
# *IPv6 - Prospects and problems. A technical and management investigation into the deployment of IPv6.*

By

Mette Olsen & Siw Ånonsen

Masters Thesis in
Information and Communication Technology

Agder University College

Grimstad, May 2003

# Abstract

IPv4 has been used for over twenty years, and will most likely be used in many years ahead. However, we are now experiencing that the IPv4 address space is running out, resulting in restrictions on who will be able to get these types of addresses assigned to them. Methods such as Network Address Translator (NAT) have been developed and implemented in order to save the IPv4 address space. It is said that this is not a good enough solution, as such techniques introduce new problems at the same time solving some.

A new version of the Internet Protocol, IPv6, has been developed and is likely to replace IPv4. IPv6 has been developed to solve the address problem, but also new features are designed to supposedly enhance network traffic.

In our thesis we give an overview of the problems with IPv4. This includes the limited address space and the limited quality of service. Further we present the features of IPv6 that are meant to solve these problems and add new possibilities. These are: New address format, the IPv6 header and Extension headers to mention some.

Further we have investigated and here present how the transition from IPv4 to IPv6 is expected to take place, followed by a thorough description of the transition mechanisms. One of the original intentions on the development of IPv6 was that IPv4 and IPv6 have to be able to coexist for a long period of time. Transition mechanisms have therefore been designed to make this possible. There are three main types of mechanisms:

- Tunnelling
- Translation
- Dual-stack

Each of these mechanisms requires different configuration and implementations in hosts and network.

Technical research on transition mechanisms states that these are not good enough for all IPv6/IPv4 scenarios and need improvements in order to make IPv4 and IPv6 coexist smoothly. There are a lot of transition mechanisms that are agreed upon as being good for general use and then there are transition mechanisms that are good for certain scenarios and not for others. Some scenarios still lack a good translation mechanism. As a result of this, IPv6 networks are being built separately from IPv4 networks. In Asia commercial IPv6 networks are offered, while the process is slower in other parts of the world. The reasons for not building IPv6 networks are many, and not agreed upon. Some believe it is because of economical restrictions, while others claim it is technical reasons and that it exists far too few applications supporting IPv6. The number of IPv6 enabled applications is growing. Large companies like; Microsoft Corporation, Cisco Systems Inc, Apple Computers Inc., Sun Microsystems Inc and various versions of Linux include support for IPv6.

The deployment of IPv6 is expected to happen at different times in different parts of the world. We have investigated the status of IPv6 globally and in Norway. The main results are

that the roll-out has reached the furthest in Asia where commercial IPv6 networks already are offered. The activity in Norway is still small, but growing.

It was desired to run an experiment in order to prove or disprove some of the information we gathered on how IPv6 interoperates with IPv4, but because of limitations in the network at Heriot-Watt University we were not able to do this. Instead we have focused on a project by Telenor R&D; "IPv6 migration of unmanaged networks-The Tromsø IPv6 Pilot". We also gathered some information from people working at Norwegian ISPs in order to address some of the aspects of the upgrading.

# Preface

This thesis is the final report at the Masters degree in Information and Communication Technology at Agder University College. The thesis represents 10 credits (one term full-time).

The thesis is given by Agder University College, but has been written in Edinburgh where we have had a supervisor at Heriot-Watt University. The work has been carried out from January 2003 till May 2003.

We would like to thank our supervisor Dr. Peter King at Heriot-Watt University, our Norwegian contact Geir Køien and the Director of studies at Agder University College, Stein Bergsmark.

Edinburgh,

May 2003

Mette Olsen

Siw Ånonsen

# Table of contents

# List of figures



# List of tables

# Abbreviations

| | |
|---|---|
| ALG: | Application Layer Gateway |
| API: | Application Programming Interface |
| APNIC: | Asia Pacific Network Information Centre |
| ARIN: | American Registry for Internet Numbers |
| ARPANET: | Advanced Research Projects Agency NETwork |
| BIA: | Bump-in-the-API |
| BIS: | Bump-in-the-Stack |
| CIDR: | Classless Inter-Domain Routing |
| CPU: | Central Processing Unit |
| DARPA: | Defence Advanced Research Projects Agency |
| DHCP: | Dynamic Host Configuration Protocol |
| DNS-ALG: | Domain Name System-Application Layer Gateway |
| ESP: | Encapsulating Security Payload |
| EUI: | Extended Unique Identifier |
| FFI: | The Norwegian Defence Research Establishment (Forsvarets Forskningsinstitutt) |
| FTP: | File Transfer Protocol |
| GPRS: | General Packet Radio Service |
| GSM: | Global System for Mobile communications |
| HTTP: | HyperText Transfer Protocol |
| IANA: | The Internet Assigned Number Authority |
| ICMP: | Internet Control Message Protocol |
| ICS: | Internet Connection Sharing |
| IEEE: | Institute for Electrical and Electronics Engineers. |
| IETF: | Internet Engineering Task Force |
| IIJ: | Internet Initiative Japan |
| IMAP: | Internet Message Access Protocol |
| INWG: | InterNetworking Working Group |
| IPng: | Next Generation IP |
| IPTO: | the Information Processing Techniques Office |
| IPv4: | Internet Protocol version 4 |
| IPv6: | Internet Protocol version 6 |
| IR: | Infrared |
| ISATAP: | Intra-Site Automatic Tunnel Addressing Protocol |
| ISP: | Internet Service Provider |
| MAC: | Media Access Control |
| MPLS: | Multi Protocol Label Switching |
| NAPT-PT: | Network Address Port Translator – Protocol Translator |
| NAT: | Network Address Translator |
| NAT-PT: | Network Address Translator – Protocol Translator |
| NCP: | Networking Control Protocol |
| NIX: | Norwegian Internet Exchange point |
| NLA: | The Next-Level Aggregation identifier |
| NTNU: | The Norwegian University of Science and Technology (Norges Teknisk-Naturvitenskapelige Universitet) |

| | |
|---|---|
| NTT: | Nippon Telegraph and Telephone |
| QOS: | Quality of Service |
| R&D: | Research & Development |
| RF: | Radio Frequency |
| RFC: | Request For Comments |
| RIPE-NCC: | Réseau IP Européens - Network Coordination Centre in Europe |
| RIR: | Regional Internet Registries |
| RPC: | Remote Procedure Call |
| SIIT: | Stateless IP/ICMP Translation |
| SLA: | The site-level aggregation identifier |
| SOCKS64: | SOCKS-based IPv6/IPv4 Gateway Mechanism |
| SSL: | Secure Socket Layer |
| sTLA: | sub TLA |
| TCP: | Transmission Control Protocol |
| TLA: | The Top-level Aggregation identifier |
| TOS: | Type of Service |
| TOTD: | Trick-Or-Treat Deamon |
| TRT: | Transport Relay Translator |
| TTL: | Time To Live |
| UDP: | User Datagram Protocol |
| UIT: | The University in Tromsø (Universitetet i Tromsø) |
| UMTS: | Universal Mobile Communications System |
| VPN: | Virtual Private Network |

# 1 Thesis introduction

## *1.1 Background*

The existing Internet protocol, IPv4, has been used for over twenty years, and has so far proven to be adequate. However, we are now experiencing a large growth of IP address consumers as more and more connections to the Internet are being made and as new technologies using IP addresses are designed [1]. This leads to an exhaustion of the already pressured IPv4 address space. Methods such as NAT have been implemented to make better use of the IPv4 addresses, but these methods are said to destroy some of the original features about the Internet Protocol, e.g. loss of transparency and loss of unique addresses [2]. With the growth in Internet hosts, the routing tables get more complex, leading to an increase in processing time. Additionally, new technologies are created that require better quality of service (QoS) than available in IPv4 [3]. These technologies can be real-time applications that are non-tolerant to loss of packages.

The limited address space and need for improved quality of service are strong indications to the fact that IPv4 needs a replacement. At what time the change from IPv4 to IPv6 will take place, and how this will be done, are still highly relevant questions [4]. The Internet Engineering Task Force (IETF) began looking at the problem of expanding the IP address space in 1991, and several alternatives were proposed [5]. However, to our knowledge, since the year 2000 there has not been any serious considerations to any other alternatives than IPv6.

What first was known as IP next generation (IPng) eventually was named IPv6. As the work progressed it was agreed upon that several features about IPv4 in addition to the address space needed an upgrading. The essential areas were [3]:

- Support for real-time services.
- Security support.
- Autoconfiguration.
- Enhanced routing functionality.

An interesting point is that in the recent years, support for all of these features has been designed for IPv4 [3].

Another nonnegotiable feature about the next generation IP was that there must be a transition plan [1]. It is not possible to set a Flag Day, where everyone upgrades to IPv6. Therefore, mechanisms are designed to make IPv4 and IPv6 coexist. The main intention for these mechanisms is that they will make it possible to upgrade individual hosts without being dependent on the network. Also, a network is supposed to be able to upgrade, without forcing all the connected hosts to do the same. The transition should be smooth, and will be an interim state that will last for an unknown number of years.

## 1.2 Thesis definition

We will investigate the results/consequences of the deployment of the next generation IP. The final thesis definition is therefore formulated as follows:
*"Considering the limited address space, an upgrading to IPv6 seems necessary. The transition from an IPv4 based infrastructure to an IPv6 infrastructure is said to have several difficulties, and a part of our thesis will be to locate these. This includes an investigation on the resources needed, what needs upgrading and when. The technical management of the introduction of IPv6 in the organisations will also be addressed."*

*"If feasible we will set up an experiment and do some tests, to prove or disprove the information we have found. Our priority will be on fixed networks. If the experiment can not be done, we will concentrate on the theory and if found the experiences of companies or organisations already using IPv6."*

In agreement with our supervisor Dr. Peter King and our Norwegian contact Geir Køien, an experiment was not run. Therefore we will focus on the experiments and experiences by other companies or organisations.

The title of the thesis was formulated as follows:

*"IPv6 – Prospects and problems. A technical and management investigation into the deployment of IPv6."*

## 1.3 Our work

As mentioned in chapter 1.1, Background, the Internet community will be challenged as a result of shortage of IPv4 addresses. The next step seems to be a new generation of IP, IPv6.

The main questions that we will investigate in this thesis are:

1) Which new features will the next generation IP contribute to networks?
2) Which resources are required for an upgrade and when must the upgrade take place?
3) How will the upgrade be done according to the complexity of IPv6?

To answer these questions we will mainly use the Internet for material on the subject. If possible, we will get information from companies or organisations that have already made the transition to IPv6.

The main source on the Internet will be information from Internet Engineering Task Force (IETF). At the beginning of this project we know of three RFCs that are of interest; RFC 2460 - *"Internet Protocol, Version 6 (IPv6) Specification"* [6], RFC 2373 - *"IP Version 6 Address Architecture"* [7] and RFC 2464 - *"Transmission of IPv6 Packets over Ethernet Networks"* [8]. These and more RFCs will help us answer the questions about what IPv6 will contribute to networks and which resources are needed.

To find organisations and companies that have already started to experiment with IPv6 or use it, we will start by looking at the IPv6 test network, 6Bone, which is a world-wide network.

We will focus on Norwegian companies to gather information as we think these will be the most likely to answer our queries. This will help us answer the questions about what needs upgrading and when, in Norway.
To gather information about the upgrading world-wide, we will have to look at the major ISPs and look at any information they have publicised about what they can offer at this stage. For additional rollout plans the different IPv6 Task Force groups around the world provide information on political level. We will focus on the three regions that are: Asia-Pacific, Europe and USA. These are so-called Regional Internet Registries (RIR).

On the subject of managing an upgrade to IPv6 we will concentrate on investigating how IPv6 is being introduced by e.g. the ISPs. We will look at whether the IPv6 network will be kept separately at the first stage of the deployment or whether it will be merged with the existing network from the start.

To investigate the experiences and experiments done on IPv6, we will focus on a project done by Telenor in Norway [9], which resembles the experiment we intended to do. We will give a description of the project and the results made. To add to this information on the experiences done with IPv6 we will contact companies that use or experiment with IPv6 in Norway. This should help us to be able to either prove or disprove our findings done through our own investigation on IPv6.

## 1.4 Report outline

Chapter 1 is an introduction to the thesis, including background and thesis definition.

Chapter 2 and 3 will be concentrating on IPv4 and IPv6. We will locate the main problems about IPv4, and describe the current status on the protocol. Further we will give an overlook of what is supposed to make IPv6 work better than IPv4, and also a status of IPv6 will be given.

In chapter 4 the transition stage will be dealt with. Mainly as a description of the current transition mechanisms, to clarify what needs to be configured in the network and hosts for IPv6 enabling.

Chapter 5 will be on the IPv6 rollout. We will as far as possible give an overview on how far the transition to IPv6 has come, both world-wide and in Norway.

The experimental part of our project will be described in chapter 6. The chapter mainly focuses on an experiment performed by Telenor R&D, as it was not feasible to set up an experiment of our own. A thorough explanation on why an interesting experiment at Heriot-Watt University was not possible is also given in chapter 6.

In chapter 7 we will discuss our investigation and results, while a conclusion will be given in chapter 8.

# 2 IPv4

## 2.1 Introduction

In order to get a better understanding of chapter 3 that deals with IPv6 and the improvements over IPv4, this chapter addresses IPv4. The chapter gives a brief overview of IPv4, including the historic background and a technical description of the main features about IPv4. The problems about IPv4 are given a thorough explanation, while the chapter ends with the status of IPv4.

## 2.2 The IPv4 history

The Internet Protocol, IP, was originally known as the Kahn-Cerf protocol, named after its inventors Robert Kahn and Vinton Cerf [10].

In 1972 the Information Processing Techniques Office (IPTO) hired Kahn to work on network technologies, and during this year he developed a technique which connected 40 different computers to the Advanced Research Projects Agency Network (ARPANET). This work made the network known to people all over the world. After this he started the development of a standard open-architecture network model, where any computer was supposed to be able to communicate with any other, independent of individual hardware and software configuration.

Vinton Cerf joined Kahn on this project in 1973. Cerf was a former scientist at the Defence Advanced Research Projects Agency (DARPA) who also had been the chairman of the InterNetworking Working Group (INWG) from 1972. Together, they first studied reliable data communications across packet radio networks. They then investigated the Networking Control Protocol (NCP), and developed this further to what became TCP/IP.

Kahn and Cerf's first draft was titled "A protocol for Packet Networking Interconnection" [10]. This was finalised and presented at the IEEE Transactions of Communications Technology in May 1974. Together with two Stanford's graduate students Kahn and Cerf presented the first technical specification of TCP/IP as an "Internet Experiment Note" in December 1974.

Four versions of the protocol were developed with TCP and IP being separated into two different layers during the third version. The fourth version, IPv4 has been the standard Internet Protocol for over twenty years, and will still be used in many years to come. Much of its acceptance is gained because of its mechanisms, which tie together systems over a wide variety of disparate networking technologies. Many of the technologies over which IP run today, were not even invented when the Internet protocol was designed, and so far, not one technology invented has been too bizarre for IPv4 [1].

## 2.3 The growth of the Internet

The Internet has grown so large that an updating of the Internet protocol seems necessary. And more important, the growth will not stop. This is the major challenge for the next generation Internet protocol, and perhaps the most important thing to learn from IPv4; it must be able to manage a severe growth [2]. To predict the future growth it is important to understand the growth up till now. Today IPv4 serves what is referred to as the computer market. The computer market has been the driver of the Internet growth. It comprises the Internet and countless smaller intranets that are not connected to the Internet. The main goal is to connect together the computers in government, business, universities, and schools. The growth of the computer market has been exponential. The future growth of the computer market is not expected to be exponential, instead other markets are expected to represent the largest growth of the Internet.

Nomadic personal computers are one of the markets expected to grow substantially. This is due to the prices falling and their performance increasing. It is predicted that these computers will be consumer devices and replace the cellular phones, pagers and personal digital assistants of today. Unlike today's networking computers they will support a variety of network attachment technologies. These may be RF connectionless, IR connectionless and physical wires for example. The computers will need an Internet protocol, which supports a wide range of network technologies. The protocol must also support large scale routing and addressing. Low overhead due to the wireless media, autoconfiguration and mobility are other basic requirements.

Another market expected to grow is networked entertainment. The main reason for believing this is the rise of the digital high definition television that will make the difference between television and computer become smaller. The possibility is that every television set will become an Internet host. These devices will also need an Internet protocol that supports basic needs like large scale routing, addressing an autoconfiguration in addition to a minimum overhead.

Device control is also predicted to grow, and will be in the need of an Internet protocol. This market consists of devices such as lighting equipment, heating and cooling equipment and other types of equipment which are currently controlled via analogue switches and in aggregate consume considerable amounts of electrical power. The solutions for this market must be robust and simple.

## 2.4 A technical description of IPv4

### 2.4.1 The IPv4 header

Most of the fields are self-explanatory but are given a short description to get a better understanding of the comparison with IPv6 later in the document.

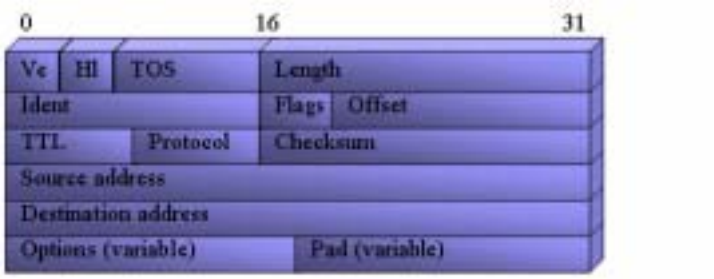


*Figure 2.1: The IPv4 header.*

The most usual length of the header is 20 bytes

- The *version* field indicates what Internet protocol version it is.
- *Header Length* gives the length of the header in 32- bit words, most of the time it is 5 words.
- *Type Of Service* indicates whether the packet should be given any different treatment in the network. The reason for the treatment could be application needs. The major choice when it comes to type of service is a trade-off between low delay, high throughput and high reliability. Beside higher costs, better performance for one of the parameters often leads to worse performance for another.


*Figure 2.2: The Type Of Service field.*

Bits 0-2 : Precedence
Bit 3 : 0 = Normal delay, 1 = Low delay
Bit 4 : 0 = Normal throughput, 1 = High throughput
Bit 5 : 0 = Normal reliability, 1 = High reliability
Bit 6 – 7 : For future use

- The *Length* field contains the length of the datagram, including the header. This field counts bytes, not words like the field *Header length.* This field is 16 bytes, and the maximal length of a datagram is 65 535 bytes.
- The *Identification* field is used to reassemble the datagram after a fragmentation, which is a value added by the sender.
- *Flags* are used for various control informations, such as fragmentation information.
- *Offset* indicates where in the datagram a fragment belongs.
- *Time To Live* indicates the maximum lifetime of a datagram.
- *Protocol* indicates the next level protocol used in the datagram.
- The *Checksum* field is the 1's complement sum of all 16-bit words in the header. For purposes of computing the checksum, the value of the checksum field is zero.
- *Options* is a field rarely used. It is optional to transmit them in an IP-datagram but they have to be implemented by all IP-modules.
- *Pad* is used to ensure that the datagram header ends on a 32-bit boundary.

### 2.4.2 Problems with IPv4

The Internet has lost a lot of the functionality it had in the early days because of the address conservation [11]:

- Loss of transparency, due to the use of mechanisms such as NAT (Network Address Translator).
- Loss of robustness because of the implemented topology that has little room for redundancy.
- Loss of unique addresses.
- Loss of stabile addresses, i.e. the address of a node changes each time it is connected to the Internet.
- Loss of connection-less services.
- Loss of "always-on" services.
- Loss of end-to-end communication model.
- Loss of application- independence. An example is that many systems are developed with functionality to avoid problems created by NAT.

