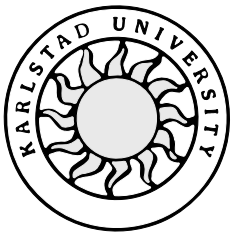

Computer Science

Floyd Andersson

Annika Fransson

Technical Investigation of IPv6 in Mobile Internet

Bachelor's Project

2001:12

Technical Investigation of IPv6

in Mobile Internet

Floyd Andersson

Annika Fransson

This report is submitted in partial fulfillment of the requirements for the Bachelor's degree in Computer Science. All material in this report which is not our own work has been identified and no material is included for which a degree has previously been conferred.

Floyd Andersson

Annika Fransson

Approved, 5 June 2001

Advisor: Eivind Nordby

Examiner: Stefan Lindskog

Acknowledgments

We would like to thank
our families for their support and
patience with us during this work.
We would also like to thank
Lennart Johannesson at Kipling
and
Eivind Nordby for their
advice, direction and support during the project.

Abstract

This technical investigation of IPv6 in mobile Internet has been a bachelor's project and the purpose was to see possible consequences and possibilities for a future transition to IPv6 and how a transition may affect mobile products. IPv4 is the present Internet Protocol, and since the addresses are running out, IETF, a standardisation organisation, decided that a new protocol should be developed. IPv6 is an upgraded version of IPv4 and has one of the biggest advantages in the large address space. The new design of IP also meets future requirements like security and Quality of Service (QoS). A decision has been made to introduce IPv6 as one of the protocols of the future 3:rd Generation (3G) networks, which will create a great demand for IP addresses that IPv4 cannot supply. Although, the IPv6 standard is not ready, the question is not if IPv4 is going to transit to IPv6, it is only a question of when. The conclusion for this report is that for future mobile applications that will have “always-on” connections, IPv6 will be the only alternative.

The final results are that companies that work with an operating system that supports IPv6 with dual stacks, does not have to change their IPv4 applications; the operating system makes sure that applications will still work unaffected.

For future developed applications that run on an operating system that contains support for IPv6, there will be no need for supporting IPv4; in these products it will be sufficient with IPv6 only.

Companies that are developing mobile products for 3G networks have to transit to IPv6 when the net in Sweden is put in operation in the end of 2003.

Contents

List of Figures

List of tables

1 Introduction

This is a bachelor's project that constitutes 10 credit points and is performed by Floyd Andersson and Annika Fransson. The project is done at Kipling Karlstad, which is a subsidiary of Kipling Holding AB, with focus on product development of Mobile Internet products in a telecom environment. The group also has four other companies in Sweden, and is also represented in Great Britain and Brazil. The products that Kipling are working on now are service enablers in the Mobile Internet with a special focus on WAP, SMS, GPRS, 3G, Mobile Push and Mobile Positioning. Kipling supplies software systems and consultancy services to the telecommunication sector.

1.1 General introduction

When looking for a project, we contacted Kipling since they are active in computer communications, which is what we found interesting. Among their bachelor projects we chose Technical Investigation of IPv6 in Mobile Internet, which suited us best.

The suggested focus area were:

- Identify the driving forces for a transition towards IPv6
- Utilize features of IPv6 that can improve Kipling's products
- Design impact on Kipling's products

1.2 Background

This section gives the reason to why our work was needed. Since 1983, Internet Protocol version 4 (IPv4) has been used for addressing through the Internet (appendix A). A good reason to its tremendous success is its simplicity, but for being used for about twenty years some problem has turned up. The fact that the addresses are going to depletion is a well-known problem. A temporary solution called NAT (appendix C.3) has been, and still is, a solution to use the IPv4 address space more efficiently. NAT servers have lengthened the time of getting a new solution, but do not definitely solve the problems for the future mobile devices that will need to be uniquely addressed and have always-on connections.

So, several years ago, the IETF started working on a replacement version of the Internet Protocol. The result was Internet Protocol version 6 (IPv6). This refreshed and upgraded version of IPv4 should also have better performance in order to support new services that have appeared as a requirement in many applications.

A good reason to start this investigation about IPv6 in mobile Internet is mainly because the introduction of the future Third Generation (3G) networks. The Third Generation Partnership Project (3GPP) is a global standardization initiative that works for the produce of technical specifications for Third Generation Mobile System [12]. An initiative for a coming transition toward IPv6 is that the 3GPP has decided to introduce IPv6 as one of the protocols for the future Third Generation (3G) networks.

