error (RERR) message format

3.5.2 AODV operations

A node that wishes to send a packet to a destination node checks its routing table to determine whether it has a current route to the destination node. If a next hop value is returned from the routing table the node forwards the packet to the next hop node towards the destination. In this case AODV is not involved. However, when no next hop value is return from the routing table, the AODV route discovery process begins. The source node creates a RREQ message containing the source node's IP address with current sequence number and destination IP address with the last known sequence number. The message also contains a Flood ID number. The IP address of the source node together with the ID number forms a unique identifier for the RREQ. The ID number is incremented by one every time the node sends out a new RREQ message. After the RREQ message is multicasted to the IPv6 All Link Local Nodes address the sender of the message starts a timer to wait for a reply. When a node receives the RREQ message it first check the ID number together with to source IP address to determine if the message has been received before. If it has, the message is discarded otherwise the node sets up a reverse route entry for the source node in its route table. The reverse route entry contains (table 3.1) the source node's IP address, sequence number, the number of hops to the source node and the last neighbour who forwarded the message (next hop value for the source node route entry).

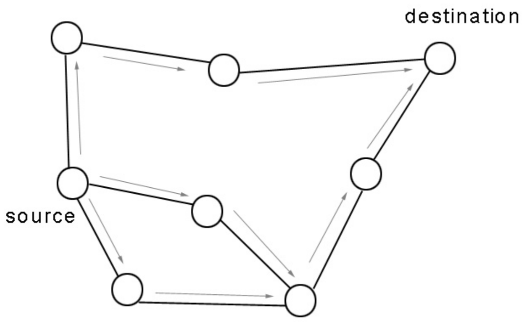


Figure 3.15: Route Request Propagation

In order to respond to a RREQ message the receiving node must either be the destination node of the RREQ message or have a valid entry for the destination in its routing table. A valid entry in the routing table must have a destination sequence number that is greater than or equal to the destination sequence number in the RREQ message. The sequence number validation prevents routing loops by ensuring that the route returned is never old enough to point to a previous intermediate node (would cause loop). If the node receiving the RREQ message does not have a valid route entry or is not the destination node of the message it increments the RREQ hop count and multicasts the packet to its neighbours.

The RREP sent in response to the RREQ contains the IP address of both the source and destination. If the node sending the RREP message was the destination node of the RREQ message, the current sequence number, hop count set to zero and lifetime of the route is placed in the RREP message. If an intermediate node is sending the RREP message, its value of the destination's sequence number is placed in the message and the hop count is set to the distance to the destination. The Lifetime field in the RREP is calculated out of the Lifetime field in its table. Any intermediate node receiving the RREP message toward its destination, update appropriate values in its routing table. If an intermediate node receives the same RREP message more then once, it forwards the first RREP and compares the destination sequence number and hop count with later received RREP. If the hops count is smaller or the destination sequence number is greater the intermediate node forwards the packet to its destination. The destination node can start send data when the first RREP message is received and then later, if a better route is received in a RREP, update its routing table and send data using the new route.

When an intermediate node or a destination node moves out of scope of the previous active path between the source and destination, a RERR message is activated by the neighbour node closer to the source node in the route path, illustrated in Figure 3.16. The RERR message contains the unreachable destination node's IP number and sequence number. If needed, additional node's unreachable information can be added to the RERR. If the node sending the RERR has a list of precursor node in its routing table for the moving node, it sends the RERR message to these nodes. The receiving nodes of an RERR message mark the route entry as invalid and, if it exists any precursor node for the broken destination in its routing table, sends RERR message to these nodes. A source node receiving the RERR that still needs to send data can reinitiate a RREQ and find a new route to the destination.

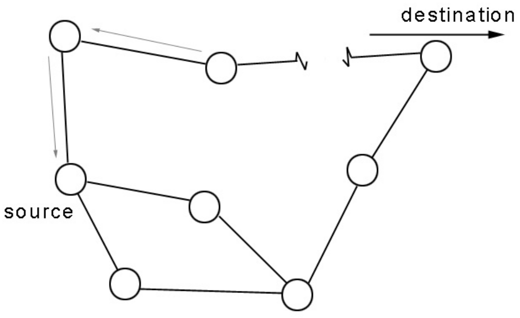


Figure 3.16: RERR propagation

3.6 Interworking Operations

3.6.1 Gateway Discovery and Address Autoconfiguration with AODV

In order to receive packets from an external internet a node in an ad hoc network needs a global and topological correct IP address. The node also needs a default access router to forward packets destined to the internet. There are two proposed solutions to gateway discovery and address autoconfiguration [7]. One involves sending route solicitation and receiving route advertisement as a part of the NDP IPv6 specification described in chapter 3.1.3 with some modification in regards to the link-local scope used in ad hoc networks. The other solution is imbedded in the ad hoc routing protocol. In this master thesis the later approach will be assumed and the operations are briefly described in chapter 3.6.2 and 3.6.3 in relation to the AODV routing protocol. This approach has several advantages in regards to the tactical scenarios described in chapter 2. The advantages will be proved in chapter 5.

The RREP and RREQ messages in the AODV protocol specification are slightly modified. In order to indicate that the messages are used in access route operations, one “I” flag is added from the reserved field (Figure 3.12 and 3.13) in the messages.