The main reason for developing a new IP standard was the expected exhaustion of the address space, but also other features about the Internet Protocol is taken in consideration and found necessary to change or upgrade.

#### 2.4.2.1 Address space

The address space in IPv4 is expected to be exhausted within the next two to three years[12]. The exhaustion is a result of a growing number of hosts and networks connected to the Internet, and also because of an inefficient assignment of IPv4 addresses. This inefficiency arises because of the structure of the IP address space, divided in class A, B and C addresses. This structure forces network address space to be handed out in fixed size chunks of three very different sizes. This leads to a bad exploitation of the address space, especially of the class B addresses. Any network with more than 255 hosts would want one class B network prefix instead of several class C network prefixes. A class B network consisting of for only 256 hosts represents an efficiency of 255/65535 = 0, 39% [3]. To solve this, CIDR (Classless Inter-Domain Routing) has been developed. In addition to saving the address space, CIDR also slows the growth of backbone routing tables.

NAT is a method for mapping multiple private addresses to a single public address. There is a lot of scepticism towards NAT as it may be appropriate to some businesses that do not need full connectivity to the outside world, but for others, who require constant and robust contact with the Internet, NAT will not fulfil the requirements. It creates a bottleneck between the business and the Internet; it does not support end-to-end security and breaks the peer-to-peer model [13]. Another problem is when applications embed IP-addresses in the packet payload, above the network layer; these can be applications like FTP programs and mobile IP. Most likely NAT will fail in translating some embedded addresses and lead to application failure [14].

#### 2.4.2.2 Routing tables

Routing tables are large and complex. As the Internet grows, so do the routing tables. In order to achieve efficient routing the address hierarchy must be well organised. The system with

class A, B and C addresses of such different sizes together with the rationing of IPv4 addresses, Internet addressing and routing is complex. The use of CIDR is supposed to make routing more efficient, but it does not guarantee an efficient and scalable hierarchy [14].

#### 2.4.2.3 Configuration

In IPv4 one must either do a manual configuration or use a stateful address configuration such as DHCP. This is complicated, especially in cases where a company needs to reconfigure the entire network. It causes much downtime, which can lead to great costs. The configuration cause more administrative problems as the Internet and other markets that require an IP-address grow.

#### 2.4.2.4 Security

Packets sent at IP-level needs encryption to protect the private data from being viewed or modified.

The standard IP security, IPSEC, is optional and some claim there is a need for a better solution [1].

#### 2.4.2.5 Quality of service

In IPv4 this depends on the TOS field in the header. The field is limited and has had a number of definitions during the years [1].

### *2.5 IPv4 status*

IPv4 is still the standard Internet Protocol, and it seems likely to remain dominant in the next few years, though we already see some Ipv6 networks. Aside from the address space issue, other features about the IPv4 have been measured and found not good enough for the future Internet. However, Internet does not yet require an upgrading of the protocol based on the need for new features as better quality of service, as it still seems to work satisfying. The discussion today is most concerned with the expected address space exhaustion. Some believe we have solved the problem with techniques as NAT and CIDR. Others claim that NAT is a bad solution as it creates new problems at the same time as it saves the address space, and is not a competitor to IPv6. CIDR on the other hand does not create the same architectural problems as NAT, and is a technique that is as good as integrated in IPv4. The use of mechanisms such as NAT, has contributed in giving the development of IPv6 a slow start. Still, the pressure on IPv4 addresses is growing, and it is getting harder to get an IPv4 address. An example of this is the GSM association, which did not get enough addresses when introducing GPRS [9]. In the near future, the demand for IP addresses is likely to grow as technologies such as UMTS are widely spread. Especially in Asia, where very few IPv4 addresses have been assigned, the pressure is expected to be very big. Figure 2.3 shows the global distribution of the IPv4 addresses.

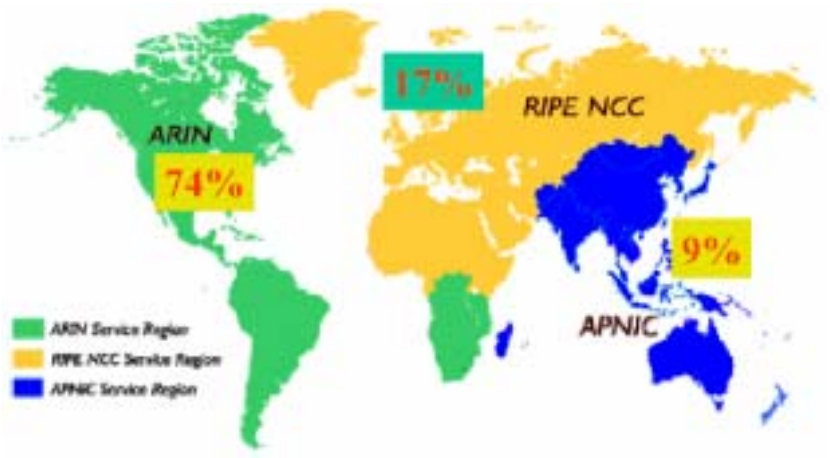


*Figure 2.3: The global distribution of IPv4 addresses.*

IPv4 is still accepted and respected, but many corporations and institutes have started the discussion and planning towards a transition to IPv6.

# 3 IPv6

## 3.1 Introduction

This chapter will present the reader with the necessary information on IPv6, so that the reader will be familiar with the differences between the new and the old protocol. This will give the reader a better understanding of the following chapters, when it is assumed that basic IPv6 theory is already known.

This chapter will in addition show some of the possibilities IPv6 will contribute to networks and which resources are needed to be able to upgrade the Internet protocol. It will highlight some of the issues concerning the complexity of IPv6. More on the complexity will be given in chapters 4 and 5.

## 3.2 The IPv6 History

IPv6 was recommended by the IPng Area Directors of the IETF at the Toronto IETF meeting on July 25, 1994 in RFC 1752. The recommendation was approved by the Internet Engineering Steering Group and made a Proposed Standard on November 17, 1994. The core set of IPv6 protocols were made an IETF Draft Standard on August 10, 1998[2].

The initiative to make a new version of the Internet protocol was mainly caused by the shortage in address space, as described in chapter 2. In addition there seemed to be possibilities to improve areas of IPv4 in the new version. The new version is supposed to allow new features in the Internet in the future to be added in a less complex way than today.

## 3.3 The new protocol, IPv6

IPv6 is designed to run well on high performance networks (e.g. Gigabit Ethernet) and at the same time still be efficient for low bandwidth networks (e.g. wireless). In addition, it has been taken into consideration that new technologies will appear in the future and IPv6 is designed to easily adjust to these.

IPv6 includes transition mechanisms, which are designed so that users should be able to adopt and deploy IPv6 in a way that provides direct interoperability between IPv4 and IPv6 hosts.

IPv6 is supposed to add further improvements in comparison to IPv4 in areas such as routing and network auto-configuration. IPv6 is expected to gradually replace IPv4, with the two coexisting for a number of years during a transition period [15].

## 3.4 Improvements from IPv4

### 3.4.1 New header format

The reasons for a next generation of IP are best shown through looking at the new header format for IPv6, shown in figure 3.1.

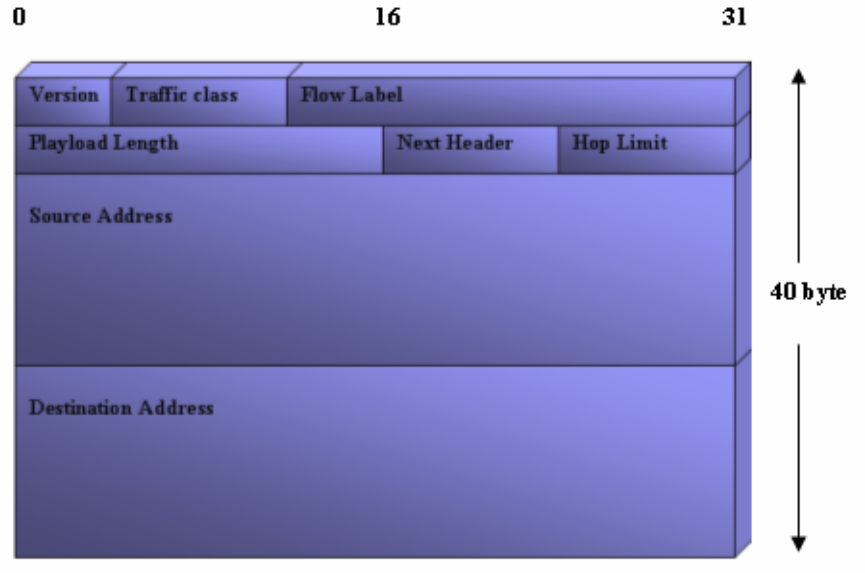


*Figure 3.1: The IPv6 Header format.*

**Explanation of IP Header fields:**

- The 4-bit *Version* field = 6, for IPv6
- The 8-bit *Traffic Class* field is available for use by originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets.
- The 20-bit *Flow Label* field may be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time" service.
- The 16-bit *Payload Length* field is a 16-bit unsigned integer, which indicates the length of the IPv6 payload, i.e., the rest of the packet following this IPv6 header, in octets. (The length of extensions is included).
- The 8-bit *Next Header* field is an 8-bit selector that identifies the type of header immediately following the IPv6 header. (The values are the same as those in the IPv4 Protocol field).
- The 8-bit *Hop Limit* field is an 8-bit unsigned integer that decrements by 1 by each node that forwards the packet. The packet is discarded if Hop Limit decrements to zero.
- The 128-bit *Source Address* field contains the address of the packet's originator.
- The 128-bit *Destination Address* field contains the address of the packet's recipient [6].

### 3.4.1.1 The improvements as a result of the new header

**Expanded Addressing Capabilities**

IPv6 increases the IP address size from 32 bits to 128 bits. This results in IPv6 being able to support more levels of addressing hierarchy. IPv6 allows a much greater number of machines to connect to the Internet and the auto-configuration of IP addresses is simplified. The scalability of multicast routing is improved, by adding a scope field to multicast addresses. And a new type of address called an "anycast address" is defined, which is used to send a packet to any one in a group of nodes [16].

**Header Format Simplification**
Some of the IPv4 header fields have been dropped or made optional. This reduces the routine processing cost of packet handling. It decreases the bandwidth cost of the IPv6 header.

**Improved Support for Extensions and Options**
Because of the way the IP header options are encoded it allows packets to be forwarded more efficiently. With IPv4, options were integrated into the basic IPv4 header. In IPv6 the options are handled as Extension headers. Extension headers are optional and only inserted between the IPv6 header and the payload, whenever necessary. In this way the IPv6 packets are believed to be more flexible and streamlined. In addition new options that may be defined in the future can be integrated more easily than for IPv4.

**Flow Labelling Capability**
IPv6 adds labelling on packets which enable packets of a certain type to get special handling on sender's request. This is for packets with non-default quality of service e.g. real-time service.

### 3.4.2 Header- and Extension headers processing

The IPv6 header has a total size of 40 bytes, which is twice the size of the IPv4 default header. But on a closer look the IPv6 header is simplified compared to the IPv4 header as the address-space alone consumes 32 bytes in IPv6. This leaves only 8 bytes with other header information [16]. This means that only 8 bytes will be processed at each router, which means process time decreases. In comparison to IPv4, IPv6 does not extend the header, but makes use of so-called **Extension headers**. This is a key improvement as these are a part of the payload instead of the header itself and therefore does not slow the processing time. The way that IPv6 has designed Extension headers there are in theory no limits to how many there can be allowed together with a packet. This makes it easy in the future to add new Extension headers for new services.

The current IPv6 specification defines six Extension headers

- Hop-by-hop Options header
- Routing header
- Fragment header
- Destination Options header
- Authentication header
- ESP (Encapsulating Security Payload) header

There is not always an Extension header with every header. There may be just one or there may be more than one between the IPv6 header and the Upper-Layer Protocol header, which is always the last header in an IP packet. It all depends on the requirements of the processing of the payload of the packet. Each Extension header is identified in the Next header field of the preceding header.

Only the destination node and none of the other nodes between the source and the destination process the Extension headers. If the destination is a multicast address all the nodes that

belong in that specific multicast group process the Extension headers. The Extension headers must be processed in the order they are arranged in, in the packet header.
The only exception to the rule about the destination node being the only one to process the Extension headers is when the Hop-by-hop Options header is in use. All nodes in the route towards the destination node must process this. The Hop-by-hop header must therefore always immediately follow the IPv6 header.

If more than one Extension header is present in a single packet the following order is recommended [6]:

1. IPv6 Header
2. Hop-by-hop Options header
3. Destination Options header[1]
4. Routing header
5. Fragment header
6. Authentication header
7. ESP header
8. Destination Options header[2]
9. Upper-layer Protocol header

The Extension headers should at most occur once except the Destination header which may occur at most twice (once before the Routing header and once before the Upper-layer header).

In cases when IPv6 is encapsulated in IPv4, the Upper-Layer header can be another IPv6 header and can contain Extension headers that will then follow the same rules [16]. The Upper-Layer Protocol header will always be the last Extension header.

The IPv6 header is therefore expected to reduce the cost of header processing between the source and destination node.

### 3.4.3 Other improvements

IPv6 supports automatic configuration, which means a computer can be plugged in and made Internet-ready without laborious manual entry of address information. IPv6 allows better plug and play. The time it takes to get a large number of machines to run with IPv6 will be clearly decreased compared to make a large number of machines run with IPv4 [17].

IPv6 includes IP Security (IPSec) for sender authentication and data encryption by default, whereas it is an optional extension to IPv4 [3].

[1] For options to be processed by the first destination that appears in the IPv6 Destination Address field plus subsequent destinations listed in the Routing header.

[2] For options to be processed only by the final destination of the packet.

## 3.5 The IPv6 Address

### 3.5.1 Address categories

An IPv6 address can be classified into one of three categories:

- Unicast.
- Multicast.
- Anycast.

IPv6 addresses are assigned to interfaces, as IPv4 addresses are. Each interface of a node needs at least one unicast address. A single interface can be assigned multiple IPv6 addresses of any type (unicast, multicast and anycast). A node can therefore be identified by any of its interfaces. It is also possible to assign one unicast address to multiple interfaces for load-sharing reasons, if the hardware and drivers support it.

The **unicast** address uniquely identifies an interface of an IPv6 node. An object sent to a unicast address is delivered to the interface identified by that address. This type of address will be described in more detail later in this chapter.

The **multicast** address identifies a group of IPv6 interfaces. A packet sent to a multicast address is processed by all members of the multicast group.

The **anycast** address is assigned to multiple interfaces (usually multiple nodes). A packet sent to an anycast address is delivered to only one of these interfaces, usually the nearest one.

Figure 3.2 below shows a typical IPv6 address, which consists of three parts – the global routing prefix, the subnet ID and the interface ID.

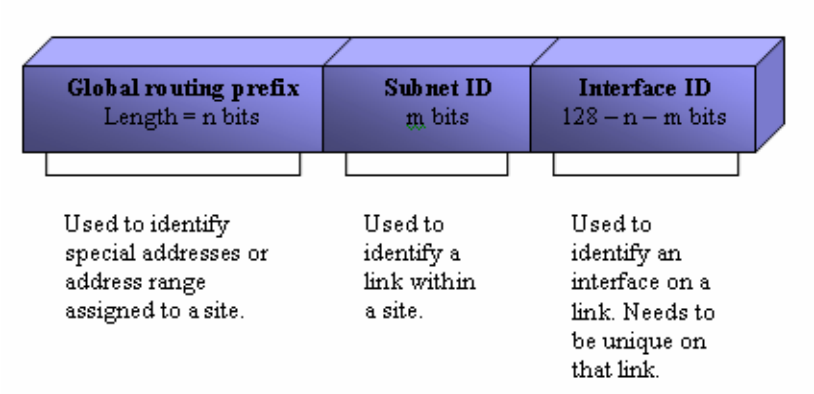


*Figure 3.2: IPv6 general address format*

The global routing prefix is used to identify a special address, such as multicast, or an address range assigned to a site. A subnet ID (also referred to as “subnet prefix” or just “subnet”) is used to identify a link within a site. An interface ID is used to identify an interface on a link and needs to be unique on that link.

### 3.5.2 Address notation

Before any further description of the IPv6 address it is important to give a basic introduction on the IPv6 address notation.

An IPv6 address has 128 bits (16 bytes). The address is divided into eight, 16 bit hexadecimal blocks, separated by colons. For example:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

There are several ways to write these addresses, many zeros can be avoided, as there will be a lot of these in the address field. The first example shows the above address:

FE80:0:0:0:202:B3FF:FE1E:8329

To make the address even shorter a double colon can replace consecutive zeros, or leading or trailing zeros, within the address. If this rule applies the above address will look like this:

FE80::202:B3FF:FE1E:8329

The double colon can only appear once in an address, as the computer always uses the full 128 bits. Where the double colon is present the computer fills the address with zeros so that the address reaches the full length of 128 bits.

In an environment where both IPv4 and IPv6 nodes are mixed, there is another convenient form of IPv6 address notation. The IPv4 address can be inserted in the end of the IPv6 address in its original form:

IPv4 address example: 128.39.0.2
IPv6 address for above example: 0:0:0:0:0:0:128.39.0.2 or ::128.39.0.2
If preferred it also can be written in hexadecimals: ::8027:2

### 3.5.3 Prefix notation

The prefix notation is an important part of understanding the more complex hierarchy of IPv6 addresses than used in IPv4. IPv4 mainly divided the addresses into A-, B- and C-class addresses. The IPv6 prefix structure allows a larger range of network/subnetwork splits in the address.

A *format prefix* (also referred to as global routing prefix) is the high-order bits of an IPv6 address used to identify the subnet or a specific type of address. The notation appends the prefix length, written as a number of bits with a slash:

*IPv6 address/prefix length*

This is very similar to the CIDR notation for IPv4 or for subnetted IPv4 addresses. The prefix length indicates how many of the left most bits are a part of the prefix. The prefix is used by routers to identify which subnet the address belongs to. The packet is then forwarded using the value of the prefix only.

Example prefix notation:
2E78:DA53:12::/40

Table 3.1 shows this more clearly with the hexadecimal digits converted into binary.

*Table 3.1: Example prefix notation.*

| Hex notation | Binary notation | Number of bits |
|---|---|---|
| 2E78 | 0010111001111000 | 16 bits |
| DA53 | 1101101001010011 | 16 bits |
| 12 | 00010010 | 8 bits |
| | | 40 bits total |

Note that in the address notation the address would have to be written 2E78:DA53:1200::, but as it is only the 40 left most bits that are of interest, the double colon (::) will replace the remaining bits with zeros until the address reaches 128 bits.

The format prefixes that are used to identify special addresses, such as link-local addresses or multicast addresses are reserved prefixes, as shown in table 3.2 below.

*Table 3.2: List of assigned prefixes*

| Allocation | Prefix binary | Prefix hex | Fraction of address space |
|---|---|---|---|
| Reserved | 0000 0000 | ::0/8 | 1/256 |
| Reserved for NSAP | 0000 001 | ::2/7 | 1/128 |
| allocation | 0000 010 | ::4/7 | 1/128 |
| Reserved for IPX allocation | 001 | ::20/3 | 1/8 |
| Aggregatable global unicast addresses | 1111 1110 10 | FE80::/10 | 1/1024 |
| Link-local unicast addresses | 1111 1110 11 | FEC0::/10 | 1/1024 |
| Site-local unicast addresses | 1111 1111 | FF00::/8 | 1/256 |

Some of the special addresses are assigned out of the reserved address space with the binary prefix 0000 0000. These include the *unspecified address*, the *loopback address* and the IPv6 addresses with the embedded IPv4 addresses.