This report was therefore initiated by Kipling to start learning about IPv6 and to get some information on driving forces, features and transition strategies of IPv6 in mobile Internet.

1.3 Purpose of this project

The purpose of this project is to write a report that can give an insight of the use of IPv6 in mobile Internet, and hopefully it can be useful for Kipling when introducing IPv6 in their products. It is our purpose to give satisfactory answers to the specified task (appendix J).

Right now, everybody is waiting on each other since nobody wants to be first to make all the mistakes or be as an isolated island that runs IPv6. On the other hand they want to be up to date with the latest technology to be attractive on the market, preferably better than its competitors.

This report can be as a start for Kipling to learn about IPv6, to be prepared for the coming shift of IP protocol. After reading this report it may be easier to make an opinion when the time is ready for IPv6.

1.4 Scope of the task

This project could be very huge and were therefore restricted in several ways. The scope was to get the answers to the questions (next section 1.5) we got from Kipling. When we searched information about Kiplings products, we found that more protocols were involved besides the Internet Protocol, in the GSM network and UMTS, but these are not discussed in this report.

We discuss and identify facts about IPv6 both in general perspective and for mobile Internet. With this limited time there is not in our scope to deliver the result in details. In the beginning we did a project plan that helped us to set breakpoints for the activities. The

specification that we made was decided to focus more on the width than of the depth. In the conclusion we recommend Kipling which strategy to use for the transition. This is only done with the focus on the IP protocol. More affects may appear but is not discussed in this investigation.

1.5 Goal

The goal of this work is to be able to deliver a report of importance with information about the coming transition to IPv6. News in the computer industry, especially in data communications, travels very fast so it is important to be aware of these new technologies, and of how other companies act. It is our goal to give a satisfied answer of the specified task (appendix J) but also to get the answer of the following questions. The goal is therefore to deliver a report that can give some answers to the questions below based on information we found through this investigation. Kipling wanted us to answer the following questions to satisfy the goal:

- What are the driving forces for transition towards IPv6?
    - Why ought Kipling change from IPv4 to IPv6?
- What are the greatest advantages of IPv6 that Kipling can make use of in their products?
    - Are there any disadvantages against a transition towards IPv6?
    - What can IPv6 offer in a security aspect?
- When should Kipling transit to be competitive towards their competitors?
- What strategy will be used at the transition?
    - What are the consequences for the company and their products?
    - Is a transition leading to great changes?
    - Do the products need to run both versions at the same time, or just change everything over a night?

After reading this report it is our goal to make it easier make an opinion about the answer of the questions above, but some of them do not have the right answer yet, since there is no final standard for IPv6 yet. This is a very hot topic and some of the questions we got are to be treated in the next meeting for 3GPP (appendix K).

1.6 Overview

This report starts with an introduction of the Internet Protocols. The function of this is to give the reader some information about the Internet Protocols, IPv4 and IPv6. If the reader is familiar with these protocols, it can be treated as optional. The purpose of it is to let other readers to have a better knowledge about what the differences are between the both versions. It also makes it easier to understand why it is necessary to transit to IPv6 and will give the base to the following discussions throughout the rest of the report.

After the descriptions of IPv4 and IPv6 we identify what the driving forces are, what features IPv6 may add to the IP protocol and how the transition may be done in general. Then we introduce the result, which is concentrated on how Kipling is affected by IPv6, in consideration to the questions defined in previous section.

Chapter 2 gives a technical overview of the headers in the Internet Protocols, IPv4 and IPv6. A brief introduction to the extension headers, in IPv6, is also included in this chapter.

Chapter 3 gives an overview of why there is a need for IPv6, and who needs the next Internet Protocol. A section will describe who supports IPv6. When it is necessary to do the transition to IPv6 will also be discussed.

Chapter 4 identifies what features IPv6 adds to the Internet Protocol. This is a general description and do not only have its focus on mobile Internet.

Chapter 5 describes different strategies to enable both IP versions, IPv4 and IPv6, to coexist.

Chapter 6 presents the result of the investigation of IPv6 in mobile Internet. This presentation is based on earlier chapters and is introduced as answers of the questions we got from Kipling.

Chapter 7 describes the approach of the task, and what experiences this project gave us.

The report ends with our references, a list that describes some terms used in this report and some appendices. These appendices contain detailed information that is referred to from this report.