When a node in the ad hoc network request a global routable address it broadcasts a RREQ message with the “I” flag set to the INTERNET_GATEWAYS global multicast address. The source address used in the RREQ message can either be a pre-defined home IP address used in the ad hoc network uniquely or it can be a temporary address from the MANET_INITIAL_PREFIX [7]. This choice is discussed further in chapter 5. An access router receiving the RREQ with the “I” flag set constructs a RREP message with the “I” flag set and unicast the RREP message back to the requesting node. The RREP message contains the prefix length as defined in AODV and together with the access router IP address found in the RREP message the receiving node can form a globally routable address. The node also uses the access router IP address found in the RREP message as the default route. If the node used the MANET_INITIAL_PREFIX in the RREQ message the node is required to delete this temporary address and then broadcast a RERR message with the temporary address to delete all the related host routes in the ad hoc network.

3.6.2 Node Operation

When a node desires to send a packet it first searches its routing table for the destination node. If an entry was found it sends the packet to the Next Hop found in the routing table. If the destination was not found, the node sends a route request for the destination node. Then, if a default route exists, the node waits for the RREP message. If a default route does not exit the node uses the method described in chapter 3.6.1 to obtain one. If the node does not receive any route reply from its RREQ message sent to the destination, the node assumes the destination node is located on the internet. The node then sends the packet using the default route and sets a route entry into the routing table with the destination node pointing towards the default route. If the node gets a route reply for the destination it requested, it sets a host route in the routing table and sends the packet to this route.

IP uses ICMP to signal routing errors and redirect messages. In ICMPv6 there are two relevant messages regarding ad hoc network operation. If a node receives an ICMPv6 Destination Unreachable Message after sending a packet to a host route, the node deletes this entry in the routing table. The node can initiate a RREQ message to find a new route. If a node receives a Destination Unreachable Message after sending a packet using the default route entry, the node can try to request a route for the destination again. If a node receives an ICMPv6 Redirect Message sent from a default route, the node tries to find a host route for the destination node instead of using the default route. This is described further in chapter 3.6.3.

If an intermediate ad hoc node receives a route request for a default router, it does not reply with global connectivity information even though it possess this information. This is to make the access router learn which nodes exist in the ad hoc network.

3.6.3 Access Router Operation

An access router in an ad hoc network has reverse routes for all the nodes in the ad hoc network. When the access router receives packets destined to the internet, it examines the route path for the packets' destination address. If a host route exists toward the ad hoc interface, it indicates the destination node can be reached in the ad hoc network. The access router sends an ICMPv6 Redirect Message to the source node to force it to find a host route for the destination. This action is taken to prevent packets with ad hoc node destination to be routed out to the internet.

When an access router receives a packet from the internet destined to an ad hoc nod, it forwards the packet using host routes generated by AODV. If such a route does not exist, it is requested by a RREQ message.

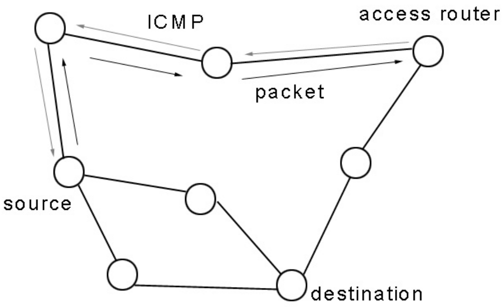


Figure. 3.17: Redirect Message propagation

4. Route Aggregation and Hierarchical Relationship

When a new node joins the internet, it needs full connectivity and an unambiguous address. That is, from every existing host there must be at least one path by which packets can travel to the new host. At each step along each of those paths, a router examines the host's address and forwards packets to the correct next hop. There are two limits, then, on growth.

First, there must be an unambiguous address available for each new host. In particular, the IP address used by the new host should never be simultaneously used by any other host. Second, each router must maintain a table that indicates the correct next hop for each destination address, and routers have a limited amount of the fast expensive memory needed to store entries in the forwarding table.

New protocols and technology can expand these limits. For example, dynamic address allocation used in mobile scenarios permits reuse of addresses under some circumstances. At least in principle, routers with more memory could keep track of extra routes. Protocol changes and additional technology, however, are costly and not always available when needed. The technology growth curve may also be unable to keep up with the growth of the internet. Sometimes it will be either cost-effective or just necessary to make more efficient use of existing resources instead.

Hierarchical route aggregation is one way to make more efficient use of existing resources. In particular, if all packets destined for addresses with the same prefix get forwarded to the same next hop, a router can maintain just one entry in its router table for that prefix, rather than a separate entry for each individual address. This method can be applied recursively to create larger and larger address blocks that share shorter and shorter prefixes.

Hierarchical route aggregation is widely used on the global Internet today and was the main motivation behind Classless Inter-Domain Routing (CIDR) [5]. Hierarchical aggregation only works, however, if traffic destined to all the addresses covered by a particular address prefix should be routed to the same next hop. Thus, the assignment of addresses to hosts must follow the connection topology of the network in order for hierarchical aggregation to be successful, see figure 3.10.

4.1 Mobility

Due to movement of a platform in the hierarchical routing structure when a new access network is used, the platforms within the ad hoc network must change IP address in order to interwork with the core network. The alternative would be to keep host specific routes globally through out the entire core network. An update would be required every time a change in the network address hierarchy is made. This approach would be very expensive when the core network is large and the changes are global. It could be considered OK to maintain host routes and a flat routing structure for mobile hosts within a single small subnet but not in a large internet infrastructure.

The fundamentals when considering mobility in a global hierarchical relationship are, what is the platforms address and route to that address and, if the address changes, how to find the current address? The resulting problems concerning aggregate routing vs. mobility are:

- What to do when (not if) connectivity is lost?
- How to reach the node when needed?
- How to keep communications seamless flowing?

When mobile nodes are discussed it is important to separate mobile hosts from mobile routers. If the access router of an autonomous system is mobile, should the hosts in the system be aware of their mobility or should they be considered to be static hosts attached to a mobile router?