Unicast addresses can be distinguished from multicast addresses by their prefix. Globally unique unicast addresses have a high-order byte starting at 001. An IPv6 address with a high-order byte of 1111 1111 (FF in hex) is always a multicast address.

Anycast addresses are taken from the unicast address space, so it is not possible to identify these only by looking at the prefix. If a unicast address is assigned to multiple interfaces, which makes it an anycast address, the interfaces need to be configured to let them all know that the address is an anycast address.

Addresses in the prefix range 001 to 111 should use the 64-bit interface identifier that follows the EUI-64 (Extended Unique Identifier) format. The EUI-64 is a unique identifier defined by the IEEE [16].

### 3.5.4 Aggregatable global unicast address

As mentioned earlier the unicast addresses are identified by the prefix 001. The initial address specification defined *provider-based addresses;* the name has been changed to *aggregatable global unicast address*. The name change reflects the addition of an ISP-independent means of aggregation called *exchange-based aggregation.* The prefix is followed by five components, as shown in figure 3.3.

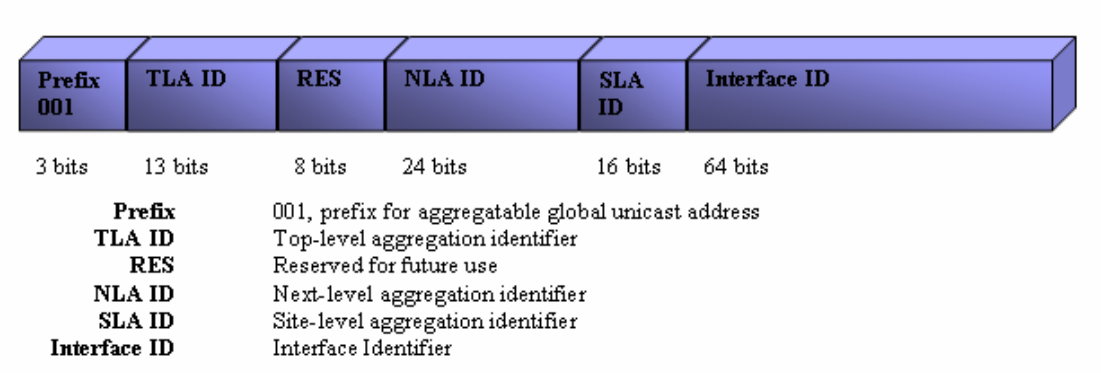


*Figure 3.3: Format of the aggregatable global unicast address.*

The format prefix 001 is assigned to the aggregatable global unicast address range. The Top-level Aggregation identifier (TLA) contains the highest level of routing information about the address. Its size of 13 bits limits the number of top-level routes to 8192. In the earlier specification, the TLA was the provider-based identifier. It was later assigned to the RIR; American Registry for Internet Numbers (ARIN) in North America, Réseau IP Européens - Network Coordination Centre in Europe (RIPE - NCC), and Asia Pacific Network Information Centre (APNIC) by IANA (The Internet Assigned Number Authority), see figure 3.4 below. With this change in the specification, the commercial aspect of the TLA has been removed and the focus is now on routing optimisation; the TLA does not have to be an ISP. At the core of the Internet, the routing tables need only one route entry per TLA, which means that the 13-bit TLA is large enough.

ISPs and exchange points use the next-level aggregation identifier (NLA). These network access providers are usually public, and they will further structure the address space assigned by the TLA with route topology optimisation as a priority.

The site-level aggregation identifier (SLA) is the address space assigned to organisations, used for internal network structure. It can be subnetted further within the organisation.

The last part of the IPv6 address is used for the 64 bit interface identifier, as discussed earlier in this chapter (EUI-64).

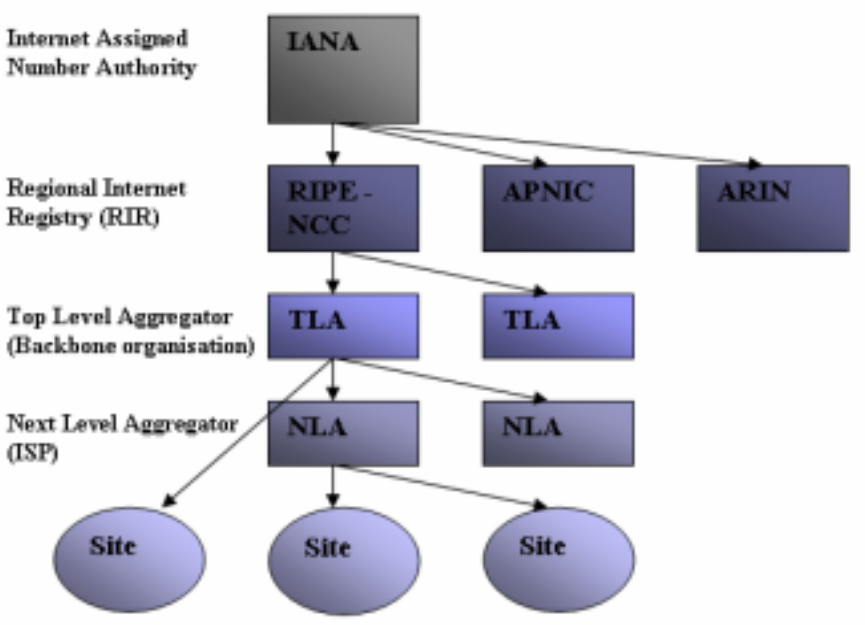


*Figure 3.4: The IPv6 address distribution hierarchy.*

From July 1999 the RIRs could allocate so-called **subTLA**s (sTLA) to ISPs. IANA will assign small blocks e.g. a few hundred of sTLA IDs to RIRs. The registries will assign the subTLA ID's to organisations meeting the requirements of certain specifications. When the registries have assigned all of their sTLA ID's they can request that the IANA give them another block. The blocks do not have to be contiguous. The IANA may also assign sTLA ID's to organisations directly. This includes the temporary TLA assignment for testing and experimental usage for activities such as the 6bone or new approaches like exchanges [18].

### 3.5.5 International registry services and current address allocations

Several TLA allocations have been made, as listed in table 3.3.

*Table 3.3: Current TLA allocations*

| Prefix | Allocation | RFC |
|---|---|---|
| 2001::/16 | Sub-TLA Assignments<br>ARIN 2001:0400::/29<br>RIPE NCC<br>2001:0600::/29<br>APNIC 2001:0200/29 | RFC2450 |
| 2002::/16 | 6to4 | RFC3056 |
| 3FFE::/16 | 6Bone Testing | RFC2471 |

ISPs in Europe will therefore have access to information about the regional registry of IPv6 addresses through RIPE-NCC web pages. For end users, the IPv6 address allocation is managed by their ISP. ISPs in other parts of the world find their information at their regional registries.

## 3.6 IPv6 Status

There is still a lot of confusion about the IPv6 standard. The RFC that was a proposed standard in 1998 on the IPv6 specification is still not agreed upon by the IETF almost five years later. Even though the standards are still only proposed standards or even drafts they are already in use. IPv6 addresses are being assigned to new machines every day and all operating systems have already upgraded their systems to support both IPv4 and IPv6 (e.g. Windows XP). IANA has already started to assign blocks of addresses to several ISPs. IPv6 has been introduced even though there is no fixed agreement about the standard.

# 4 Transition mechanisms

## 4.1 Introduction

This chapter gives an overview of the different transition mechanisms designed to make the migration from IPv4 to IPv6 as smooth as possible. The technical description of the different mechanisms include information on what needs to be upgraded in the network elements, i.e. hosts and routers, and also presents some limitations about the techniques.

There are tens of mechanisms for transition. Only a few are widely used for general situations. These are presented in this chapter. The mechanisms not mentioned in this chapter are mechanisms for very specific scenarios, which may only differ slightly from one to the other.

## 4.2 Background

The deployment of IPv6 is a long and complicated process, which has only just started. The migration will happen gradually, and for many years IPv4 and IPv6 will have to exist together. Anything else will be impossible, since the number of elements to be upgraded is all the elements that depend on the Internet Protocol, including all from routers and operating systems to end-systems and applications. Parts of the Internet will migrate at different times, and at different speed. It is not possible to design one standard solution for how to migrate; the mechanism to be used depends on the situation. Different networks need different mechanisms, and different mechanisms are needed at different stages of the migration progress.

Globally, one will also see a big difference in how fast the migration is going. Asia is already far ahead of the rest of the world in the process. This as a result of the great lack of IPv4 addresses in Asia. In the years ahead the structure of the Internet will be at different stages. A couple of years ago there were few IPv6 network, most of them built for research. Today, commercial IPv6 networks are created, and IPv6 islands rises. Transition mechanisms are used in order to create connectivity between the islands, and between the islands and the IPv4 network. The next stage will come when there are more IPv6 networks than IPv4 networks, and IPv4 islands use tunnelling to communicate with each other. In the last stage the migration process is completed, and the Internet is completely migrated to IPv6. It is naturally hard to presume a time aspect of these stages, but in a report from Telenor, an assumption is made that the migration will be completed in the years after 2011 [9].

To make IPv4 and IPv6 coexist, transition mechanisms have been designed. The mechanisms can be divided into three groups:

- Tunnelling techniques, used when IPv6 packets traverse the IPv4 infrastructure.
- Dual-stack techniques, allowing IPv4 and IPv6 to coexist in the same devices and networks
- Translation techniques, making IPv6-only nodes able to communicate with IPv4-only nodes.

Even though the techniques are presented separately, they can and likely will be used in combination with one another.

## 4.3 Tunnelling

Until all routers understand IPv6, the Internet is effectively partitioned into subnetworks consisting of IPv6 aware routers embedded in the IPv4 Internet. These subnetworks use tunnelling to transfer IPv6 packets between different IPv6 subnetworks. Figure 4.1 illustrates these *IPv6 islands.*

Tunnelling is used in four common ways, each implying which elements in the network encapsulate and decapsulate the packet:

- Host-to-host
- Host-to-router
- Router-to-router
- Router-to-host

The IPv6 in IPv4 tunnel behaves like a single link in an IPv6 network, only decrementing the hop limitation in the IPv6 header by one. By doing so, the tunnel's existence is hidden.

An overview of the different tunnelling mechanisms used to create connectivity between IPv6 islands is given in this chapter.

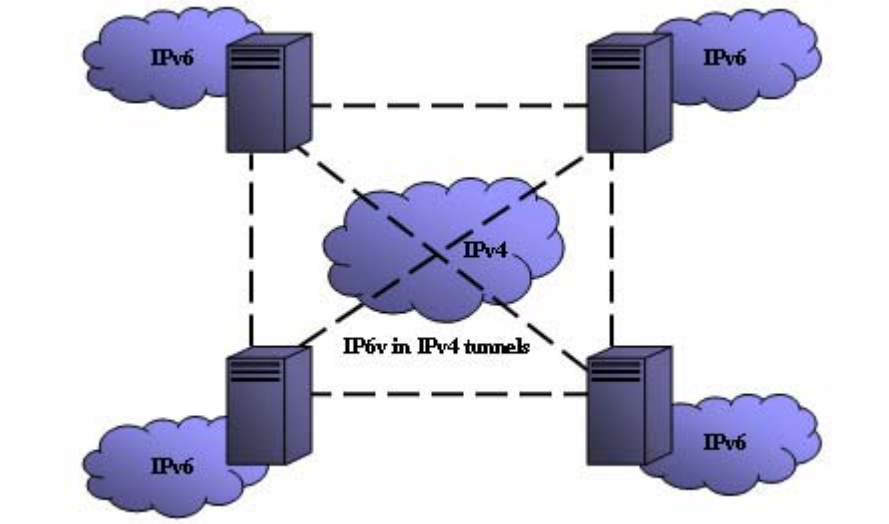


*Figure 4.1: IPv6 islands.*

### 4.3.1 Configured tunnelling

Figure 4.2 illustrates this IPv6 in IPv4 tunnelling method, where the tunnel's endpoint IPv4 address is decided by configured information at the tunnel's encapsulating node. The encapsulating node must store the tunnel endpoint address for each tunnel. The tunnel endpoints are manually configured at both ends, this is something all IPv6 implementations

support. To make this work, the tunnel endpoints must be dual stack nodes. NAT can not be used between the endpoints, as the IPv4 address must be reachable.

Which IPv6 packets are to be tunnelled, is usually decided by routing information at the encapsulating node. This is usually done via a routing table, which directs packets based on their destination address using the prefix mask and match techniques.

The tunnel can be either unidirectional or bi-directional. If it is bi-directional, the tunnel behaves like a virtual point-to-point link.

A *default* configured tunnel can be set up to allow an IPv4/IPv6 host that has no reachability to any IPv6 router to communicate with the IPv6 Internet. The IPv4 address of an IPv4/IPv6 border-router to the IPv6 backbone has to be known, and can be used as the tunnel endpoint address. When this sort of tunnel is set up as default, all IPv6 destination addresses will match the route and can use the tunnel. A *default* configured tunnel is only used if there are no other routes that match the destination address.

A configured tunnel is easy to set up for small networks, and the hosts need not be aware of it. A drawback is that it may be difficult to maintain for larger networks, due to the manually configuration [19].

The *tunnel broker* described later in this chapter, uses configured tunnelling.


*Figure 4.2: Configured tunnelling.*

### 4.3.2 Automatic tunnelling

Automatic tunnelling allows two IPv4/IPv6 hosts to communicate with each other by using the IPv4 network without pre-configuring tunnels. Figure 4.3 shows the network topology when automatic tunnelling is used.

The nodes performing automatic tunnelling are assigned an IPv4 compatible address. This sort of address is identified by a 96 bit prefix consisting only of zeros and an IPv4 address in the low-order 32 bits. This IPv4 address is the node's IPv4 address. Only the nodes that support automatic tunnelling should be assigned an IPv4 compatible address.

When the packet is being processed in the router, it is redirected if the destination IPv6 address is an IPv4 compatible address, and automatic tunnelling is then used. The packet being tunnelled determines the tunnel endpoint. If the destination address is a native IPv6 address, automatic tunnelling can not be used. The destination IPv4 address is now the low-

order 32 bits of the IPv6 destination address, and the source address is the IPv4 interface address the packet is sent via.

Automatic tunnelling requires no configuration in hosts. A drawback is that the tunnel is not transparent for both hosts, since the destination node has to decapsulate the incoming packet itself [19].

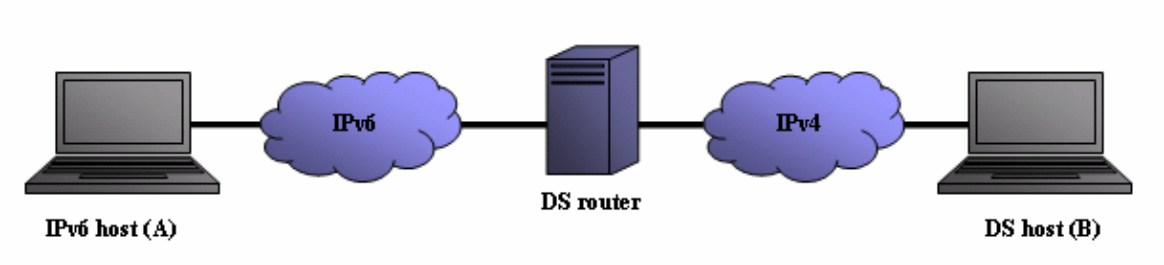


*Figure 4.3: Automatic tunnelling.*

In figure 4.3, the following addressing is used:

| | | |
|---|---|---|
| Packet from Host A to host B: | src=IPv6 | dst=0::IPv4(B) |
| Tunnel from Router to Host B: | src=IPv4 | dst=IPv4 |
| Tunnel from Host B to router: | src=IPv4 | dst=IPv4 |
| Packet from Host B to Host A: | src=0::IPv4(B) | dst=IPv6 |

Examples of automatic tunnelling are *6to4*, *6over4*, *Teredo* and *ISATAP*. These techniques are described in this chapter.

Configured tunnelling and automatic tunnelling may also be combined in different ways, depending on the hosts' needs.

### 4.3.3 Tunnel broker

The Tunnel broker connects one single host to the IPv6 Internet. Figure 4.4 shows how it configures a tunnel endpoint at a tunnel server. A tunnel server is a plug-and-play IPv6 that uses the current IPv4 Internet as the transport medium. It provides IPv6 connectivity on demand and assigns an IPv6 address to the host and connects the host to the Internet. The configuration data from the tunnel server is sent to the client, who uses the data to configure the local end of the tunnel. The client node must be dual stack and the client IPv4 address must be globally routable with no use of NAT.

This method is a little more scalable than configured routing, but could cause an inefficient routing [19].

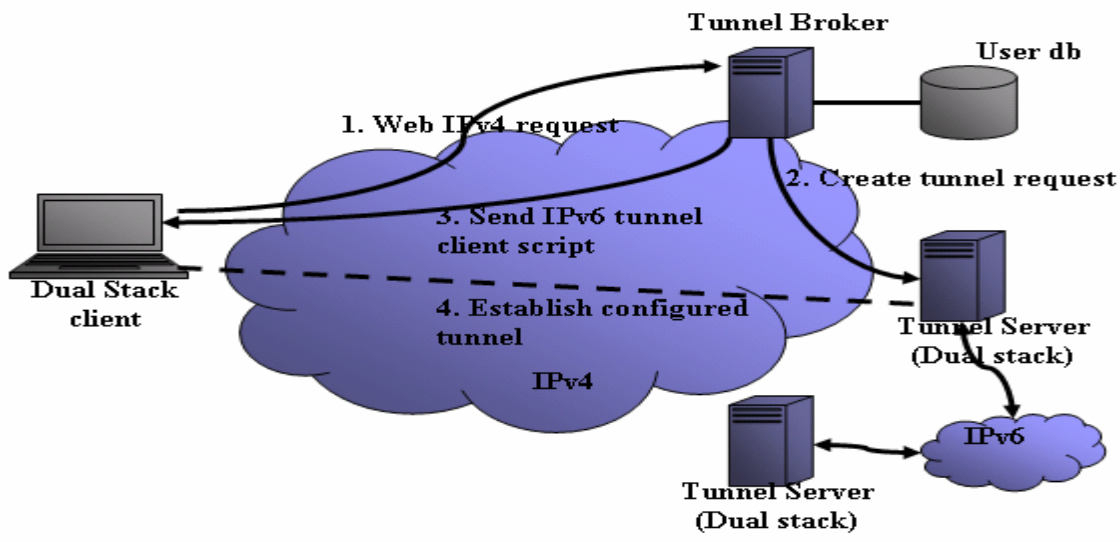


*Figure 4.4: Tunnel broker.*

### 4.3.4 6to4

6to4 is a mechanism for IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel set-up, and for them to communicate with native IPv6 sites via relay routers. A relay router is a 6to4 router configured to support transit routing between 6to4 addresses and native IPv6 addresses.

The communication can be between two 6to4 sites on separate local IPv6 networks as in Figure 4.5, or between a native IPv6 site and a 6to4 site. In the latter case we differentiate between communication from a native site to a 6to4 site as shown in Figure 4.7 and communication from a 6to4 site to a native site as in Figure 4.8.

The mechanism assigns an interim unique IPv6 address prefix to any site that currently has at least one globally unique IPv4 address, and thereafter transmits IPv6 packets using such prefix over the global IPv4 network.

The mechanism is specified for a site, but can also be applied to an individual host or a very small site, as long as it has at least one globally unique IPv4 address

6to4 is typically implemented almost entirely in border routers, without specific host modifications with the exception of a default address selection [20]. The address selection is implemented to ensure a correct 6to4 operation in complex topologies. This means that if one host has only a 6to4 address, and the other host has both a 6to4 and a native IPv6 address, then the 6to4 address should be used for both. If both hosts have a 6to4 address and a native IPv6 address, then it is preferred that the native IPv6 address should be used for both.

The 6to4 router must have a dual stack, a global IPv4 address and a 6to4 implementation. The method introduces no new entries in the IPv4 routing table, and exactly one new entry in the native IPv6 routing table.

IANA has permanently assigned one 13-bit IPv6 TLA identifier under the IPv6 format prefix 001 for the 6to4 scheme. It has a numeric value of 2002.

In all scenarios the 6to4 router advertises the prefix 2002:IPv4::/48 to the local net, which is the same format as normal /48 prefixes assigned according to an IPv6 aggregatable global unicast address format. The router uses its own global IPv4 address in the prefix. The 6to4 hosts on the local IPv6 network must use this prefix. The 6to4 prefix can be used within the site like any other valid prefix, e.g., for automated address assignment, for native IPv6 routing, or for the 6over4 mechanism as described later in this chapter.

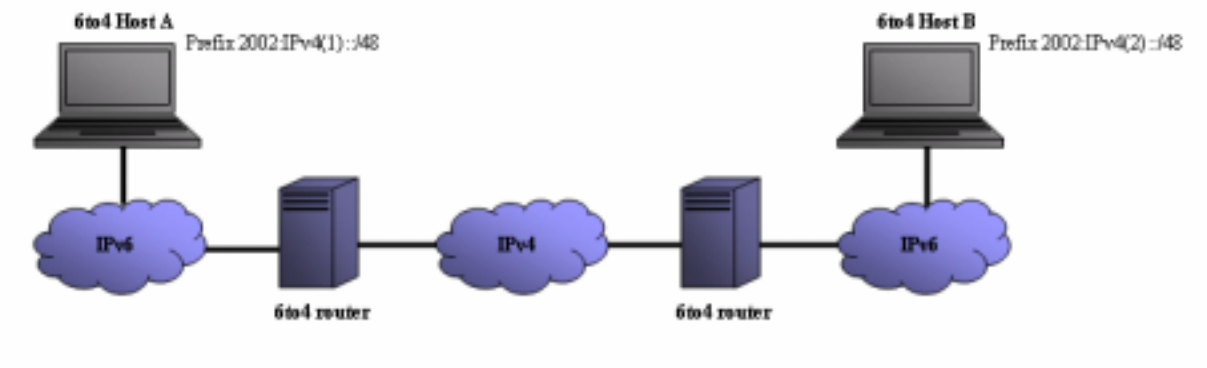


*Figure 4.5: Communication between two 6to4 hosts.*


*Figure 4.6: The headers when 6to4 is used between to 6to4 hosts.*

**Communication from a native IPv6 host to a 6to4 host, Figure 4.7:**

- The native **Host A** is assigned the address IPv6 (A).
- The **6to4 Router 2** advertises the prefix 2002:IPv4(2)::/48 to the 6to4 network, which gives the 6to4 **Host B** the address 2002:IPv4(2)::EUI-64(B).
- The **6to4 Relay router 1** advertises the prefix 2002::/16 in the native IPv6 network; i.e. the prefix is being stored in the routing table.
- When **Host A** sends a packet to **Host B**, the **6to4 Relay router 1** encapsulates the packet with src=IPv4(1) and dst=IPv4(2).
- When the packet arrives at **6to4 Router 2**, this decapsulates and forwards the packet to B.

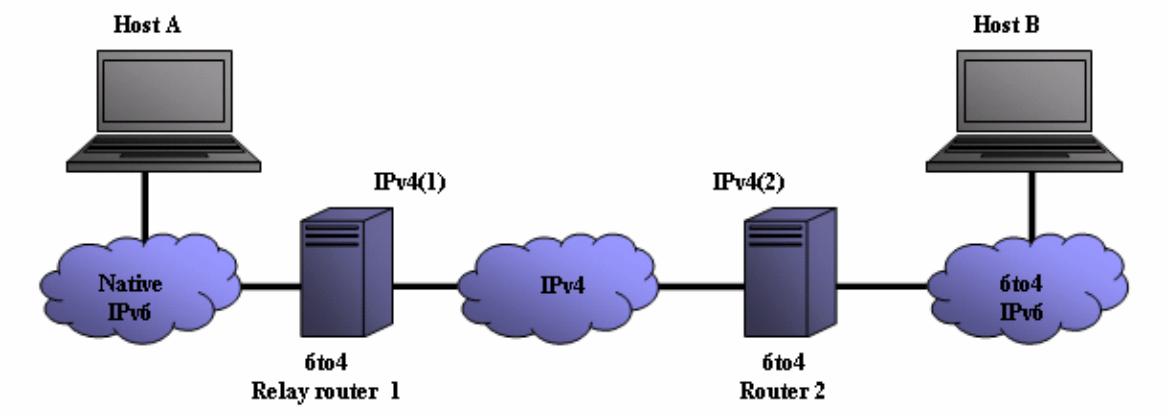


*Figure 4.7: Communication from a native IPv6 host to a 6to4 host.*

**Communication from a 6to4 host to a native IPv6 host, Figure 4.8:**

- **Host A** has address IPv6(A).
- **Host B** has address 2002:IPv4(2)::EUI-64(B).
- The **6to4 Router 2** has a route to a default 6to4 relay router, e.g. **Relay router 3**. This route could either have been statically configured or obtained from a routing table.
- When **Host B** wants to communicate with **Host A**, the **6to4 Router 2** encapsulates the packet with src=IPv4(2) and dst=Ipv4(3).
- The **6to4 Relay router 3** then decapsulates the packet and forwards it to A

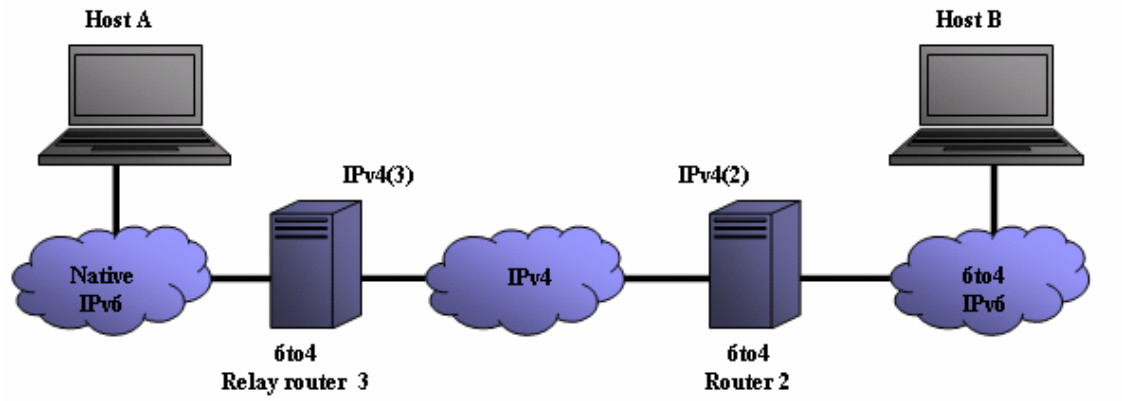


*Figure 4.8: Communication from a 6to4 host to a native IPv6 host.*

6to4 is an efficient method for routing between 6to4 networks, but may be inefficient between native IPv6 networks and 6to4 networks. It is a simple method, as it involves no change in hosts, only some configuration in routers is needed [19].

### 4.3.5 6over4

The purpose of this method is to allow isolated IPv6 hosts, located on a physical link which has no directly connected IPv6 router, to become fully functional IPv6 hosts by using an IPv4 multicast domain as their virtual local link. In this context a domain is a fully interconnected set of IPv4 subnets, within the same local multicast scope, on which there are at least two

IPv6 nodes conforming to this specification. The IPv4 domain could form part of the globally unique IPv4 address space, or can form part of a private IPv4 network.
IPv6 hosts connected using this method do not require IPv4 compatible addresses or configured tunnels. In this way IPv6 gains considerable independence of the underlying links and can step over many hops of IPv4 subnets [21].

When using 6over4 a site can communicate with other 6over4 sites on the same IPv4 domain, but is also able to communicate with the native IPv6 Internet. For the latter to occur, an IPv6 router with a 6over4 implementation connected to the IPv6 Internet must be part of the domain.

6over4 requires no configuration, but IPv4 multicasting must be enabled. All host stacks included must have a 6over4 implementation.

Figure 4.9 illustrates what happens when two 6over4 hosts wants to communicate, the host initiating the communication uses IPv6 neighbour discovery to ask for the IPv4 link layer address of the other host. Then, IPv6 neighbour advertisement packets reply with the 6over4 hosts IPv4 address.
Link layer broadcasts are simulated using IPv4 multicast.

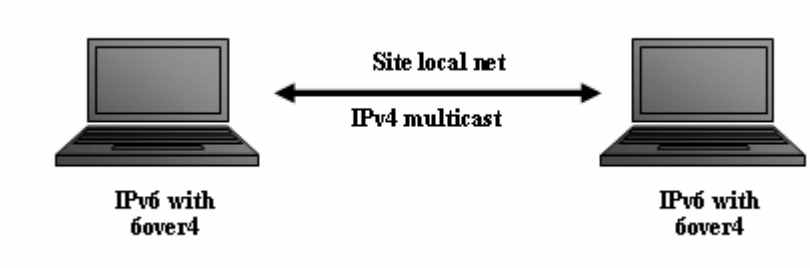


*Figure 4.9: 6over4 between two IPv6 hosts.*

### 4.3.6 Teredo

This method is called **Shipworm** in earlier drafts, and is still under development.

Teredo is designed to make IPv6 available through one or more layers of NAT, which can not be upgraded to 6to4. It works the same way as 6to4 but uses UDP IPv4 tunnelling and is illustrated in Figure 4.10. TCP and UDP are through observation proven to be the only protocols guaranteed to cross the majority of the NAT devices. UDP is preferred because it will give a better quality of service then TCP [22].

The address format to be used is xxxx:IPv4:UDP-port:EUI-64/64.

The UDP mapping does not last forever, and to avoid NAT time-out some “keep alive” traffic must be send before the lifetime expires.

Teredo is efficient for communication between two Teredo hosts, but as for 6to4 it can be inefficient when a native IPv6 host is involved [19].

Teredo will cause a large amount of overhead, and is designed only as a last resort method [22].


*Figure 4.10: Teredo used between two IPv6 sites.*

### 4.3.7 ISATAP

Figure 4.11 and Figure 4.12 illustrate this tunnelling mechanism. The Intra-Site Automatic Tunnelling Addressing Protocol (ISATAP) is still under development, but is expected to become very popular [16]. The protocol is designed to provide connectivity between IPv6 nodes within an IPv4 network that does not have an IPv6 router in the site. It uses IPv4 infrastructure and automatic IPv6-in-IPv4 tunnelling. ISATAP allows automatic tunnelling also when NAT and private addresses are used.

Using ISATAP, the IPv6 hosts on the same IPv4 network can communicate with each other without implementing an IPv6 router; automatic tunnelling does this.

Because the ISATAP host on the IPv4 network does not have an IPv6 router that advertises the prefix to be used for autoconfiguration, it needs to be manually configured for the prefix.

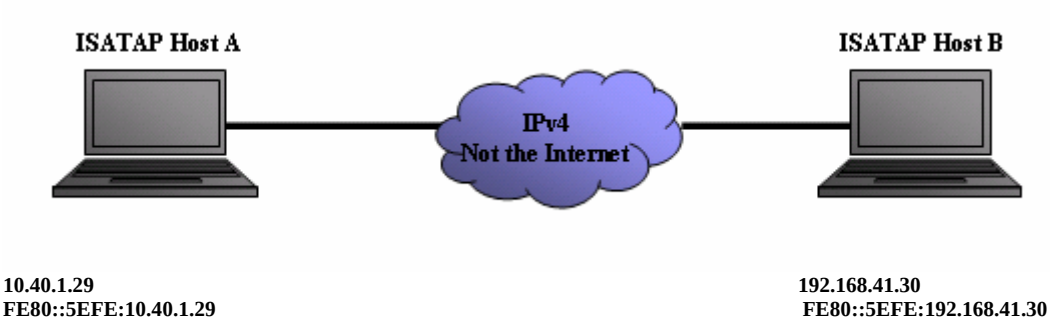


*Figure 4.11: ISATAP on IPv4 (not the Internet).*

When Host A in Figure 4.11 sends a packet to Host B, the IPv6 traffic is as follows:

- Destination IPv4 address: 192.168.41.30
- Source IPv4 address: 10.40.1.29
- Destination IPv6 address: FE80::5EFE:192.168.41.30
- Source IPv6 address: FE80::5EFE:10.40.1.29

As illustrated in Figure 4.12, the IPv6 hosts can also communicate with hosts on a native IPv6 network or with hosts on other IPv4 subnets. Configuring a border router does this; it can be a 6to4 gateway or an ISATAP router. The ISATAP router acts as a default router for the ISATAP hosts, it advertises the address prefix identifying the local network that the hosts are connected to, the ISATAP hosts then uses this prefix in their addresses.


*Figure 4.12: ISATAP on the Internet.*

The ISATAP address has a standard 64 bit IPv6 prefix, which can be link-local, site-local, a 6to4 prefix, or belongs to the global aggregatable unicast range. The interface identifier is 0000:5EFE(32 bits), FE tells that this address contains an IPv4 embedded address. This gives us the ISATAP address format: *prefix:0:5EFE:IPv4 address*

Table 4.1 gives a comparison of the tunnelling mechanisms described in this chapter. The comparison is based on complexity, routing efficiency and how many IPv4 addresses are needed.

*Table 4.1: Comparison of the different tunnelling mechanisms [19].*

| Tunnel type | Add new tunnel | Router/Host implementation | Routing efficiency | Network Type | IPv4 Addresses | Special |
|---|---|---|---|---|---|---|
| **Configured full mesh** | Complex | Either | Good | Small size | 1 per router | |
| **Configured star shaped** | Simple | Either | Bad | Medium size | 1 per router | |
| **Automatic** | None | Both | Good | Large size | 1 per host | Non symmetric |
| **6to4** | None | Router | Good | Leaf network | 1 per router | |
| **6over4** | None | Host Gateway | Optimal | Company network | 1 per host | IPv4 multicast |
| **Tunnel broker** | Simple | Host Broker | Bad | Home network | 1 per host | |
| **Teredo** | None | Client Gateway | Bad | NAT network | 1 per gateway | Works over NAT |

## 4.4 Translation between IPv6-only and IPv4-only nodes

The previous transition mechanisms take care of interconnecting IPv6 domains. This section will explain how IPv6-only hosts communicate with IPv4-only hosts i.e. old printers and other network equipment, as a lot of these types of hosts will stay IPv4 until they are out of work. This section will look at what resources are needed to avoid idle hosts in the network, as a result of the upgrade to IPv6.

When a node is an IPv6-only node it requires another method to communicate with IPv4-only nodes and vice versa. The nodes need a mechanism for address translation, in order to make the connection. There are several translation methods that are either at work or under development.

Translation approaches:

- SIIT, Stateless IP/ICMP Translation.
- NAT-PT, Network Address Translator – Protocol Translator.
- SOCKS64, SOCKS-based IPv6/IPv4 Gateway Mechanism.
- TRT, IPv6-to-IPv4 Transport Relay Translator.

### 4.4.1 SIIT

This mechanism allows the IPv6-only host to talk to the IPv4 hosts. The translation is on the IP packet header. This method requires one temporary IPv4 address per host. The temporary IPv4 address will be used as an IPv4-translated IPv6 address. The packets will travel through a stateless IP/ICMP translator that will translate the packet headers between IPv4 and IPv6. In addition it will translate the addresses in the headers between IPv4 addresses on one side and IPv4-translated or IPv4-mapped IPv6 addresses on the other side [23].
The SIIT is a protocol translation mechanism that allows communication between IPv6-only and IPv4-only nodes via protocol independent translation of IPv4 and IPv6 datagrams, requiring no state information for the session.

The figures below show how the SIIT algorithm can be used initially for small networks (e.g. a single subnet) in figure 4.13 and later for a site that has IPv6-only hosts in a dual IPv4/IPv6 network in figure 4.14. This usage of SIIT assumes a mechanism for the IPv6 nodes to acquire a temporary address from the pool of IPv4 addresses.

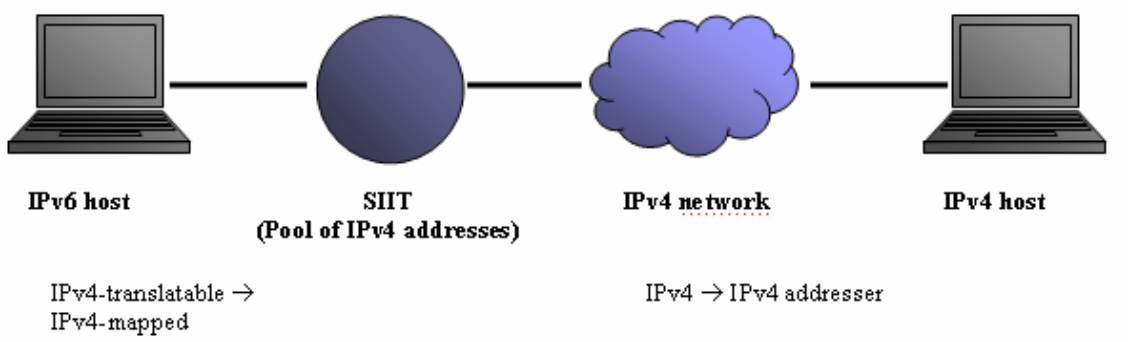


*Figure 4.13: Using SIIT for a single IPv6 only subnet.*

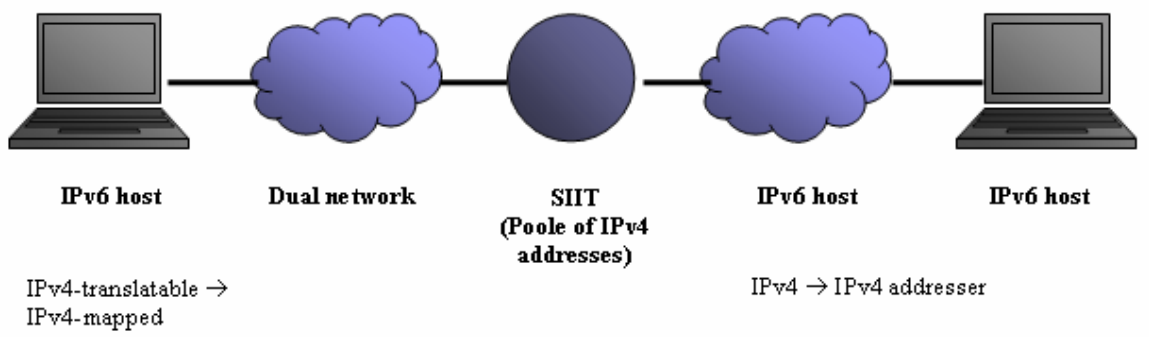


*Figure 4.14: Using SIIT for an IPv6-only or dual cloud (e.g. a site) which contains some IPv6-only hosts as well as IPv4 hosts.*

The SIIT is most likely to only be useful in the initial part of transition, until IPv6 becomes dominant on the Internet [23].

### 4.4.2 NAT-PT: Network Address Translator – Protocol Translator

This approach, which is stateful in comparison to SIIT, also allows IPv6-only hosts to talk to IPv4-only hosts and vice-versa. It uses a dedicated server and requires at least one IPv4 address per site [24].