The size of a mobile network is also an issue. Can the core network handle large mobile networks without affecting the performance at the backbone routing in the core network.

In the scenario described in 2.4, a military ad hoc network has multiple radio link connections, for instance via an UTRAN and a Satellite access network, to the core network. The goal is to use both connections simultaneously, considering either redundancy or efficiency. The fundamentals in this multihoming scenario are how to assign addresses to the interfaces in the network. The resulting problems are:

- How to reach the terminal depending on active interfaces?
- How to move communications from one interface to another?
- How to react to a total loss of connectivity?

4.2 Addressing and Naming

People need human-rememberable names for platforms reachable in the core network. An example of this is given in chapter 2, where a tank is identified with a name bound to an IP address. The names should be static while the name directory must be global and reachable. Names should always resolve the current location of a platform. This is a concern when it comes to mobility and multihoming. In IPv4 networks IP addresses are used for identifying the destination and source at the socket, finding the destination using the routing system and in some cases to authorise traffic flows at a firewall. In the network centric warfare system using IPv6 described in chapter 2, the address management and usage would be very different compared to today’s IPv4 networks. Platforms may be reachable by several different dynamical IP addresses with no relation to each other. Some of the IP addresses may be valid just for a given time and removed after its usage. Host IP addresses alone are therefore not very good to use as identifiers for mobile nodes in an IPv6 network centric warfare system.

In scenario 2.5 the ad hoc network can for instance use a local military infrastructure as the TS9000 system together with a global NATO satellite communication system to interoperate with the core network. The addresses assigned to platforms by these two access networks are topology different and are not related. In order for platforms in an ad hoc network to be reachable by their current attachments to the core network a mechanism must be introduced to associate addresses and access networks together.

Ad hoc networks generally have a flat routing structure while the core network and the global Internet have a hierarchical arrange structure. The access router in the ad hoc network, attached to the core network, need a mechanism to notice a movement and assign topologically correct addresses to platforms within the ad hoc network. An issue is also where to place the processing. Should it be done in the core network by routers and routing protocols or should it be done at the end-hosts, platforms participating in the network. Some of the questions concerning addressing in mobile ad hoc networks are:

- Mobility frequency, how often does the access network change?
- Is nested mobility (mobility within mobility) a concern?
- Multihoming issues.
- Where should the address management be placed, at the hosts or at the network?

Also, does the chosen mechanism meet the demands for a secure mobility management required in a high demand tactical ad hoc network?

4.3 Is Mobile IPv6 Enough?

In this master thesis the chosen mechanism to manage the defined problems is Mobile IPv6 together with an ad hoc routing protocol, AODV. But can these two network layer protocols handle the events described in chapter 2? Mobile IPv6 was initially designed to manage mobile hosts. The mobile hosts are usually either considered to be nomadic hosts, moving between fixed networks without seamless connectivity, or fully mobile hosts with seamless connectivity between the host itself and a corresponding node. Initially Mobile IPv6 was not concerned with mobile networks.

There are, as described in chapter 3, proposed extensions to the Mobile IPv6 standard to support mobile networks. But the mobile network itself is considered to be a fixed infrastructure in these proposals. This is not the case in the scenario described in chapter 2. The mechanised battalion contains highly mobile platforms that form a temporary network in an ad hoc fashion. Every platform in the battalion must be capable of interacting with corresponding nodes through the core network on the behalf of the entire network. Every platform must also be allowed to act as an access router on the behalf of the network when it is needed. The routing structure in these ad hoc networks is flat and cannot be considered to be hierarchy aligned together with the core network. Mobile IPv6 is not concerned with the quality or any other affecting parameters of the different access networks. The access networks available in the tactical scenario described in chapter 2 are very different in both quality and availability. Mobile IPv6 does not provide any functions to manage the access networks in regards to additional parameters such access network availability and quality

5. Suggestion for Mobility Management in Tactical Scenarios

5.1 Network Location Centre

In order to pinpoint the location of a mobile battalion and the platforms participating in it, we introduce a conceptional mobility management centre, a Network Location Centre (NLC), in the Core Network. An NLC is updated with the current location of a predefined group of mobile platforms operating in the Core Network. The NLC provides seamless connectivity between corresponding nodes and mobile platforms. While a mobile platform changes its point of attachment to the Core Network and hence its location in the address hierarchy by changed access network, it informs the NLC of its current reachable address. The NLC keeps the location information of every mobile platform it is serving in the Core Network. A corresponding node in the Core Network that wishes to communicate with a mobile platform always goes through the NLC that redirect the communication to the mobile platforms current location. The NLC strictly operate and perform its functions on the network layer only, and is transparent for applications and users.

Compared to general network management/monitoring systems, Network Operating Centres (NOC), where passive management functions are performed by application protocol such as SNMP, the NLC is performing active traffic redirect services for the network. The NLC is transparent for the NOC.

The NLC also provides a centralised security location to authorise both the corresponding nodes that wishes to communicate with a mobile platform and the mobile platform itself. By using the NLC as a centric system the security can be optimised and focused on this system. Security mechanism on the network layer as authorisation, authentication, packet filtering, and intrusion detection can be implemented on this single system instead of at the end platforms. This should not neglect the network layer security at the platforms but help to minimise the complexity of it. Only one node in the Core Network is authorised to communicate with the mobile ad hoc platform, the NLC. By this, security mechanisms like encryption and authorisation can be handled in a more secure manner at the mobile platform.

There should be several NLC available in the Core Network serving different groups of mobile platforms. This is both for redundancy and for shared cost purposes. In the tactical scenario described in chapter 2 the mechanised battalion is using one NLC to pinpoint its location in the Core Network. The battalion can primary considered to be managed by one NLC and have a secondary NLC for redundancy.