The term NAT here is very similar to the IPv4 NAT mentioned earlier but is not identical. IPv4 NAT translates one IPv4 address into another IPv4 address. Here, NAT refers to translation of an IPv4 address into an IPv6 address and vice versa. Also, while the IPv4 NAT provides routing between private IPv4 and external IPv4 address realms, NAT in this context provides routing between an IPv6 address realm and an external IPv4 address realm.

There are three operation variants of NAT-PT; Basic NAT-PT, NAPT-PT and Bi-Directional NAT-PT.

Basic NAT-PT is uni-directional, which means that it is outbound from an IPv6 network. Basic NAT-PT allows hosts within an IPv6 network to access hosts in the IPv4 network.

In this operation a block of IPv4 addresses are set aside for translating addresses of IPv6 hosts, as shown in figure 4.15 below.

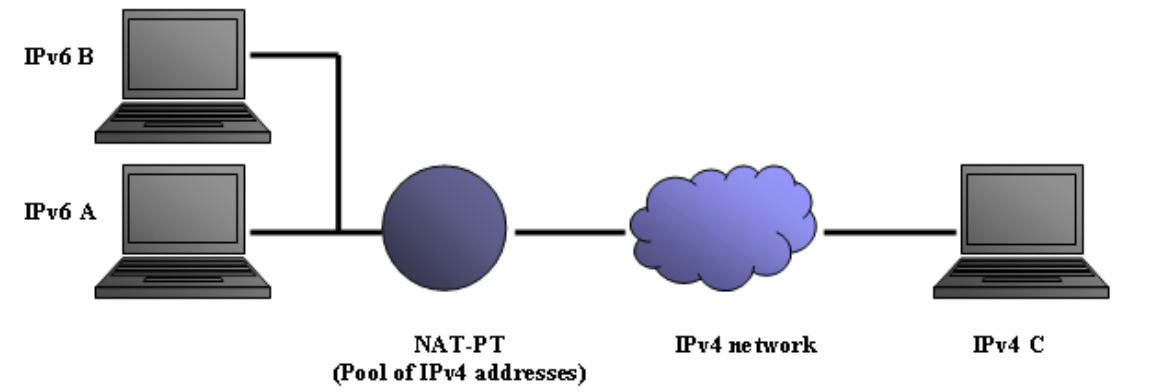


*Figure 4.15: Basic NAT-PT scenario.*

Example IP addresses for figure 5.15:
Node IPv6 A has an IPv6 address → FEDC:BA98::7654:3210
Node IPv6 B has an IPv6 address → FEDC:BA98::7654:3211
Node IPv4 C has an IPv4 address → 132.146.243.30

The IPv4 addresses in the address pool could be allocated one-to-one to the IPv6 addresses of the IPv6 end nodes, in which case one needs equally many IPv4 addresses as IPv6 end points. The more interesting variant is when the IPv6 network has fewer IPv4 addresses than IPv6 end nodes and therefore dynamic address allocation is required for at least some of them.

For example the IPv6 Node A wants to communicate with the IPv4 Node C. Node A creates a packet with: Source Address, SA=FEDC:BA98::7654:3210 and Destination Address, DA = PREFIX::132.146.243.30

The packet is routed via the NAT-PT gateway, where it is translated to IPv4, using the same method as in SIIT.

If the outgoing packet is not a session initialisation packet, the NAT-PT should already have stored some state about the related session, including assigned IPv4 address and other parameters for the translation. If this state does not exist, the packet should be silently discarded. If the packet is a session initialisation packet, the NAT-PT locally allocates an address (e.g.: 120.130.26.10) from its pool of addresses and the packet is translated to IPv4.

The translation parameters are cached for the duration of the session and the IPv6 to IPv4 mapping is retained by NAT-PT. The resulting IPv4 packet has SA=120.130.26.10 and DA=132.146.243.30. Any returning traffic will be recognised as belonging to the same session by NAT-PT. NAT-PT will use the state information to translate the packet, and the resulting addresses will be SA=PREFIX::132.146.243.30, DA=FEDC:BA98::7654:3210. Note that this packet can now be routed inside the IPv6-only stub network as normal.

The second variant of NAT-PT is NAPT-PT, which stands for “Network Address **Port** Translation”. This is still an uni-directional option, but extends the notion of translation one step further by also translating the transport identifiers (e.g., TCP, UDP port numbers and ICMP query identifiers). This allows the transport identifiers of a number of IPv6 hosts to be multiplexed into the transport identifiers of a single assigned IPv4 address. NAPT-PT allows a set of IPv6 hosts to share one single IPv4 address. NAPT-PT can actually be combined with Basic-NAT-PT so that a pool of external addresses is used in conjunction with port translation.

The Bi-Directional NAT-PT is bi-directional as the name implies and this means that sessions can be initiated the same way as for Basic NAT-PT, but from both hosts in an IPv4 network (inbound) as well as hosts in the IPv6 network (outbound).

As described previously, the SIIT proposal is stateless and assumes that IPv6 nodes are assigned an IPv4 address for communicating with IPv4 nodes, and does not specify a mechanism for the assignment of these addresses. NAT-PT uses a pool of IPv4 addresses for assignment to IPv6 nodes on a dynamic basis as sessions are initiated across IPv4-IPv6 boundaries. The IPv4 addresses are assumed to be globally unique. NAT-PT binds addresses

in IPv6 network with addresses in IPv4 network and vice versa to provide transparent routing for the datagrams traversing between the different address settings. This requires no changes to end nodes and IP packet routing is completely transparent to these. It does, however, require NAT-PT to track the sessions it supports and make sure that inbound and outbound datagrams pertaining to a session traverse the same NAT-PT router.

A fundamental assumption for NAT-PT is only to be used when no other native IPv6 or IPv6 over IPv4 tunnelled means of communication is possible. In other words the aim is to only use translation between IPv6-only nodes and IPv4-only nodes, while translation between IPv6 only-nodes and the IPv4 part of a dual stack node should be avoided over other alternatives.

### 4.4.3 SOCKS64

The SOCKS64 aims to enable smooth heterogeneous communications between the IPv6-only nodes and IPv4-only nodes [25].

The SOCKS64 is an extension of the already existing SOCKSv5. SOCKSv5 is designed to provide a framework for client-server applications in both the TCP and UDP domains to conveniently and securely use the services of a network firewall. The protocol is thought of as a shim-layer between the application layer and the transport layer, and does not provide network-layer gateway services, such as forwarding of ICMP messages. The SOCKSv5 extends the SOCKSv4 model and extends the framework to include provisions for generalised strong authentication schemes, and extends the addressing scheme to include domain-name and IPv6 addresses [26].

By applying the SOCKSv5 mechanism to the heterogeneous communications and relaying two "terminated" IPv4 and IPv6 connections at the "application layer" (the SOCKS server), the SOCKS-based IPv6/IPv4 gateway mechanism is accomplished as shown in figure 4.16 below.

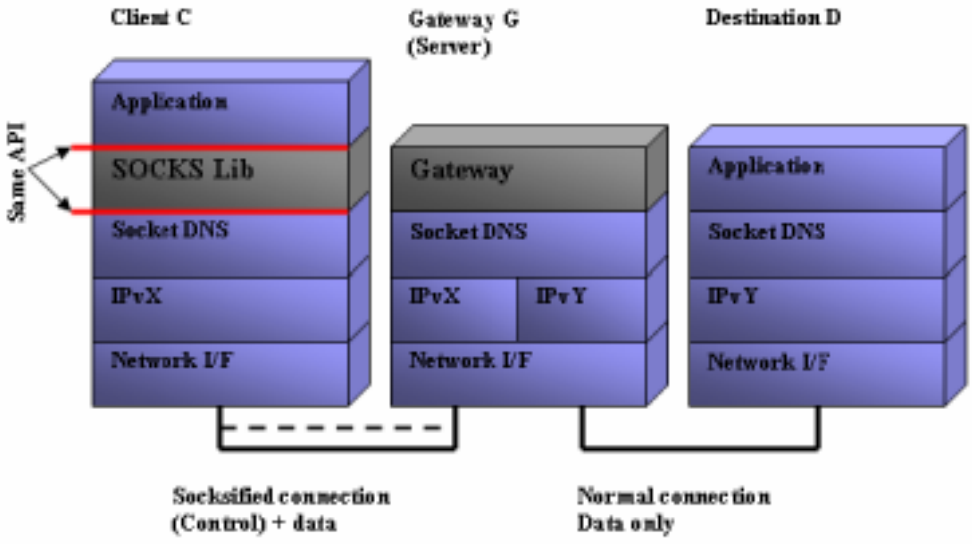


*Figure 4.16: Basic SOCKS-based gateway mechanism.*

The Client C initiates the communication to the Destination D. Two new functional blocks are introduced and they compose the mechanism. One, **SOCKS Lib**, is introduced into the client

side (Client C) (this procedure is called **socksifying**). The SOCKS Lib is located between the application layer and the socket layer, and can replace applications' socket Application Programming Interfaces (API) and Domain Name System (DNS) name resolving APIs. Each socksified application has its own SOCKS Lib. The other functional block, **Gateway,** is installed on the IPv6 and IPv4 dual stack node (Gateway G) and this is where the translation process occurs. It is an enhanced SOCKS server that enables any types of protocol combination relays between Client C (IPvX) and Destination D (IPvY). When the SOCKS Lib invokes a relay, one corresponding Gateway process (thread) is spawned from the parent Gateway to take charge of the relay connection.

The figure 4.17 below shows the following four types of combinations of IPvX and IPvY that are possible in the mechanism.

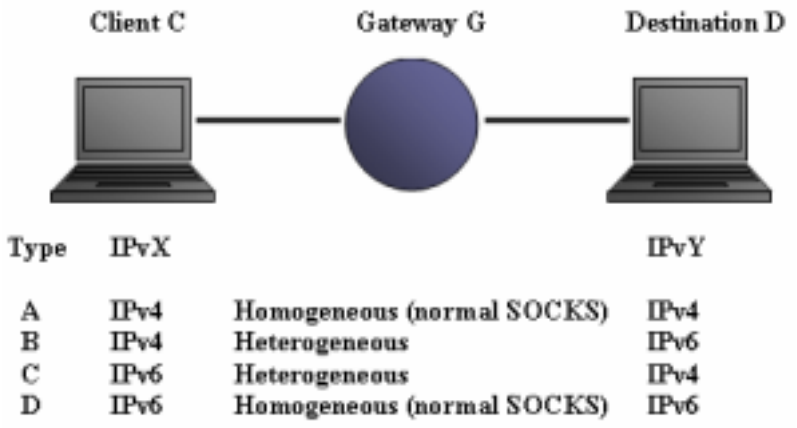


*Figure 4.17: The four types of combination of IPvX and IPvY in the SOCKS64 translation mechanism.*

Type A is supported by the normal SOCKSv5 mechanism. Type B and C are the main targets for the SOCKS64 mechanism. They provide heterogeneous communications. Type D can be supported by the natural extension of the SOCKSv5 mechanism, because it is a homogeneous communication. Since SOCKS Lib communicates with Gateway by using the SOCKSv5 protocol, the connection between them (the Client C and the Gateway G) is a special connection and is called a **socksified** connection. It can transfer not only data but also control information (e.g., the location information of Destination D). The connection between the Gateway G and the Destination D is a normal connection. It is not modified (socksified). A server application that runs on Destination D does not notice the existence of the Client C. It recognises that the peer node of the connection is the Gateway G (not Client C).

The SOCKS64 protocol allows multiple chained relays. But as this is more complex than one-time relay, it is recommended that the multiple chained relay communication should be used only when it is necessary for some reason (e.g., usable protocols or topologies are limited by routers etc.).

### 4.4.4 TRT

This translator is still at the informational stage of standardising. It will be mentioned as it is a method that will manage to avoid translation at the IPv6 header, as the translation is set at the transport layer, which means it is free from dealing with the issues on path MTU and

fragmentation. But then again, there are other disadvantages to TRT, which may only support bi-directional traffic and does therefore not handle multicast datagrams and needs a stateful TRT system.

It uses TCP/UDP relay, which enables IPv6-only hosts to exchange TCP/UDP traffic with IPv4-only hosts. The system, which is located in between the communicating hosts, translates TCP/UDP-IPv6 to TCP/UDP-IPv4, or vice versa.

The TRT is designed to require no extra modification on IPv6-only initiating hosts, nor that on IPv4-only destination hosts. Some other translation mechanisms need extra modifications on IPv6-only initiating hosts, limiting possibility of deployment. TCP/UDP relay is therefore one of the simplest translation techniques to use [27].

## 4.5 Dual stack host approach

The dual stack host approach is when the node has both an IPv6 and IPv4 stack to handle both types of addresses. In this case when a host initiates a communication, the DNS will provide an IPv6 address, an IPv4 address or both. The host will then establish the communication using the appropriate IP stack. This will be the same on the server side. It will listen on both the IPv6 and IPv4 network socket. But every host needs an IPv4 address. When using this method there is no problem for an IPv4 node to use IPv6 applications [28].

There are two methods used together with dual stack.

- BIS, Bump-In-the-Stack.
- BIA, Bump-In-the-ASP.

### 4.5.1 BIS

In the initial stage of the transition from IPv4 to IPv6, it is hard to provide a complete set of IPv6 applications. BIS is a mechanism used in the IP security area. The mechanism allows the hosts to communicate with other IPv6 hosts using existing IPv4 applications [29].

Several transition mechanisms have been presented in this chapter. But in comparison to IPv4 there are very few applications for IPv6. If the transition is to be advanced smoothly, it will be an advantage if the availability of IPv6 increases to the same level as IPv4. This is however expected to take a very long time. In the meantime the BIS mechanism is proposed for dual stack hosts in the IP security area. The technique inserts modules, which snoop data flowing between a TCP/IPv4 module and network card driver modules and translate IPv4 into IPv6 and vice versa, into the hosts, and makes them self- translators. When they communicate with the other IPv6 hosts, pooled IPv4 addresses are assigned to the IPv6 hosts internally, but the IPv4 addresses never flow out from them. Moreover, since the assignment is automatically carried out using DNS protocol, users do not need to know whether target hosts are IPv6 hosts. That is, this allows them to communicate with other IPv6 hosts using existing IPv4 applications; thus it seems as if they were dual stack hosts with applications for both IPv4 and IPv6. So they can expand the territory of dual stack hosts. Furthermore they can co-exist with other translators because their roles are different [29].

Dual stack hosts defined in RFC1933 need applications, TCP/IP modules and addresses for both IPv4 and IPv6. BIS have 3 modules instead of IPv6 applications, and communicate with other IPv6 hosts using IPv4 applications. These modules are a **translator**, **an extension name resolver** and an **address mapper**.

Figure 4.18 illustrates the structure of the host in which they are installed.

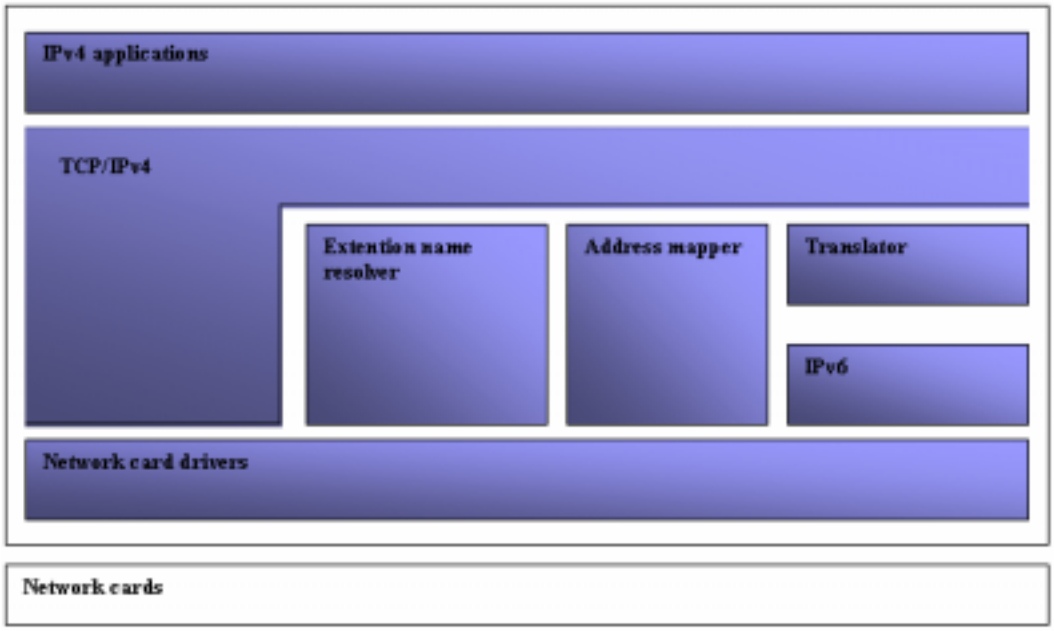


*Figure 4.18: Structure of the proposed dual stack host.*

**The translator**
It translates IPv4 addresses into IPv6 and vice versa using the IP conversion mechanism defined in SIIT. When receiving IPv4 packets from IPv4 applications, it converts IPv4 packet headers into IPv6 packet headers, then fragments the IPv6 packets (because the header length of IPv6 is typically 20 bytes larger than that of IPv4), and sends them to IPv6 networks. When receiving IPv6 packets from the IPv6 networks, it works symmetrically to the previous case, except that there is no need to fragment the packets.

**The extension name resolver**
It returns a "proper" answer in response to the IPv4 application's request. The application typically sends a query to a name server to resolve 'A' records [30] for the target host name. It snoops the query, and then creates another query to resolve both 'A' and 'AAAA' records for the host name, and sends the query to the server. If the 'A' record is resolved, it returns the 'A' record to the application as it is. This does not require an IP conversion by the translator. If only the 'AAAA' record is available, it requests the mapper to assign an IPv4 address corresponding to the IPv6 address, then creates the 'A' record for the assigned IPv4 address, and returns the 'A' record to the application.

**Address mapper**
The address mapper maintains an IPv4 address pool. The pool consists for example of private addresses. Also, it maintains a table that consists of pairs of one IPv4 address and one IPv6 address. When the resolver or the translator requests it to assign an IPv4 address

corresponding to an IPv6 address, it selects and returns an IPv4 address out of the address pool, and registers a new entry into the table dynamically. The registration occurs in the following 2 cases:

1) When the resolver gets only an 'AAAA' record for the target host name and there is not a mapping entry for the IPv6 address.
2) When the translator received an IPv6 packet and there is not a mapping entry for the IPv6 source address.

There is only one exception; when initialising the table, it registers a pair of its own IPv4 address and IPv6 address into the table statically.

### 4.5.2 BIA

BIA is a method for dual-stack hosts and is still categorised as experimental. The goal for this mechanism is the same as for BIS, but this mechanism is supposed to provide the translation between the APIs, which means that the goal is going to be achieved without IP header translation [31].

The BIA technique inserts an API translator between the socket API module and the TCP/IP module in the dual-stack hosts, so that it translates the IPv4 socket API function into IPv6 socket API function and vice versa. With this mechanism, the translation can be simplified without IP header translation.

When the IPv4 applications on the dual stack communicate with other IPv6 hosts, the API translator detects the socket API functions from IPv4applications and invokes the IPv6 socket API functions to communicate with the IPv6 hosts, and vice versa. In order to support communication between IPv4 applications and the target IPv6 hosts, pooled IPv4 addresses will be assigned through the name resolver in the API translator.

Figure 4.19 shows the architecture of a dual stack host in which BIA is installed.

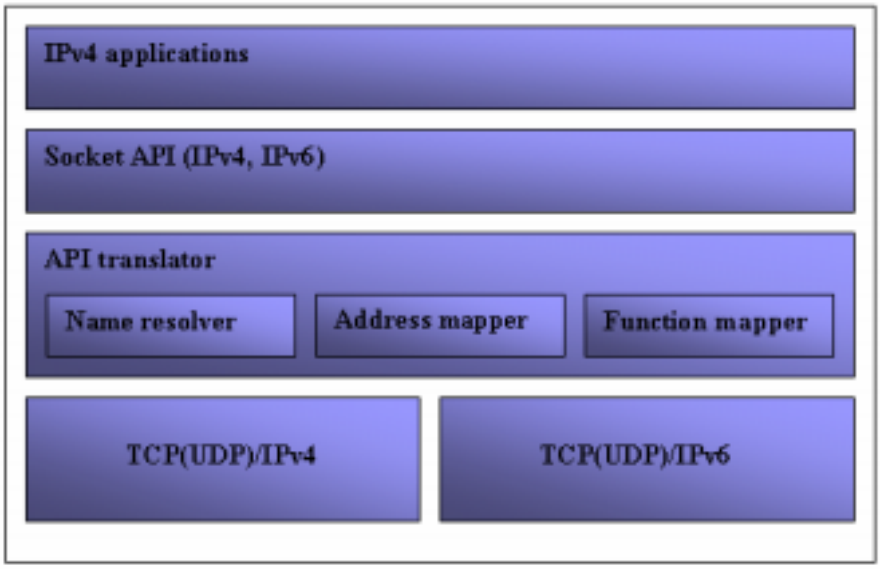


*Figure 4.19: The architecture of a dual stack host in which BIA is installed.*

**Function mapper**
It translates an IPv4 socket API function into anIPv6 socket API function, and vice versa. When detecting the IPv6 socket API functions from IPv4 applications, it intercepts the function call and invokes new IPv6 socket API functions. Those IPv6 API functions are used to communicate with the target IPv6 hosts. When detecting the IPv6 socket API functions form the data received from the IPv6 hosts, it works symmetrically in relation to the previous case.

**Name resolver**
It returns a proper answer in response to the IPv4 application's request.

When an IPv4 applications tries to resolve names via the resolver library (e.g. gethosbyname()), BIA intercepts the function call and instead call the IPv6 equivalent functions (e.g. getnameinfo()) that will resolve both 'A' and 'AAAA' records.

**Address mapper**
This is equivalent to the address mapper in BIS, which was mentioned above.

# 5 The IPv6 roll-out

## 5.1 Introduction

In this chapter we will present our investigation on how the IPv6 deployment takes place today and how it seems to take place in the future. We look mainly at large ISPs and how they present IPv6 to their customers. We look at the different dates set at political level for when a roll-out should be initiated.

The chapter is divided in two main parts where we first look at the IPv6 roll-out world-wide and thereafter look at the IPv6 roll-out in Norway.

## 5.2 The IPv6 roll-out world-wide

The deployment of IPv6 has carefully started world-wide. The progress is still slow, but according to the estimates on availability of IPv6 addresses, the rate of IPv6 deployment should increase drastically during the next two to three years in most parts of the world. The initiative is taken on political level in several parts of the world e.g. Asia, Europe and U.S.

### 5.2.1 Asia

As the IPv4 address allocations has been historically lower in the Asian countries particularly a roll-out of IPv6 is led by this region, especially Japan.

In September 2000 Japan took political leadership of the design of the IPv6 roadmap by setting a deadline in 2005 to upgrade their Internet protocol to IPv6, existing networks in every business and public sector. Japan sees IPv6 as one of the ways of helping them take the lead in the development of Internet and e-business in Asia and hope this will result in a positive effect on the Japanese economy. Japan has therefore established an IPv6 Promotion Council [32] tasked with the realisation of the e-Japan program.

The Japanese initiative seems to have been crucial to the Asia-Pacific region. Korea followed suit in February 2001 by announcing plans to roll out IPv6. Taiwan has also taken a decision concerning IPv6 and has established an IPv6 steering Committee. Bilateral consultations, at ministerial level, between P.R. of China and Japan have taken place on the means to further promote IPv6 [12].
In Japan there are two major companies that offer IPv6 networks. One is provided by IIJ (Internet Initiative Japan) and the other is provided by NTT Communication.

#### 5.2.1.1 Commercial IPv6 network in Asia

IIJ is Japan's leading Internet access and solutions provider, which targets high-end corporate customers. IIJ offers a trial IPv6 service (tunnelling through IPv4) and a native IPv6 service that is independent from existing IPv4 networks.

In addition to offer an IPv6 network, IIJ will from April 01, 2003 offer an IPv6 Gateway service which enables customers to roll out their own IPv6 services by assigning an IP address to each of their products or services. IIJ hopes that the new service will spur the use

of IPv6 in many industries, including home appliances, medicine, distribution, and hardware and software, thus will drive the uptake of IPv6 in the retail market.

Already one year ago IJJ claimed to have experienced a huge interest for IPv6 services. The following parts of a press release dated March 11, 2002 comments the status of usage of IPv6 in the IIJ network:
…"Trends in IPv6 usage are undergoing changes in Japan," said Koichi Suzuki, President and CEO of IIJ. "The enormous popularity of the new broadband access lines has made 24-hour network access a standard practice. Various IPv6 promotion activities have opened the way for home users to enjoy IPv6-capable appliances and applications such as IP telephones, IP controllers and IP cars. In response to these changes, IIJ has decided to extend the trial period for one more year to continue to actively promote new network usage over IPv6, while offering our IPv6 knowledge and operational expertise to corporations recognising IPv6's enormous business potential…." [33]. Whether this was a publication stunt or not is difficult to prove or disprove. At least compared to other parts of the world, IPv6 networks are offered to clients who are interested. What IIJ claims the situation to be this year, is still not known.

NTT Communication is another Japanese company that offers a global commercial IPv6 network. The backbone for this network is called NTT/VERIO Global IPv6 Backbone. It covers Asia, USA, Europe and Australia as shown in figure 6.1. It operates independently of the IPv4 network. NTT has offered an IPv6 Gateway service since April 2001. The NTT/VERIO plays a great part in standardisation / commercialisation of the IPv6 network, representing the largest commercial IPv6 network world-wide.

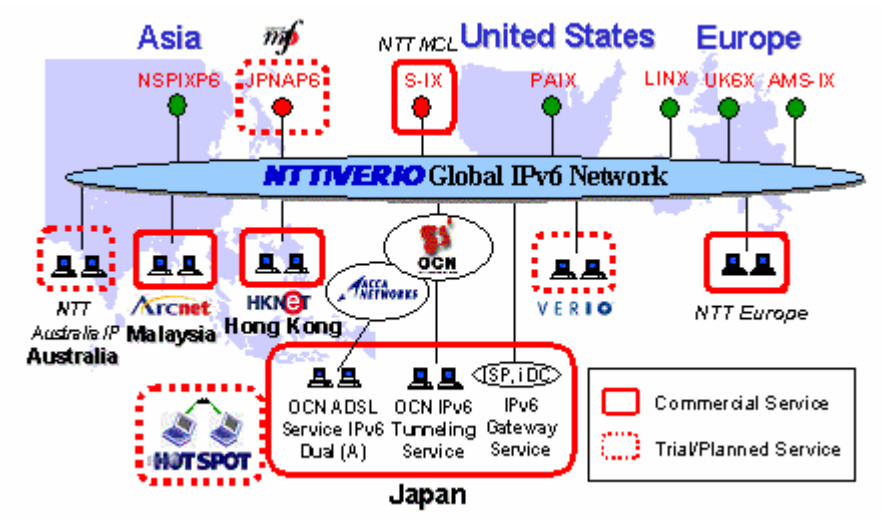


*Figure 5.1: The NTT/VERIO Global IPv6 network [34].*

### 5.2.2 USA

As the U.S. was first in the "land rush" for IPv4 address space, they are not yet in such a critical position as the Asia-Pacific region and Europe. However an industrial initiative towards the establishment of a North American IPv6 Task Force was launched on December 2001, reflecting the growing pressure for an upgrade of the Internet.

In February 2003 the U.S. states in a report on "The national strategy to secure cyberspace" that the U.S. "…will to form a task force to examine the issue related to IPv6, including the appropriate role of government, international interoperability, security in transition and benefits. …" [35]. This could mean that even if the progress is slower in the U.S. than in Asia and Europe, the U.S. seems to look at IPv6 as the next step for the Internet.

#### 5.2.2.1 Commercial IPv6 network in USA

NTT/VERIO Global IPv6 network offer IPv6 network connection in the U.S. on a trial basis. No native commercial IPv6 in the U.S. are known to us.

### 5.2.3 Europe

In the EU the commercial IPv6 roll-out has been marginal compared to the Asian-Pacific, but the focus is larger than in the U.S. The European IPv6 Task Force was launched in April 2001 [36] as a part of the EU's plan to make sure that Europe will not be left behind for the next generation IP. They state in their press release on the "IPv6 2005 roadmap recommendation" in January 2002, that they expect that the depletion of the address space is expected to be critical by 2005[12]. They also think that IPv6 will be needed to meet the further requirements to offer a transparent and affordable Internet service to all citizens, to increase security in the networks, to sustain competitiveness of the Internet, coupled with the emerging convergence of wireless and Internet technologies.

The European Commission itself recommends first and foremost the EU to support the IPv6 enabling in public sectors, including educational sectors. The EU member countries are recommended to launch educational programmes on IPv6 tools, techniques and applications. The EU thinks it is necessary to promote the adoption through awareness raising programmes. The EU will continue to stimulate the wide spread use of Internet across the EU member countries. They wish to strengthen the financial support towards national and regional research networks and ensure testing of IPv6 products, tools, services and applications in the new economy sectors [12].

The IPv6 Task Force expects that a transition to IPv6 will provide Europe with a unique opportunity to capitalise on its technology know-how, notability in mobile communications, to strengthen its competitive edge. They hope that in being early with the roll-out that the European entrepreneurs will create the future applications and services on which new business opportunities can be built to the benefit to all players in the new Internet economy.

The IPv6 Task Force sees IPv6 as a major evolutionary step towards an enhanced next generation Internet infrastructure.

The IPv6 Task Force emphasises the importance to be able to structure, consolidate and integrate European efforts to develop the necessary base of skilled human resources, to sustain the research effort, to accelerate the standards and specifications work to ensure that all sectors of the new economy likely to be impacted by IPv6 are fully aware of potential benefits accruing from its adoption.

The report of the IPv6 Task Force [37] puts forward a number of key recommendations addressed to Member States, the European Commission and Industry at large. Beyond the overall requirements to structure, consolidate and integrate European efforts on IPv6 the report calls for the following initiatives to reach their goals, stated above:

- Increased support towards IPv6 in public networks and services.
- Launching of educational programmes in IPv6.
- Promotion of IPv6 through awareness raising campaigns.
- Further stimulation of Internet across Europe.
- Creation of a stable and harmonised IPv6 policy environment.
- Strengthening of IPv6 activities in the 6th Framework environment.
- Strengthening of support towards the IPv6 enabling of national and European Research Networks.
- Acceleration of contributions towards IPv6 standards works.
- Integration of IPv6 in all strategic plans concerning the use of new Internet services.

The industry is also called by the EC to fully participate in the research and development of activities to be supported in the context of the 6th Framework programme.

All of the European Commission IPv6 Task Force recommendations were made more than a year ago, and if they are to reach their goal before 2005 they will have to work fast.

#### 5.2.3.1 Commercial IPv6 network in Europe

NTT Europe, which is a branch of NTT Communications (Asia), has taken the lead in the European IPv6 roll-out by announcing in February 2003 that following the success of NTT Communications of commercial service in Japan from April 2001, they are launching a full commercial IPv6 service in Europe, targeting ISPs, corporate users and research centres. We assume that they would offer it from the date of the press release, so there should be a commercial IPv6 network available in Europe at this moment.

NTT Europe has the last three years been offering IPv6 Trials to hundreds of European users. NTT Europe will now take the next step, by setting up its commercial-quality IPv6 Points of Presence in several European Cities (London, Amsterdam, Paris, Frankfurt and Madrid). This will provide an IPv6 native connection as well as an IPv6 over IPv4 tunnelling connection, whereby IPv6 equipment is connected over existing IPv4 networks. NTT Europe will provide a direct connection to the NTT/VERIO global IPv6 backbone, a commercial Tier 1 IPv6 backbone that operates in Europe, U.S. and Asia. This single AS (Autonomous System) IPv6 backbone connects to most of the IPv6-IXs and directly to major sTLA (subTLA) holders which proves its high quality IPv6 service [38].

In summer 2001, Telia, in Sweden, announced its intention to build a new generation Internet based on IPv6. By the end of 2001, connection points were installed in Stockholm, Farsta, Malmoe, Gothenborg (all in Sweden), Vasa (Finland), Oslo (Norway), Copenhagen (Denmark) and London (England). Telias intent was to break through the lethargy of the chicken and the egg problem: vendors do not develop because the market is not asking for it, and the market does not ask for it because the vendors do not develop. In 2001 Telia kept their IPv6 network separate form the existing IPv4 infrastructure, to avoid that all of Telias

engineers would have to know all about IPv6 overnight. Also, if there were a problem with the IPv6 network, the IPv4 network would not be affected by this. The configuration was also less complicated [16].

We have not been able to find any updated information on the European IPv6 Telia stated to build in 2001. We have searched both Telia sites as well as Skanova sites, which were the company supposed to build the network for Telia, we have not been able to establish whether the network is still running.

### 5.2.4 IPv6 enabled product

More and more products are IPv6 enabled at this point. More products are announced to be IPv6-ready in within the next year or two. Cisco Systems Inc. has routers that include software support for IPv6 and Juniper Networks Inc.'s routers have the IPv6 stack in the router hardware. Microsoft Corporation offers Windows XP with IPv6 (turned off) and Microsoft has announced support for IPv6 in Windows CE .Net, which will also include "coexistence and migration" utilities. Apple Computer Inc.'s Mac OS X has IPv6 (turned on) as do Sun Microsystems Inc.'s Solaris 8 and various versions of Linux [17].

Mario Tokoro[1] in Sony Corporation states that starting from the autumn 2003 Sony will make IPv6 enabled products. By the year 2005 all Sony products will support IPv6 [39].

## *5.3 The IPv6 roll-out in Norway*

Only five Norwegian sites are at this moment (March 2003) connected to the 6bone, and compared to for example Sweden with its fifty-four sites, this is a quite small number. Searching the Internet for press releases and similar facts on IPv6 roll-out in Norway gave little results. We therefore contacted some of the large ISPs in Norway and the Norwegian organizations connected to the 6bone to get a picture of the situation

### 5.3.1 Telenor

Telenor is the largest ISP in Norway. A report on an IPv6 project done by Telenor says:
"Internet technology is today a central part of the business activity of Telenor, and as a provider of both mobile and fixed Internet-services, Telenor has to relate to the technological challenges and the opportunities in a business manner that IPv6 gives. As an Internet provider it is also important for Telenor to be prepared in the best possible way, in order to be able to maintain already existing services throughout the entire migration process" [9]. More exact information has not been found, as it turns out that most information about new network services is confidential.

Telenor does not provide an IPv6 network today, but are doing research on IPv6 and IPv4/IPv4 migration. The company is also involved in multinational projects.

"IPv6 migration of unmanaged networks – the Tromsø IPv6 pilot" is one of the projects performed by Telenor themselves. The report is dated February 2003. The report analyzes

[1] Corporate Executive Vice President, Co-CTO and President of Network & Software Technology Center at Sony Corporation

issues related to the migration of unmanaged IP-networks, i.e. home or small business networks, from IPv4 to IPv6. There has also been an implementation of a large IPv6 pilot network where dual stack IPv4/IPv6 home networks was connected to an IPv6-only core network.

### 5.3.2 Powertech

Powertech is a large Norwegian ISP, which is a company concerned with the deployment of IPv6 and also interested in promoting IPv6. Powertech has been testing IPv6 since 1996, and is still doing research. The tests being done today is mainly concerning interoperability between different IPv6 implementations, e.g. Linux/Cisco/Allied, and also scale issues, stability and applications. Powertech has also deployed IPv6 into parts of its backbone, and delivers some services with IPv6 support, e.g. web servers and login-services. In the near future the company plans to adjust most of their wholesale-services to IPv6, e.g. DNS and WWW.

### 5.3.3 Tele2

Tele2 has access to a test network provided by RIPE, but this has not been put in production yet. The reason for this is that Tele2 means it is today more disadvantages than advantages with IPv6, and the demand from customers have been to a minimum. Additionally, Tele2 has still not had any problems getting IPv4 addresses from RIPE.

The Tele2 concern, which primarily is located in Sweden, but also in the rest of Europe, has a test network that is in production and available for customers. Nearly no customers have wished to connect to this.

### 5.3.4 Uninett

Uninett is a Norwegian research network, which is possible to connect to for non-commercial institutions for research and higher education.
Uninett provides an IPv6 test network to some of the most advanced research institutes in Norway. Among these are The Norwegian University of science and technology (NTNU), Oslo College, The University of Tromsø (UIT), and the Norwegian Defense research Establishment (FFI). The Test net is supposed to connect the most important research environments and make the realization of a national IPv6 network possible.

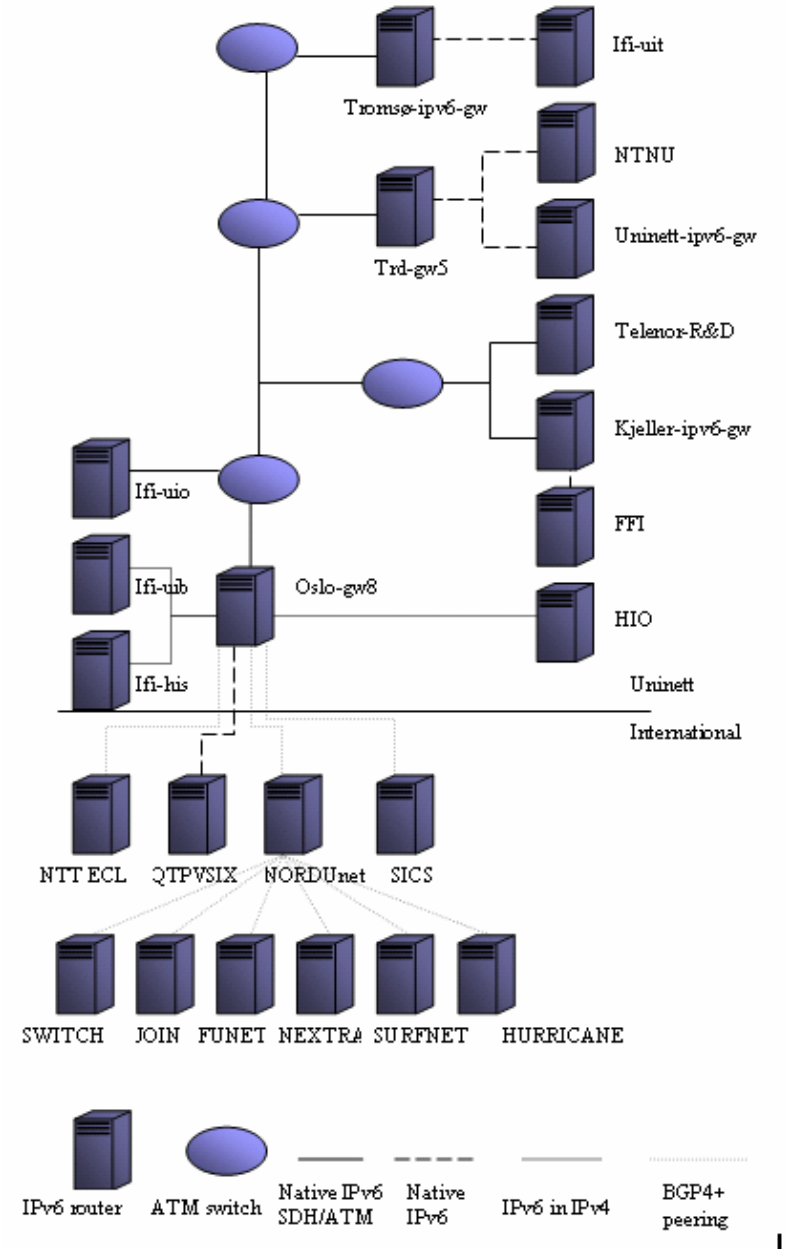


*Figure 5.2: The Uninett IPv6 test network [40].*

Uninett is also about to deploy IPv6 in the production network, and intends to provide an IPv6 pilot service to customers wishing to test or deploy IPv6. This service will be available when IPv6 is deployed in Uninett's production network. The deployment is planned to take place as soon as the production quality router software with necessary features are available, and IPv6 production addresses will then be used. Ipv6 connectivity will be provided to customers by enabling IPv6 in their routers, and a tunnel to one of the Uninett IPv6 backbone routers.