In technical terms an NLC is acting as a Mobile IPv6 defined Home Agent, with some modifications, for the group of mobile platforms it is serving. The network location information sent from the mobile platforms are Binding Updates described in chapter 3. Whenever a platform changes its access network, and thereby its location in the address hierarchy, it updates the NLC with correct information. The information sent by the mobile platforms differs depending on the scenario. A more detailed description on the information that is sent and by which platform, is given further in this chapter.

The mechanised battalion described in chapter 2 is acting as a mobile network including several platforms capable of acting as access routers through the various access networks available. This mobile network has a base configuration on its Home Network and every platform participating in ad hoc networking within the battalion has one Home Address attached to its network interface or interfaces. This IP address is used in the global Name Lookup service. Every platform in the battalion has one, or possible several, DNS entry bound to its Home IP Address as described in chapter 2. Whenever a mobile platforms DNS name entry is requested by a corresponding node, the Home Address is returned. Platforms within the ad hoc network should have host entries to every specific platform within the ad hoc network to prevent external name lookups when communicating within the autonomous ad hoc system.

By using the reverse tunnel procedure described in chapter 3.4 instead of triangular routing, the current care-of address and possible, indirectly, the actual geographical location can be hidden to the corresponding node. The corresponding node is not aware of the type of access network current in use by the battalion.

The overall scenario described in chapter 2 is somewhat different compared to a more traditional civilian ad hoc interworking scenario. Among the differences are the various types of access network available and the fact that every platform in the ad hoc network could act as an access router for the rest of the network. The dynamic changes and the role of the access routers are also typical for the tactical scenario described.

In the following chapters a description of the procedures performed by the involved platform in regards to the five scenarios in chapter 5 are given. The goal is to describe relevant node operations that provide seamless connectivity for layers above the network layer between corresponding and mobile nodes in all the five tactical scenarios described in chapter 2. The chapters both describe the general operation of the used techniques, with references to chapter 3, and suggested modification in order to accommodate the tactical scenarios. An evaluation of the solution is given in chapter 6.

Also, in the following chapters, it is assumed that every platform in the battalion acting as a host has performed the operation described in chapter 3.6.1 and 3.6.2 in order to discover the initial access router in the scenarios. It is also assumed that every platform in the battalion has performed the base configuration at the home network. By that every platform in the battalion has a topology correct Home Address. The Home Address is used for ad hoc routing within the battalion. Every platform in the battalion also knows the Home Agent IP address. The access router is assumed to perform the operations described in chapter 3.6.3 in order to maintain local ad hoc traffic within the battalion. For communication within the battalion the general AODV routing operations described in chapter 3.5.2 are implemented.

The access router performs mobile router functionality described in chapter 3.3. The internal network interface, the interface used towards the ad hoc network, of the router is pre-assigned with a Home IP Address. Communication within the battalion is performed with the AODV ad hoc routing protocol with pre-assigned home addresses as identifiers for the platforms. The external interface that interworks with the core network through an access network is auto configured with a topology correct IP address by the next-hop network layer node, the Access Gateway. The auto configuration mechanism is described in chapter 3.1.3. The access router sends the assigned care-of address together with its home address network prefix to the Home Agent at the NLC. This is done with the Mobile Router Binding Update message described in chapter 3.3.2. Any packet sent by corresponding node on the core network to the mobile router platform itself, or any host platform on the internal ad hoc network behind it, is sent to the Home Agent at the NLC. Then the packet is tunnelled from the Home Agent to the access router, see Figure 5.1.

Any platform within the battalion that wishes to initiate a communication to an external node on the core network goes through the access router platform, which tunnels the packets to the Home Agent at the NLC. From the NLC the packet is de-tunnelled and transported through the core network to the corresponding node in a general internet routing fashion. This hides the location of the platform to the corresponding node, and also protects the often low performance access network link from a direct usage from corresponding node. It is also considered crucial to hide the access network location in the address hierarchy due to certain attacks, for example Denial of Service. Therefore triangular routing is avoided.