Uninett is planning to run IPv4 and IPv6 in parallel and therefore does not focus the testing on transition mechanisms. Instead they are getting experience with managing an IPv6 network and using IPv6 applications.

# 6 Experiment

## 6.1 Introduction

We wanted to set up a test network our selves and do some tests, to prove or disprove the information we had found. If this was not possible, we were going to concentrate on the theory and if found the experiences of companies or organisations already using IPv6.

As an experiment was not feasible we, in agreement with our supervisor Dr. Peter King and Norwegian contact Geir Køien, decided to concentrate on an experiment already run by Telenor R&D in Norway.

This chapter contains a thorough explanation of why we did not run an experiment and further a description of the Telenor R&D project "IPv6 migration of unmanaged networks-the Tromsø IPv6-pilot". In the end of this chapter we will present some opinions gathered by people at Norwegian ISPs.

## 6.2 Heriot-Watt Experiment

Windows XP has dual-stack implemented and enabling the IPv6 stack is very easy. With this background in mind we decided that we would use Windows XP in our experiment. When using Windows XP only one command is needed to enable IPv6. One simply opens a command prompt and writes *ipv6 install*. The IPv6 stack in Windows XP is a pre-release code and is intended for developer and test networks [16]. Following features are available in the current version of Windows XP:

- 6to4 tunnelling.
- ISATAP.
- 6over4 tunnelling.
- Anonymous addresses.
- Site prefixes in router advertisements.
- DNS support.
- IPSEC support.
- Application support.
- RPC support.
- Static router support.

If a host has a public IPv4 address, this configures it as a 6to4 host. A 6to4 host can perform its own tunnelling to reach 6to4 hosts in other sites or hosts on the 6bone.

If a host does not have a public IPv4 address, the situation is more complicated. If Internet Connection Sharing (ICS) is enabled on an interface that is assigned a public IPv4 address, the 6to4 service enables routing on the private interface and sends Router Advertisements that contain 6to4 address prefixes based on the public IPv4 address of the public interface. The SLA ID in the 6to4 address prefix is set to the interface ID of the interface on which the Router advertisements are sent. This host is now able to act as a 6to4 router that can encapsulate and forward 6to4 traffic to other hosts in the Internet and forward 6bone traffic to a relay router in the Internet.

The network at Heriot-Watt University uses private IP addresses and the ICS seemed not to be enabled. This makes it impossible to tunnel IPv6 packets through the IPv4 network. We believe this is the reason why the 6to4 mechanism did not work.

"The Janet IPv6 Experimental Service" is an IPv6 test network in the UK. Heriot-Watt University is at the moment not connected to this test network. Even though the university is not connected to it, it is possible to connect to the Janet test network with a tunnel broker. Permission to connect to Janet through the tunnel broker required a written application. Considering the time issue, we were not able to wait for this process, as it was not clear how long it would take.

As it was not possible to connect to the Internet when using IPv6, the alternative was to set up a small intra network. Microsoft XP uses ISATAP to make IPv4/IPv6 hosts communicate over the IPv4 network. This was considered, but not found interesting enough to go through with. To enable IPv6 in Windows XP is not a problem, and we could not see the aim behind connecting two or three computers together when it was not possible to connect them to the Internet. It would consume a lot of our already limited time, and we did not come up with any tests to run on an intra network that was of such value that it would be worth spending time and resources on.

## 6.3 *"IPv6 migration of unmanaged networks - the Tromsø IPv6 pilot"*

### 6.3.1 Description

Telenor R&D has done a project called "IPv6 migration of unmanaged networks-the Tromsø IPv6 pilot", as described earlier in chapter 6. We decided to use the information in this project, in order to help answer the questions raised in the thesis definition. This chapter contains a brief description of the project and the pilot network that was set up. Further, the requirements made for the pilot network and the experiences made from this are dealt with. In the last section the conclusion on the Telenor R&D project is presented.

The report from Telenor R&D focuses on mechanisms for migrating unmanaged networks. Figure 6.1 illustrates this sort of network, which is small and simple and not administrated by any technical personnel, but is being connected and run by the user himself. An example of this sort of network is a small office-network in a small company. The topology is usually a simple subnetwork with one or more nodes. This subnetwork is connected to the ISP via a router that also may work as a NAT and/or a firewall. An unmanaged network is recognised by the fact that the router is unmanaged, and is delivered and configured by the ISP. In some cases it is also under active administrative control by the ISP.

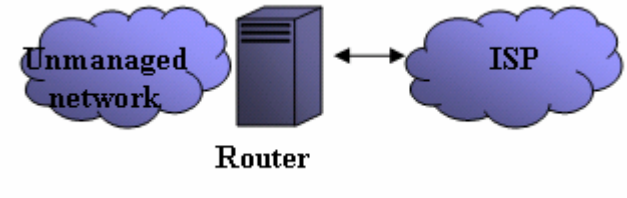

*Figure 6.1: The topology of an unmanaged network.*

As a part of the Telenor R&D project, a pilot network was established in Tromsø. Figure 6.2 shows the topology of this pilot network. The network was a radio-based IPv6 infrastructure that covered most of the city. One of the reasons for setting up such a network was to establish an IPv6 network of larger scale, in order to test an infrastructure as the one in the last stage of the IPv6 migration (chapter 4). At that point the ISP will offer nothing but IPv6, and not IPv4, to different home-networks, which consists of a mixture of IPv4 nodes, IPv6 nodes and dual-stack nodes.

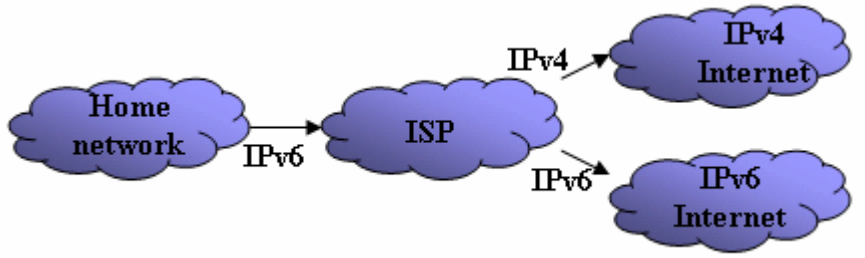


*Figure 6.2: General topology of the Tromsø pilot network.*

### 6.3.2 Requirements for the pilot network

The traffic on the pilot network was from/to the home-network to/from the Internet. How this was managed and which transition mechanisms were being used, depended on who initiated the traffic and on the type of traffic, i.e. from/to IPv4/IPv6 to/from IPv6/IPv4. In the home-network only private IPv4 addresses were being used, and the traffic from IPv4 hosts to IPv6 Internet or IPv4 Internet was done with transition mechanisms implemented in the access-router and the core network. These migration mechanisms also made traffic between IPv6 Internet and IPv4 Internet possible. The transition mechanisms in the pilot network managing the traffic from IPv6 to IPv4 were:

- NAT-PT was used for translation on IP level and FAITHD was used for translation on TCP level. These mechanisms worked together with a DNS-ALG, TOTD (Trick Or Treat Daemon).
- For one-to-one port translation on TCP level *6tunnel* which is a TRT was used.
- Application-specific translators: FTP-proxy.

The mechanisms used for managing traffic from IPv4 to IPv6 were:

- For one-to-one port translation on TCP level 6tunnel was used.
- Application-specific translators: FTP-proxy (*www6to4*) and HTTP-proxy.

The network supported TCP, UDP, HTTP, FTP, SMTP, POP and IMAP.

When setting up the pilot network, the functionality required was:

- A core network consisting only of IPv6, i.e. no direct connection between the IPv4 home-network and the IPv4 Internet.
- A home-network consisting of IPv4 nodes and dual stack nodes.
- The IPv6 nodes in the home-network should communicate directly over IPv6.

- The IPv6 nodes in the home-network should have access to the services on the IPv4 Internet.
- The IPv4 nodes should have access to the IPv4 Internet. The quality of this access should be as if the ISP supported IPv4 directly.
- The IPv4 nodes in the network should have access to the IPv6 services on the Internet.
- The migration-mechanisms should be transparent.

### 6.3.3 Experiences made from the pilot network

When the Telenor R&D report was written, the pilot-network had been running for more than six months. It had been constantly running and used for routine purposes. The experiences made from this usage are presented below.

Forwarding of traffic to IPv6-to-IPv4 translator was done automatic with TOTD. TOTD is a DNS-ALG that returns a "false" IPv6 address if the destination only has an IPv4 address. This false address consists of a network prefix pointing to the translation service in the network in addition to the destination's IPv4 address. However, this would work only if the application uses DNS to locate the destination address. If a web page uses an IPv4 address in the HTTP-reference, the TOTD would fail. The user does not get a direct message if so happens, the only indication is that "nothing happens".

Secure Socket Layer (SSL) can not normally be used over a 6tunnel. The reason for this is that SSL implementations uses source and destination addresses as identification of endpoints, and as 6tunnel works as a "man in the middle" an end-to-end authentication like this will not work.

The research group experienced several cases of hardware problems when using IPv6. These problems did not occur when using IPv4. An example of this is that network cards were not able to detect the media type, causing a failure in external routing of IPv6.

Some Internet sites are registered with an IPv6 address in DNS ('AAAA') while the web server only supports IPv4. Since the normal listing of a net browser with IPv6 support is to use the IPv6 address if the 'AAAA' listing has succeeded, this would lead to a problem for a user in an IPv6/IPv4 world. The user could experience that some Internet sites are not possible unreachable with a web browser supporting IPv6, while it is possible with an IPv4 web browser.

Another reason why Internet sites can not be reached with IPv6, but with IPv4, is because of bad quality on IPv6 connections. Many sites are connected to IPv6 Internet via 6bone, which is well known for its traffic problems. As a consequence, an IPv6 node gets much worse quality and functionality than an IPv4 node.

Many transition mechanisms, such as IPv4-to-IPv6 relays present a security problem. This is because of the relay's IP address, which is an extension of the connection's source- IP address. Because of this, access control to services based on source IP address can no longer separate external and internal clients based on just subnet addresses. During the Telenor project an IPv4-to-IPv6 relay that originally was protected against external connections was open for a short period of time. This happened when the relay was configured with a global

IPv4 address. Because of this, an e-mail server on the network forwarded about 260 000 spam mail.

In home-networks the nodes are usually automatically configured by the mechanisms in IPv6. In some cases the nodes has to be reachable from the external network, and a method for addressing these is therefore needed. The automatically configured IPv6-address has a complex format, and is difficult to handle. A manual updating of the DNS server can be done where addresses are stored in the server making it possible to address the node with its symbolic name. Some services use this sort of DNS mapping to authenticate a client, and on these grounds some times denies it access to the service when it should have been allowed. Because of this it is important to maintain DNS mapping of automatically configured IPv6 nodes. Another solution is to combine automatically and manually configured name-servers, but this is not an optimal solution either. The Telenor R&D report claims that what is needed is support for dynamic updating of DNS for automatically configured addresses. This is supported in IPv4 since the DHCP server, arranges addresses on request to the IPv4 nodes and at the same time often is responsible for updating the address mapping in a specific DNS server. In IPv6 stateless autoconfiguration is used, and there is therefore no such server to maintain the DNS updating. A mechanism is needed in order to allow the node itself to dynamically update DNS with its address(es).

The report also raises the issue of locating the DNS server in IPv6. In the pilot network dual-stack nodes located the DNS server by using a DHCPv4 server. IPv6-only nodes had to be manually configured.

All the access routers in the pilot network were manually configured. It was not possible to use a general configuration for all the home network routers, but locating the network-prefixes was relatively uncomplicated when dealing with simple radio-links in the network. However, the configuration was more complicated when it concerned networks connected to the central point. The radio network beams are spread in many directions and a manually mapping between the radio-link and network prefix was complicated. Therefore it is need for a mechanism that automatically configures network prefixes. Today, this is an unsolved problem about the IPv6 migration.

The transition mechanisms also had to be manually configured. This is acceptable in small networks, but for a bigger network there has to be an automatic mechanism for configuring the transition mechanisms.

### 6.3.4 Conclusion

From the experiences made, the requirements listed early in this chapter were analysed, to see whether they were fulfilled:

- *A core network consisting only of IPv6.*
  The requirement was fulfilled, as the core of the pilot-network was an IPv6 only network.

- *A home-network consisting of IPv4 nodes and dual stack nodes.*

Mainly, Windows computers were used in the home-networks. These computers were a combination of IPv4 nodes with Windows 98, Windows ME and Windows 2000. Additionally, there were Windows XP that has support for IPv6, and multiple Windows 2000 clients patched with Ipv6 support. The pilot-network was therefore said to fulfil this requirement.

- *The IPv6 nodes in the home-network should communicate directly over IPv6.*

  No IPv6-only nodes were used in the home-networks, but this functionality was tested by using a NetBSD-client which had support for IPv4 deactivated. I.e. the pilot-network supported the IPv6-only nodes in the home-network.

  Dual-stack nodes in the home-network communicated directly over IPv6 for application and services with IPv6 support. This is what actually happens when using Internet Explorer in Windows XP and in Windows 2000 with IPv6-patch.

  The requirement was said to be fulfilled.

- *The IPv6 nodes in the home-network should have access to the services on the IPv4 Internet.*

  An NAT-PT implementation was used at first, but did not work satisfying. Therefore, a transport-layer-translator, FAITHD, was implemented. FAITHD is configured to translate individual TCP-ports, and was in the pilot-network configured to translate TCP-ports such as POP3, SMTP and HTTP. This means that there was no support for translation of connectionless UDP-protocols or other less familiar TCP-protocols, which the translator was not configured for.

  At the time the Telenor report was written, there existed no satisfying NAT-PT implementations.

  The requirement was said to be partly fulfilled, by the IPv6 nodes in the home-network that had access to IPv4 Internet for the most common services.

- *The IPv4 nodes should have access to the IPv4 Internet, the quality of this access should be as if the ISP supported IPv4 directly.*

  IPv4 applications in the home network communicated with the IPv4 Internet in two steps; first via 4to6 proxies/TRT in the access router and then through the transport-layer-translator as described above.

  4to6 translating in the access router was done by using a HTTP and FTP proxy, and one-to-one transport-layer port-relays. The relays were configured manually on basis of the needs of the end-users. These relays forward the transport-layer-port directly to a concrete port on a specific destination address.

  In addition to all the limitations in the translation of IPv6 to IPv4 via FAITHD, there was neither any general support for all TCP-services. There was neither any support

for UDP-based services. The IPv4 nodes in the home network only had support for web browsing, simple file-transfer and e-mail services on pre-configured e-mail accounts.

Because of the very little support for IPv4 based services, the report concludes with that this requirement was not fulfilled.

- *The IPv4 nodes in the network should have access to the IPv6 services on the Internet.*

  The 4to6 proxies and transport-layer-relays mentioned above gave a general IPv6 connection for those protocols and ports these supported. This means that IPv4 nodes in the home network had access to IPv6 Internet for web-browsing, simple file-transfer and e-mail services on pre-configured e-mail accounts.

  A minimal support for IPv4 services in the home-network also results in a limited access to IPv6 services and the requirement was therefore not fulfilled.

- *The migration-mechanisms should be transparent.*

  An IPv4 based web browser or FTP client in the home network had to be configured manually with a description of the access router's IPv4 address. This is the same as with any other HTTP/FTP proxy. Further, e-mail clients had to be configured by giving up the access router as an e-mail server. Since this manually configuration is no different from the way these services often are being configured in IPv4 networks, the transition mechanisms were said to be transparent.

The conclusion of the Telenor R&D project "IPv6 migration of unmanaged networks" is:

Configuration of network equipment against an IPv6-only ISP is too complicated for non-technical users. This is mainly because of the lack of autoconfiguration mechanisms with regards to DNS-location, problems with handing out prefixes to access routers and lack of autoconfiguration of transition mechanisms.

The quality of service achieved by the IPv4 hosts is not as good as the one achieved by the IPv4 Internet. Support for services mainly like web browsing and file-transfer causes this.

The quality of service for IPv6-only hosts is also reduced. This is caused by the fact that the quality on IPv6 connections with dual-stack nodes is much worse than the one on IPv4 connections.

There are weaknesses in the translation mechanisms. Because of this, the IPv4 connections from an edge network should be made with 4-in-6 tunnels instead of using translation mechanisms both in the edge network and in the core network.
The main conclusion on the project is that it is possible for end-users to have an IPv6-only ISP. Still, the user friendliness and experienced service quality have many limitations. Therefore, there is much work to be done before it is realistic that end-users can have an IPv6-only Internet connection.

## 6.4 Contact made with Norwegian ISPs

In addition to the information we got from the Telenor R&D report, we also contacted some Norwegian ISP's in order to get an impression of how these relates to IPv6. Telenor, which is the largest ISP in Norway, was first contacted. Tele2 is a large ISP in Norway, and was also contacted. Thereafter we got in touch with Uninett, as this is a big research network in Norway. We found the Norwegian sites connected to 6bone and contacted all of them by e-mail. Of the five we contacted only Powertech replied. The IPv6 status of these companies is given in chapter 5. We asked the people we got in touch with about their opinions on the migration, and what they assumed was the problem about it. In this chapter we present these opinions. We would like to point out the fact that these people speak on behalf on themselves, and do not represent the company they work for.

One of the biggest problems about IPv6 seems to be the lack of applications supporting it. The vendors are slow in the process of producing software of production quality. Øystein Homelien is responsible for the IPv6 deployment at Powertech and says that they just recently found the software from Cisco good enough to implement it in the Powertech production network. Trond Skjesol at Uninett tells that most of the technical problems they are experiencing with IPv6 are related to applications because there is no support for many of the services.