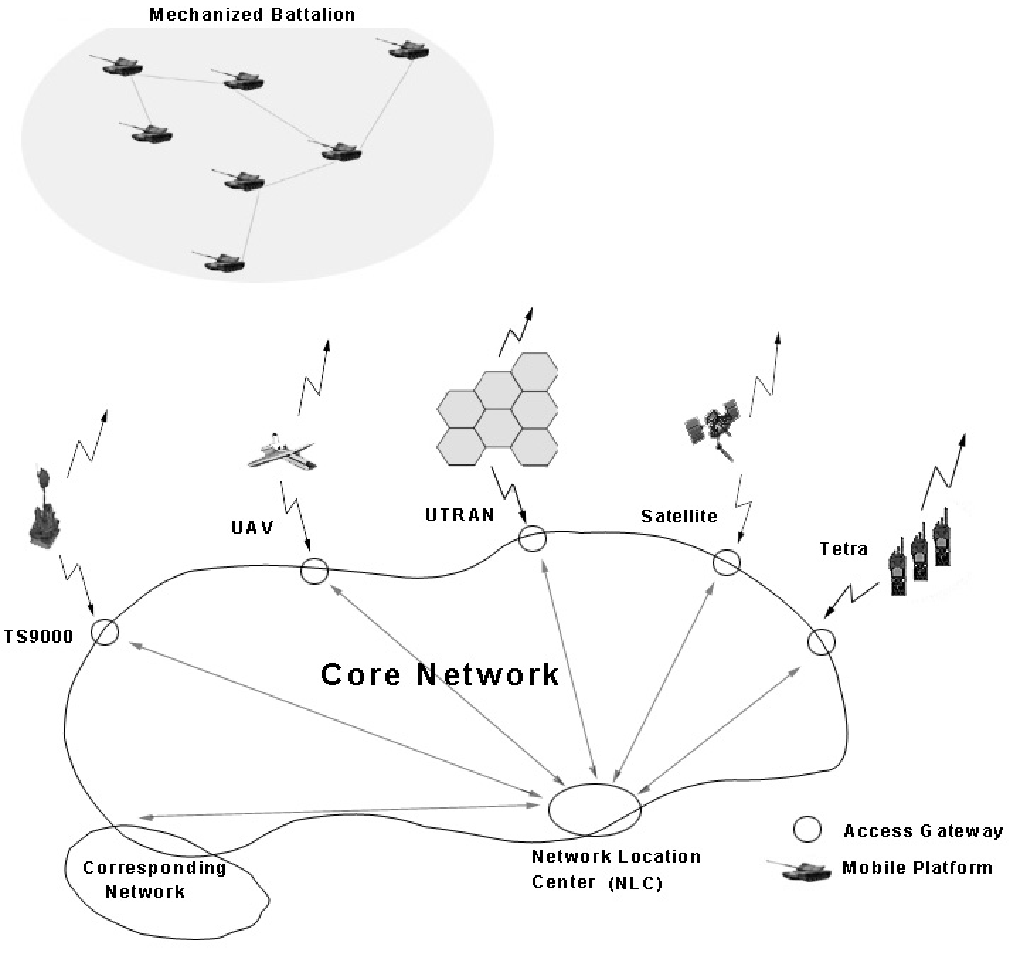


Figure 5.1: Network Location Centre

5.2 Scenario 1. Access network variation

5.2.1 Ad Hoc Access Router Platform Operations

In this scenario the initial access network is destroyed. The access router notices this, either by a broken connection to the access gateway, router advertisement timeouts or any other mechanism described in chapter 3. In this scenario the access router has an additional satellite interface available to interoperate with Core Network. The access router sets up the link and is assigned a topology correct IP address from the access gateway trough address auto configuration. The access router then updates the Home Agent at the NLC with this new information through a Router Binding Update message. Packets send to the battalion from corresponding nodes are now pinpointed to the correct location.

5.2.2 Home Agent Operations

The Home Agent perform authentication of the binding messages received from the platforms in the mobile battalion, in this case the access router platform. After authentication the Home Agents binding cache is updated with the new many-to-one relation binding entry. All packets received from corresponding nodes to mobile platforms are tunnelled from the Home Agent to the access router platform in ordinary Mobile IPv6 procedures.

5.2.3 Ad Hoc Host Platform Operations

The change of access network is transparent for the hosts in the ad hoc network. The access router platform can still be reached by the initial Home Network IP address attached to its internal interface.

5.3 Scenario 2. Access router variation

5.3.1 Ad Hoc Access Router Platform Operations

In scenario 2, the current access router is destroyed. A new access router can either manual be selected by an management application, or a access router with available interoperating interface can automatically set up a new link when it notice that access router in its routing table becomes unavailable. The new access router could multicast a RREP message carrying information saying that it’s now available as an access router, the “I” flag. The new access router also joins the INTERNET_GATEWAYS multicast group, described in chapter 3.3.1.

The new access router should multicast a RERR message, with the old access router IP address, to the ad hoc network indicating the failure of the previous access router platform. Hosts in the network should then delete the default route entry in their routing tables and initiate the access router discovery procedure, if needed.

5.3.2 Home Agent Operations

The Home Agent receives a Mobile Router Binding Update message from the new access router. When the message it authenticated, the Home Agent should send a Binding Refresh Request message to the old access router platform. If the previous access router sends no response to the request, the old entry should be deleted. Then all packets address to the ad hoc network should be tunnelled to the new access router.

5.3.3 Ad Hoc Host Platform Operations

When a host has not received a RERR message indicating the failure of the initial access router and detects the failure of the access router, it starts the gateway discovery procedure described in chapter 3.6.1 to find any additional available access routers. This is done if the platform itself is not capable to act as a new access router for the ad hoc network. If the host finds a new default router it then updates its routing table with the new access router entry.

5.4 Scenario 3. Ad hoc split

5.4.1 Ad Hoc Access Router Platform Operations

In this scenario the ad hoc network is divided into two separated ad hoc networks. The initial access router still performs router functionality for the remaining nodes in the initial network.

The separated part of the ad hoc network can chose a new available platform to act as the access router in order to interwork with the Core Network. This can be done when a platform in the network cannot reach the default access router or it can be initiated manually by a management application. The new access router joins the INTERNET_GATEWAYS multicast group and sends a Mobile Router Binding Update message to the Home Agent. The new access router could also send out an RREP message with the "I" flag set.

5.4.2 Home Agent Operations

If the Home Agent already has a binding entry for the ad hoc network it sends a Binding Refresh Request to the existing access router as described in chapter 5.3.2. In this case a reply is received.

In this situation the Home Agent has two binding entries for the ad hoc network and consequently two tunnels. This could indicate an ad hoc split but also a multihoming scenario described in chapter 5.5. An example of duplicate binding entries for the same network prefix:

```
1. 3ffe:306:1130:100::/64 -> Care-of-Address1.
2. 3ffe:306:1130:100::/64 -> Care-Of-Address2.
```

If a Home Agent receives a packet from one tunnel not destined to a corresponding node on the Core Network but to the same network prefix as the source IP of the packet, it assumes there has been an ad hoc network split. The packet is then tunnel to the other tunnel available. The reason the Home Agent can assume a network split is that every access router available in the ad hoc networks must have reverse routes for every node participating in the ad hoc network. The access router would not have sent the packet to the Home Agent if the source address of the packet could be reached within the ad hoc network. This is described in chapter 3.6.3.