We raised the question about why the process of presenting IPv6 networks has not got further, and whether this is because of technical or economical reasons. On this question we got quite different answers. Geir Egeland at Telenor R&D claims it is first of all because of economical reasons that an ISP does not upgrade. He points at the negative situation in the telecom business we are experiencing today, and says that many operators have paid high UMTS fees and therefore has to follow economic restrictions. He thinks it is possible to upgrade an IP network, though there still is need for more applications. In addition he claims that the need for IPv6 will not be severe until the end application is good enough, thereby creating a need for IPv6 among the end users. Skjesol at Uninett also points out the fact that a commercial IPv6 network will be expensive, but does not believe this is the main reason for not building it. He calls it a "chicken and egg" problem; with no network there is no need for applications and vice versa. Skjesol claims that the need for IP addresses is not enough for building IPv6 networks in Europe and USA. Homelien at Powertech does not think the economical aspect is of large relevancy; he claims the reason for the slow process is technical, that there exists little knowledge about the upgrading. He says that NOT upgrading will have economic consequences. He says: "People believe it is too expensive to upgrade, but the money saved on not doing so will be lost when one deploys techniques such as NAT instead of real public IPv4 access or (in the future) IPv6". Kåre Ljungmann is a network planner at Tele2, and believes the need for IPv6 will not be severe until the need for Virtual Private Networks (VPN) is larger. He further says the use of Multi Protocol Label Switching (MPLS) in the VPNs will make the transition easier and cheaper, because it will be unnecessary to change the network equipment we are using today. MPLS is a technique for switching with the use of labels instead of IP addresses, thereby reducing the use of IPv6 to the edge of the network.

All the people we contacted said that even though there is little activity on IPv6 in Norway these days, it is very relevant and is being discussed. Homelien says that especially the last year the theme has been more focused on in his surroundings, maybe as a result of that it just

recently became possible to run IPv6 traffic through the Norwegian Internet Exchange point (NIX).

# 7 Discussion

## 7.1 Introduction

In this thesis we have investigated what the prospects and problems for an IPv6 deployment are and will be. In this chapter we will discuss the different approaches and methods we have investigated in this thesis, on the deployment of IPv6.

We will discuss the three questions asked in chapter one:

1) Which features will the next generation IP contribute to networks?
2) Which resources are required for an upgrade and when must the upgrade take place?
3) How will the upgrade be done according to the complexity of IPv6?

Through a discussion on these questions we will try to give the reader more angles on the deployment of IPv6.

## 7.2 The contributions of IPv6 to networks

When fully deployed, IPv6 will contribute in more than one way to networks. It will, as stated before, contribute to a much larger address space than that available today. Additionally, it is supposed to contribute to the enhancement of speed and mobility. Real-time services are also supposed to profit from the new protocol. During the transition period, while IPv4 and IPv6 coexist, these advantages are not as clear, as tunnelling and other transition mechanisms prohibit some of the IPv6 services.

One of the main arguments from those who wish to wait with the deployment of IPv6 is that IPv4 offers most of the services the new internet protocol can offer, only in a less elegant way and possibly with poorer quality and service. Several people still feel that expanding the existing protocol with additional methods, rather than to upgrade to a completely new protocol, is a better solution at this moment in time. The real advantages will not be clear until the final stage of the deployment, when IPv6 is the dominant protocol. There will therefore be a long period of time where the two will have to coexist both when IPv4 is dominant and eventually when IPv6 is dominant. The main issue in this intermediate stage is whether the Internet is provided with less quality of service than now or not.

## 7.3 Resources for upgrading

### 7.3.1 Dual-stack hosts

At the moment the machines which are upgraded to IPv6 are dual-stacks, which means that these machines still will need IPv4 addresses for several operations (e.g. enter IPv4-only Internet sites).

At the moment all dual-stack machines understand IPv6 applications, but they need methods to run IPv4 applications (e.g. BIS and BIA). Until the point when IPv6 applications are just as common as IPv4, methods like BIS and BIA will reduce some of the quality of service e.g.

security. None of the transition or translation mechanisms are as efficient or as secure as the communication in native IPv4 or IPv6 networks.

### 7.3.2 Tunnelling methods

There are several tunnelling mechanisms intended for single hosts or entire networks. The ones intended for several hosts on the same network need one IPv4 address per router. Single IPv6 hosts using the IPv4 network also needs one IPv4 address.

Some of the methods require no configuration at all, while other needs a manually configuration in the host or router, e.g. 6to4 which requires only a configuration in the router and not in the hosts. The manually configuration could make some of the mechanisms unsuitable for larger networks.

Another important case for the tunnelling methods is whether it can be used together with NAT. Most of the methods require global IPv4 addresses, while e.g. ISATAP is supposed to work with NAT.

Most of the tunnelling methods require dual-stack hosts.

The transition tunnelling mechanisms have the disadvantages already known from other tunnelling mechanisms used in the IPv4 network. Tunnelling puts extra load on the router, and encapsulating and decapsulating demands time and CPU power. Problems also occur due to fragmentation.

IPv4 security will not be able to protect IPv6 traffic once it is being sent through the IPv4 network. Implementation of IPv6 security is therefore required even if IPv4 security is available [20]. As IP security at both IPv4 and IPv6 level should be avoided because it reduces the efficiency, these methods are not as good as native IPv4 or IPv6 communication.

### 7.3.3 IPv6-only host to IPv4-only host

For IPv6-only machines there are several translation mechanisms. These are meant as last resort methods e.g. when dual-stack is not available and only until the stage of IPv6 merging with IPv4 has changed from dominated by IPv4 hosts until equal share between IPv4 hosts and IPv6 hosts. When the latter occurs, similar methods to those for IPv6-only hosts must be implemented for IPv4-only hosts.

The main limitation of all the transition methods that uses translation mechanisms is on the subject of security. None of the translation mechanism seems to be able to use the IPSEC mechanism that comes with IPv6. The main problem is that the translators do not decrypt encrypted addresses. When using IPSEC, IP addresses are encrypted and this causes the problem.

In the case of SOCKS64 the security feature of the mechanism matches that of SOCKSv5. The mechanism is based on relaying two "terminated" connections at the "application layer". The end-to-end security is maintained at each of the relayed connections (i.e., between Client C and Gateway G, and between Gateway G and Destination D in figure 4.16). The mechanism does not provide total end-to-end security relay between the original source

(Client C) and the final destination (Destination D), which means there could be faults occurring at the Gateway stage, which are not discovered by either the destination node or the client node.

The mechanisms used by dual-stack hosts to make use of IPv4 applications e.g. BIS and BIA, work on the network layer. The security is limited to the security area of IP and is still not able to handle the problem of encryption in IPSEC.

For TRT, the TCP/UDP relay mechanism also has the same problem with IPSEC, as it will never be possible to use IPSEC over relay [27].

## 7.4 The upgrade according to the complexity of IPv6

The process of upgrading to IPv6 seems to be done in several ways. In Asia, where they are the furthest in the deployment process, they seem to offer a separate IPv6 network. Their IPv6 Gateway service will enable customers to roll-out their own IPv6 services by assigning an IP address to each of their products or services, which is one step toward merging of the two Internet Protocols. In Norway there is no ISP that offers any similar service to their customers, to our knowledge. On the other hand, Asia has very little access to IPv4 addresses as they were very late to build networks. There will not be as many routers and networks that need upgrading.

As the above limitations on transition and translation mechanisms show it will not come as a surprise that ISPs still are reluctant to offer both IPv4 and IPv6 on the same network. In Asia the commercial IPv6 networks seem to be kept separate from the IPv4 network because of these problems. The network community does not seem satisfied enough, because of the lack of fully end-to-end security, for them to merge the two versions of network from the start. Both NTT Communications in Asia, Australia and Europe and Telia in Sweden (in 2001) have preferred to make separate version networks or make their customers use tunnelling.

How and when the merging of the two protocols will take place is not easy to estimate. The different IPv6 Task Forces use the date of 2005 to be a critical year for the IPv4 address space i.e. 15-20 months from now. Very little activity seems to take place in the field of upgrading in most countries, even though many have it on the political agenda.

As the returning dilemma seems to be lack of IPv6 applications, it looks like the lethargy of the chicken and the egg problem. There will be no network to support IPv6 applications until there are applications that have enabled IPv6. There will not be any IPv6 applications until there is a network that demands them. As IPv6 has a more complex structure the upgrading might require severe modification to the application and the manufacturers will be reluctant to do this if there will not be any need for it soon. Even though those who support IPv6 feel that a bad investment is not to make the applications IPv6 enabled, as they see IPv6 as a part of an evolution of the Internet rather than a revolution.

As more and more electronic device provide a need for more addresses, the address-space might run out sooner if one of these devises should reach enormous popularity in a short period of time. This could be a hidden factor that network people do not see today, as the

device is not yet on the market. Cell-phone vendors and similar companies may very well be in the process of making new devices that need static IP addresses to be in use. There are indications but no facts written, as this is most probably highly confidential information.

Some manufacturers have already taken responsibility and stated that by a certain date they will make products that are IPv6 enabled. But will this be enough? Will these manufacturers stick to their plan if nothing happens in other companies that make similar applications or products or if nothing happens to the networks?

Must IPv6 be forced into the network community by the different governments in different countries, by making a decision that by a certain date all university and government networks will be IPv6 only? This will definitely force the manufacturers of applications to make them IPv6 enabled.

The Asian ISPs claim that the IPv6 networks are a great success and that this is the future. They even present it as the only type of network these days, already. Whether this is "propaganda" or actual facts or something in between, is something that needs to be taken into consideration when looking at the future deployment of IPv6.

## 7.5 Experiment

Experiences from the Telenor experiment shows that an upgrade to IPv6 for non-technical end users is still complicated in a small home network environment. It is possible to go through with it, which raises the issue on who wants to go first? Those who start to upgrade first might experience more problems than those who start later. But those who start later might risk falling behind during the roll-out process. Those who start early to upgrade will gain experience and might reach the stage of advanced use of the IPv6 network before those who start later. The sooner the problems of the upgrading are located, the sooner these can be fixed and complicated procedures can be simplified.

The Telenor experiments showed that there was a lack of services for web browsing and file transferring compared to IPv4 Internet for IPv4 host. This means that the quality of service was poorer in this setting for IPv4 hosts. As the connection to dual-stacks was not as good as connection with native IPv4, IPv6 hosts also suffered in quality of service.

The translation methods used showed weaknesses, which might result in that 4-in-6 tunnelling should be used instead when IPv4 connections from an edge network has to be made.

When we contacted people in networking in Norway other factors are given to us for why there is little activity on the IPv6 roll-out in Norway. There are economic reasons and the fact that there is little talk about the subject in their surroundings. Nobody seems to feel any pressure to upgrade. They manage so far with IPv4. Some of those who know some about IPv6 and answer our questions have had bad experiences with products for IPv6. They all seem to be waiting good applications for IPv6.

# 8 Conclusion

In this thesis we have investigated the prospects and problems of IPv6. We have wanted to address the issues of what IPv6 will contribute to the network, what is required for an upgrading and when this has to be done, and finally how the upgrade will be done according to the complexity of IPv6.

To find the information we needed we have mainly used the Internet for articles on the subject. On the technical parts we have used RFCs from IETF. A report from Telenor R&D named "IPv6 migration of unmanaged networks-the Tromsø IPv6 pilot" and contact made with selected Norwegian ISPs also added valuable points, which made it possible for us to answer our questions.

We have given an overview of the problems about IPv4, which mainly are the limited address space and the limited quality of service. IPv6 is supposed to solve these problems, with its expanded address field and improved header format, where the extension headers are the key improvement. The use of extension headers makes the processing time shorter as it is a part of the payload and not the header itself. The managing of IPv6 addresses is also supposed to be more efficiently compared to the system in IPv4 with class A, B and C addresses. We feel that the improvements offered in the new protocol and the chance of a sudden need for an expanded address space is enough reason for the upgrade to take place. As there are already several routers and operating systems that support IPv6, the upgrade should not take too much effort. We think that within a very short period of time there will be even more IPv6 enabled applications, which should make the upgrading even more effortless than it is today.

One of the most important features about IPv6 is that it is supposed to coexist with IPv4. The transition from IPv4 to IPv6 is supposed to be smooth allowing hosts and ISPs to upgrade independent of the network and vice versa. Mechanisms are designed to make this possible.

The mechanisms are mainly divided into:

- Tunnelling mechanisms.
- Translation mechanisms.
- Dual-stack mechanisms.

We have found that the mechanisms are still not standardised and are not perfect. From tests there has proven to be limitations in security, scalability issues and complicated configuration. As a result of this IPv6 networks are built separated from IPv4 networks. According to the Asian ISP's that have built IPv6 networks, the IPv6-only network is a great success and suffers from no great problems, therefore the migration of IPv4 and IPv6 seems to be the biggest challenge and not IPv6 itself. We still feel that when routers and operating systems offer IPv6 enabled systems, the upgrade should be possible to make in the very near future, and we think that those who wait will suffer more than those who start now. We think that the roll-out will take off as soon as it starts outside of Asia.

Globally, the upgrading process is at very different stages. Asia is the leading area, already offering commercial IPv6. Lack of IPv4 addresses has made this a necessary action. At other

parts of the world, e.g. in Norway, the process is still slow, but moving forward. There are many opinions on why the process is slow. One obvious reason for this is the technical aspects. There is still a lack of applications supporting IPv6, and without these there is no need for networks. Other reasons are of economical aspects, upgrading to IPv6 is expensive. Beside this, many ISPs do not experience any pressure to upgrade. So far they feel that IPv4 is adequate. We do think that even though there still is some lack in the transition mechanisms that companies who do work toward the Asian market should very soon consider an upgrade to IPv6.

After our investigation we do feel that there should be more activity on IPv6 in most parts of the world, than it is today, as there might be a shortage to the address space sooner than most people think, as both more people and more electrical devices will consume a lot of addresses in the very near future. Smaller companies with national activity with no global activity could still leave it for some time and wait for a more mature IPv6 stack, but we think that companies with global activity, especially towards Asia should at least start to experiment with IPv6 now.

# References


[1] www.Microsoft.com, *"Introduction to IPv6"*, 27.03.2003
http://www.microsoft.com/windowsserver2003/technologies/ipv6/introipv6.mspx

[2] R. Hinden, *"IPng overview"*, 14.05.1995
http://playground.sun.com/ipng/INET-IPng-Paper.html

[3] Larry L. Peterson, Bruce S. Davie (2000), *"Computer Networks"*, second edition, Morgan Kaufmann publishers, USA

[4] J. Cope, Computerworld, *"IPv6 Is it inevitable?"*, 28.05.2001
URL: http://www.computerworld.com/printthis/2001/0,4814,60869,00.html

[5] C. D. Marsan, NetworkWorldFusion, *"The next best thing to IPv6?"*, 20.09.1999
URL: http://www.nwfusion.com/news/1999/0920ipv6.html

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

[7] R. Hinden, S. Deering, *"IP Version 6 Address Architecture"*, RFC2373, July 1998 (Proposed Standard)

[8] M. Crawford, *"Transmission of IPv6 Packets over Ethernet Networks"*, RFC2464, December 1998 (Proposed Standard)

[9] F. Kileng, T. Solvoll, "IPv6 migration of unmanaged networks-The tromsø IPv6 pilot", 18.02.2003
http://www.telenor.no/fou/publisering/foupubl.shtml

[10] V. Cerf and R. Kahn, *"A protocol for Packet Network Interconnection"*, IEEE Transport of Communications Com-22 (5) 637-648, May 1974

[11] S. Deering, *"Next steps for IPv6 standards"*, Global IPv6 summit in Korea 2002, presentation I-1
http://www.ipv6.or.kr/summit/presentation/I-1.pdf

[12] Commission of the European communities: Communication from the Commission to the Council and the European Parliament; *"Next Generation Internet –priorities for action in migrating to the new Internet protocol IPv6"*, Brussels 21.02.2002
URL:
http://www.europarl.eu.int/meetdocs/committees/agri/20020710/com(2002)080_en.pd

[13] S. Hagen, *"IPv6: Revitalizing the Internet Revolution"*, September 2002
www.oreillynet.com/lpt/a/2741

[14] S. King, R. Fax, D. Haskin, W. Ling, T. Meehan, R. Fink, C.E. Perkins, *"The case for IPv6"*, Internet draft, version 6, 25.12.2002
http://www.6bone.net/misc/case-for-ipv6.html

[15] A general IPv6 information homepage
http://www.ipv6.org

[16] S.Hagen (2002),*"IPv6 Essentials"* , first edition, O'Reilly & Associates, Inc., USA.

[17] G. H. Anthes, Computerworld, *"Internet Protocol Version 6"*, 20.01.2003
URL: http://www.computerworld.com/printthis/2003/0,4814,77627,00.html

[18] R. Hinden, S. Deering, R. Fink, T. Hain, *"Initial IPv6 Sub-TLA ID Assignments"*, RFC 2928, September 2000 (Informational)

[19] Ericsson Telebit AS, *"Tunneling"*, 13.01.2003, Appendix

[20] B. Karpenter, K. Moore, *"Connection of IPv6 Domains via IPv4 clouds"*, RFC 3056, February 2001 (Proposed standard)

[21] B. Karpenter, C. Jung, *"Transmission of IPv6 over IPv4 Domains without Explicit Tunnels"*, RFC 2529, March 1999 (Proposed standard)

[22] C. Huitema, *"Shipworm: Tunneling IPv6 using UDP through NATs"* , Internet draft, version 3, 16.10.2002
http://www.ietf.org/proceedings/01dec/I-D/draft-ietf-ngtrans-shipworm-03.txt

[23] E. Nordmark, *"Stateless IP/ICMP Translation Algorithm (SIIT)"*, RFC2765, February 2000, (Proposed Standard)

[24] G. Tsirtsis, P. Srisuresh, *"Network Address Translation - Protocol Translation (NAT-PT)"*, RFC 2766, February 2000, (Proposed Standard)

[25] H. Kitamura, *"A SOCKS-based IPv6/IPv4 Gateway Mechanism"*, RFC 3089, April 2001, (Informational)

[26] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, L. Jones, *"SOCKS Protocol Version 5*", RFC 1928, March 1996, (Proposed Standard)

[27] J. Hagino, K. Yamamoto, *"An IPv6-to-IPv4 Transport Relay Translator"*, RFC 3142, June 2001, Informational

[28] M. Blanchet, F. Parent, *"IPv6 transition mechanisms"*, May 2002, Viagénie
URL: http://www.viagenie.qc.ca

[29] K. Tsuchiya, H. Higuchi, Y. Atarashi, *"Dual Stack Hosts using the Bump-In-the-Stack Technique (BIS) "*, RFC 2767, February 2000, (Informational)

[30] S. Thomson, C. Huitema, *"DNS Extensions to support IP version 6"*, RFC 1886, December 1995, (Proposed Standard)

[31] S. Lee, M-K. Shin, Y-J. Kim, E. Nordmark, A. Durand, *"Dual Stack Hosts Using Bump-in-the-API (BIA)*, RFC 3338, October 2002 (experimental)

[32] IPv6 Promotion Counsil, Japan
URL: http://www.v6pc.jp/en/index.html

[33] IIJ Hompage, "IIJ to Extend Trial Period for IPv6 Tunneling and Native Connectivity Services", Press release, Mach 11, 2002
URL: http://www.iij.ad.jp/en/pressrelease/2002/ipv6-e.html

[34] NTT Communications' Home Page
URL: http://www.v6.ntt.net/globe/index_e.html

[35] U.S. Department of Homeland Security, *"The National Strategy to Secure Cyberspace"*, February 2003
URL: (http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf)

[36] *"Welcome and Introduction"*, Document on IPv6 Task Force pages, Europe. (September 2002)
URL:
http://www.ec.ipv6tf.org/PublicDocuments/IPv6TF_second_phase_welcome.pdf

[37] www.ipv6-taskforce.org

[38] NTT Europe Home Page
URL: http://www.ntt.co.uk.

[39] IPv6Style, Internet education site sponsored by NTT Communications
URL: http://ipv6style.m-t.com/en/index.html

[40] *"Strukturen for testnett"(" the topology of the test network"),* 17.02.2003, Uninetts homepage
URL:http://www.uninett.no/testnett/bilder/ipv6.gif