If there are numerous ad hoc split and in result more then two binding entries with the same network prefix these binding must be managed manually in order to decide to which access router the packet should be sent. An alternative could be to send the packet to both access routers and after receiving an ICMP “no route to host” message from one access router this would indicate where the destination node is.

Corresponding node is not aware of the ad hoc network split and any packet addressed to any of the platforms in the divided ad hoc network is sent to the Home Agent as usual. The Home Agent must then decide to which access router the packet should be sent. The Home Agent is not aware of which nodes are situated behind an access router, only the available access routers.

The location of a platform in the divided ad hoc network could be recorded when the platform communicates with corresponding nodes on the core network. When an additional corresponding node wishes to reach a platform in the divided ad hoc network, the packets are tunnelled to the correct access router. This should be managed by an application at the home agent that influenced the traffic redirect service by editing the binding cache with appropriate one-to-one relationships.

If there are no such recordings at the home agent the ICMP approach described above could be used to acquire the location of a platform.

5.4.3 Ad Hoc Host Platform Operations

The access router of each of the ad hoc has a reverse route for all the platforms in the ad hoc network it serves.

If a host desires to communicate with a platform in the other part of the ad hoc network it sends the packet to the access router. The reason for this is either that the host does not have a host route entry, or that a RERR message is returned if the packet is sent to an old host route entry. The access router then, as it does with all the packets it receives from the internal interface which it does not have a reverse route for, sends the packet through the tunnel to the Home Agent.

5.5 Scenario 4. Multihoming

5.5.1 Ad Hoc Access Router Platform Operations

Initially, there is one access router available in this scenario. In addition, when using the UAV as an alternative access network, a second access router is introduced in the ad hoc network. The new access router must configure a topologically correct IP address on the external interface. This is done through the address auto configuration process described in chapter 3.1.3. The new access routers must also join the INTERNET_GATEWAYS multicast group and send a RREP message with the “I” flag set as described in chapter 3.6.1 and send a Mobile Router Binding update message the Home Agent.

5.5.2 Home Agent Operations

When the home agent receives a binding update message from an additional access router in the ad hoc network, the home agent must send a Binding Refresh Request to the initial access router as described in chapter 5.3 and 5.4. The reason for this is to ensure that the ad hoc network can still be reached by the initial access router. In this case the initial access router is still available and sends a response to the home agent. The home agent now has two binding entries to the ad hoc network and to available tunnels. When the Home Agent receives a packet from any of the tunnels it forwards the packet to the corresponding node over the core network. When the Home Agent receives a packet from the corresponding node to the ad hoc network the Home Agent can decide which tunnel and to which access router the packet will be sent. The decision can be made depending on the cost of the access networks or the Home Agent can keep a record of the above layer session and send the packet back to ad hoc network via the tunnel it received the initial packet.

5.5.3 Ad Hoc Host Platform Operations

If there are several access routers available in an ad hoc network they need to be identified by the hosts in the ad hoc network. An additional column in the host route table is introduced in order to identify which node in the table is capable to act as an access router. The “Access Network Cost” entry is a value indicating that the node in the “Destination IP Address” field is acting as an access router. If the value is set to 0 this is an indication that the node is not acting as an access router. Any value above 0 is used as a priority to arrange the available routers after some scheme, for example highest/lowest cost.

The value in the “Access Network Cost” column could be pre-assigned to an IP address if the available access routers are known in the initial configuration. For example, an IP address assigned to a possible satellite access route could have a low “Access Network Cost” value indicating the high cost of this particularly access network. The value could also be set dynamically by the access routers and be carried in the RREP message with the “I” flag set. The bits used by the value could be taken from the reserved field in the RREP message illustrated in chapter 3.5.1 (not including the I flag).

Destination IP Address	Destination Seq. Nr.	Valid Destination Seq. Nr.	Interface	Hop Count	Next Hop	List of Precursors	Lifetime	Routing Flags	State	Access Netw. Cost

Table 5.1: AODV node routing table modification

The host must choose the default router out of the available access routers in the routing table on every packet destined to the core network. The IP-stack algorithm at the host controls which default router to choose. The algorithm itself can and should be controlled by an application with additional information about the available access networks. For example the UAV in scenario 4 described in chapter 2.4 could have a low value in the “Access Network Cost” column but is available to only one platform in the battalion because of its need to use the entire bandwidth. The access network control application should be updated by an application level network protocol.

5.6 Scenario 5. Node Roaming

5.6.1 Ad Hoc Access Router Platform Operations

Access routers in this scenario are not affected in addition to their ordinary operations. The Access router in the “home ad hoc network” should delete the reverse route to the nomadic host after either a RERR messages is propagated through the ad hoc network or the reverse route entry simply times out. This action indicates that the nomadic node is not available in the home network anymore and that packet destined to that node should be sent to the default route by hosts in the ad hoc network. The default route then sends the packets to the Home Agent.

5.6.2 Home Agent Operations

In order to accommodate a nomadic platform moving between ad hoc networks we introduce a priority scheme in the binding management at the home agent. If the Home Agent receives a packet, either from a node in the Ad Hoc network or any corresponding node on the core network, it checks the binding cache for a one-to-one relationship that match the packets destination. If such exists the packet is tunnelled to the care-of-address of the binding. If it does not exist the Home Agent sends the packet according to the many-to-one binding matching the destination network. The Home Agent must prioritise a one-to-one relationship higher then a many-to-one relationship in its binding table. An example:

The destination IP of a packet received by the Home Agent is:

```
3ffe:306:1130:100:4:3:ff56:12
```

And the following binding entries exist:

```
1. 3ffe:306:1130:100::/64 -> Care-of-Address1.
2. 3ffe:306:1130:100:4:3:ff56:12 -> Care-Of-Address2.
```

The entry number 2 is used to forward the packet to the care-of-address2.

5.6.3 Ad Hoc Host Platform Operations

The host detects its presence at the new ad hoc network, either by lost connection to the default route entry and the discovery mechanism described in chapter 3.6.1, or by the Mobile NDP described in chapter 3.2.3. The later should not be used considering the high cost of sending unsolicited router advertisement over low bandwidth ad hoc links. After the detection the platform performs the usual address autoconfiguration to obtain a care-of-address on the visiting network described in chapter 3.6.1 and send a Host Binding update to the Home Agent.

6. Evaluation

6.1 Seamless connectivity

The initial goal was to maintain seamless connectivity for layers above the network layer in the five scenarios described in chapter 2. This could, with the modification described in the following chapters, be achieved with more or less latency. In the following chapter we will try to round up the functions that where not available by the chosen techniques in chapter 3 to accommodate the tactical scenarios. Further on in chapter 6.3 and 6.4 additional comments on security, robustness and traffic load are discussed.

6.2 Additional functions

In scenario 1 (access network variation) no additional function at the network layer is needed. The loss of the initial access network could be considered equal to the more traditional scenario where the mobile access router moves out of range from the access router.

In scenario 2 (access router variation) no additional function at the network layer is needed either. But the detection of the failure of the access router could be management by an application in order to increase the efficiency.

In the third scenario (ad hoc network split) new functions must be introduced to fulfil reachability to the platforms when they are separated. A method to manage the location of the platforms and the available access networks is needed.

In the fourth scenario (multihoming) the available access routers must be managed to handle the variety of quality at the access networks. The network layer does not provide this function. As a result, a method must be introduced to manage the access networks.

In the last scenario (node roaming) the roaming platform is equal to an ordinary Mobile IPv6 defined mobile platform that moves between fixed networks. No additional functionality needs to be introduced in this scenario.

The modifications described in chapter 5 are mainly at the Home Agent, leaving the network protocols and additional network nodes unmodified, with the exception of the RREP message in AODV and the additional column at the routing table. The modification is summarised below:

- An additional column at the ad hoc node AODV routing table to indicate the cost of the access networks.

- Home Agent Binding priority scheme to manage the many-to-one and one-to-one relationship.

- Function at the Home Agent to manage multiple available access networks in regards to cost and availability.

- Recording of the used access router used by an ad hoc platform when communicating with corresponding nodes if there is multiple prefix binding entries at the home agent.

- The additional cost variable in the RREP message sent out by access routers to indicate the quality of the access network.

6.3 Security considerations

The data must be transferred in a secure manner over the network. Protection against eavesdropping and manipulation of data is crucial. Encryption can be performed at various levels in the network infrastructure to ensure the integrity of the data. IPsec [3] provides homogenous encryption at the network layer throughout the network infrastructure. The impact on IPsec in a highly dynamic environment, such as described in chapter 2, should be investigated further. The use of a key-exchange protocol for management of the IPsec-defined keys should be considered a vast security threat in a Mobile IPv6 environment. The robustness of the suggested mobility management model described in chapter 5 is also a security consideration. Mobile IPv6's Home Agent is a single point of failure in the network. If the Home Agent becomes unavailable the location of the mobile nodes in the ad hoc network cannot be reviled.

The access router could initiate a new communication with an additional Home Agent and be able to communicate with corresponding nodes. Corresponding nodes, however, cannot initiate communication to any of the nodes in the ad hoc network when the initial Home Agent is unavailable because of the triangular routing procedure. A distributed network of Home Agents could solve this issue. The network of Home Agent would provide a redundancy to the ad hoc network. The Home Agents would have to exchange information whenever the ad hoc network changes access gateway to the core network in order to be able to serve corresponding nodes if the primary Home Agent fails.

6.4 Traffic considerations

The traffic in the suggested network layout always goes through the Home Agent. This triangular routing procedure could be considered to be a bottleneck when discussing traffic load. Though Mobile IPv6 has features to avoid triangular routing, to ease the traffic from the routing paths to and from the Home Agent, traffic load is not considered an issue in the described scenarios.

The core network is considered to be a secure high bandwidth network. The traffic generated by the low bandwidth ad hoc network would not be a problem either to the network path to the Home Agent or the Home Agent itself. When it comes to traffic going to the ad hoc network, triangular routing could be a way to manage the load to the low bandwidth ad hoc network.

7. Further Research

7.1 Mobility Management Application, MMA

Mobile IPv6 cannot fully cope with the events described in chapter 2. In chapter 5 we often referred to an application providing functions that Mobile IPv6 together with AODV does not provide.

This application would have to manage the different types of access networks available accordingly to the given scenario. The Network Location Centre together with other network functions additional to mobility management would control the application.

We introduce a Mobility Management Application (MMA) to raise the management of the unavailable necessary operations at the network layer to the application layer. The MMA application could be considered to be equal, from a system interconnection point of view, to other more traditional network layer management application like a firewall or IPv4 network address translation applications. But in this case the MMA application would manage the mobility through binding cache management.

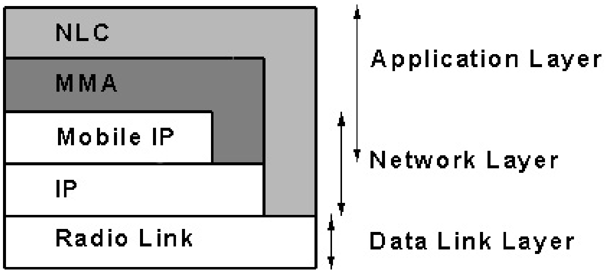


Figure 7.1: System interconnection model at the Home Agent

Figure 7.1 illustrates the relationship between the Network Location Centre, Mobility Management Application, Mobile IP, IP and the Data Link Layer. The MMA controls the Bindings at the Home Agent in regards to the additional function introduced in chapter 6.2. The NLC controls the MMA and also additional conceptional functions at the Network Layer such as encryption and authentication, for example firewall and proxy functionality. The Data Link Layer is not affected. The NLC provides external information about the access networks to the MMA. The MMA manages the Mobile IPv6 binding cache in regards to the external information about the cost and availability of the existing access networks.

The practical interworking between the application and the network layer is done through Binding Cache manipulation at the Home Agent.

8. Conclusions

Mobile IPv6 together with AODV is not enough to manage the access networks in a military tactical scenario, such as a mechanised battalion interworking with a core network. Mobile IP uses the access networks in a “best effort” manner with no concern about the availability, quality or tactical consideration. These concerns must be included in the management of the access networks.

In this master thesis a mobility manage model is introduced, which includes a conceptional Network Location Centre and a Mobility Management Application. These two services together with Mobile IPv6 and AODV could provide seamless traffic management and connectivity to host applications in the network centric warfare system with the additional concerns. The application could be administrated or automatic provided with external information not available in the network and control the Mobile IP layer and the traffic redirect operations. The Network Location Centre would manage additional concerns as traffic load and tactical consideration.

The introduction of an application that influences the network layer is against the traditional concept of the Open System Interconnection model. But these types of applications are today a standard in network engineering. Firewall applications for instance, affects the networking layer with security management not available at the network level. Network and Port address translation application also affects the network level to accommodate the lack of addresses in IPv4.

Firewall applications provides authorisation management at the network layer, Network and Port Address Translation applications provides address management at the network layer, and just as equal the Mobility Management Applications would provide seamless mobility management at the network layer. The application could be controlled by a rule scheme similar to the one used in firewall management. The rules could be management both manual, by a mobility administrator, and by Mobile IPv6 signalling through binding messages.

References

[1] B. Adamson, “Tactical Radio Frequency Communication Requirements for Ipng”, RFC1677, August 1994.

[2] Björn von Sydow, “Fortsatt förnyelse av totalförsvaret”, Government Bill 2001/02:10

[3] S. Deering, R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC2460, December 1998.

[4] Fredrik Grahn, “Struktur Taktiskt internet”, AerotechTelub, Mars 2002, Work in Progress.

[5] Fuller, V., Li, T., Yu, J., and K. Varadhan, "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy ", RFC 1519, September 1993.

[6] Fredrik Alriksson and Ulf Jönsson, “MIPMANET Mobile IP for Ad Hoc Networks”, Sweden 1999.

[7] Ryuji Wakikawa, Jari T. Malinen, Charles E. Perkins, Anders Nilsson, Antti J. Tuominen, “Global Connectivity for Ipv6 Mobile ad hoc Networks”, Work in Progress.

[8] S. Thomson, T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC2462, December 1998.

[9] David B. Johnson, Charles Perkins, "Mobility Support in IPv6", Work in Progress.

[10] T. Narten, E. Nordmark, W. Simpson "Neighbor Discovery for IP Version 6 (IPv6)" RFC 2461, IBM, Sun Microsystems, Daydreamer, December 1998.

[11] Thierry Ernst, Ludovic Bellier, Castelluccia Claude, Hong-Yon Lach, “Mobile Networks Support in Mobile Ipv6”, Work in Progress.

[12] Timothy J. Kniveton, Jari T. Malinen, Vijay Devarapalli, Charles E. Perkins, “Mobile Router Support with Mobile IP”, Work in Progress.

[13] S. Corson, J. Macker, “Mobile ad hoc Networking: Routing Protocols Performance Issues and Evaluation Considerations”, RFC2501, January 1999.

[14] Charles E. Perkins, Elizabeth M. Belding-Royer, Samir R. Das, “ad hoc On-Demand Distance Vector (AODV) Routing for IP version 6”, Work in Progress.

[15] F. Eklöf, B. Johansson, “On situation awareness for a mechanized battalion in two tactical scenarios“, Defence Research Establishment, Division of Command and Control Warfare Technologies, FOA-R-00-01734-504-SE, Linköping, Sweden, December 2000.

Glossary

ad hoc	”For this purpose”
internet	A set of autonomous networks forming an homogenous system using IP technology.
Internet	The civilian world wide internet.
network cost	Can be different type of priority factors. For instance bandwidth, security consideration or actual cost in money
node	A device that implements IP.
router	A node that forwards IP packets not explicitly addressed to itself.
host	Any node that is not a router.
upper layer	A protocol layer immediately above IP. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunnelled" over (i.e., encapsulated in) IP.
access router	The node in the mobile network that is attached to the access gateway through the access network.
mobile router	The border router of the mobile network that attaches the mobile network to the rest of the Internet. Mobile Router maintains the internet connectivity for the mobile network. It is used to route packets between the mobile network and the fixed Internet.
access network	A Data Link Layer radio technology that provides a link between the mobile network and the internet.
access gateway	The network layer border router that is attached to both the internet and to the mobile network through an access network.
link	A communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IP. Examples are Ethernets (simple or bridged); PPP links; TS9000, UMTS, or ATM networks; and internet layer "tunnels", such as tunnels over IP itself.
neighbours	Nodes attached to the same link.
interface	A node's physical attachment to a link.