2 Technical overview of the Internet Protocols

Every computer connected to the Internet has a unique identifier, the Internet Protocol address. The Internet Protocol makes it possible to connect computers between different networks without knowing anything about the other computers, except from its addresses. Besides a uniquely identifying address to each computer, the computers must be able to send and receive data to and from all other computers in a format that any computer can understand. IP achieves these goals. In this chapter we will give you a technical introduction to the Internet Protocols, IPv4 and IPv6. We are going to describe the headers with their fields, and we will also describe the IPv6 extension headers. When the reader have read this chapter, it will be easier to see the differences between these two protocols appendix E. If the reader wants to read about the address structure in IPv6 and the control messages sent between nodes, we refer to appendix B.

2.1 Internet Protocol version 4

IPv4 [1] is the most common protocol used for communication between network-connected devices. All IPv4 addresses are 32 bits long, and encode a network and a host number. The formats used for IP address are shown in Figure 1.

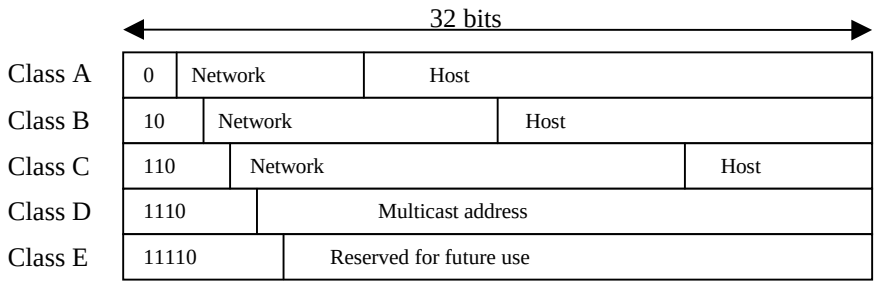

Figure 1: IPv4 address formats.

The A, B, C, D, and E formats allow up to 126 networks with 16 million hosts each, 16,382 networks with up to 64K hosts, 2 million networks with up to 254 hosts each, and multicast, in which a datagram is directed to multiple hosts. Class E is reserved for future use.

2.1.1 IPv4 header

An IP datagram consists of a header part and a text part. The header in IPv4 (Figure 2) has a 20-byte fixed part and a variable length optional part.

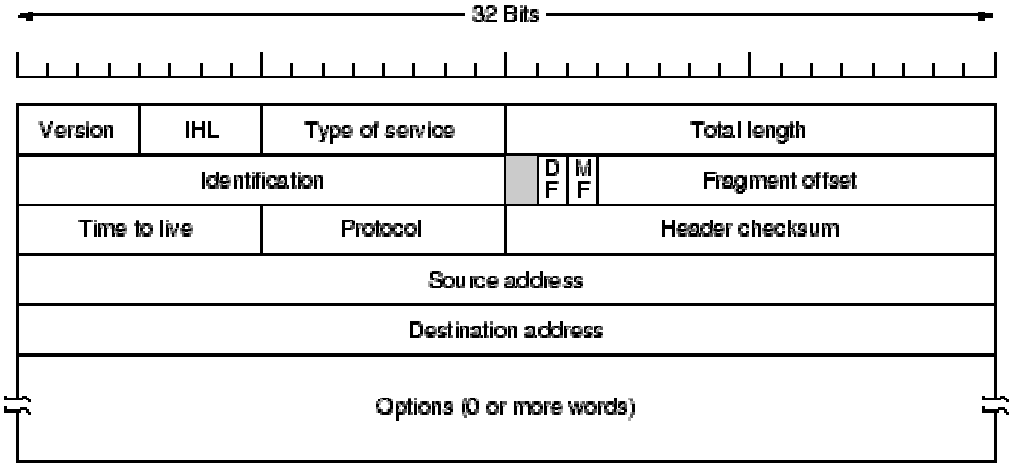

Figure 2: The IPv4 header

The **Version** field keeps track of which version of the protocol the datagram belongs to. This is the first field processed, because the recipient must know how it should interpret the rest of the header.

Since the header length is not constant, a field in the header, **IHL** (IP Header Length), is provided to tell how long the header is. IPv4 headers can be anywhere from 5 to 15 32-bit words.

The **Type of service** (TOS) field allows the host to tell the subnet what kind of service it wants. One TOS bit may be chosen to signify preferences about how the datagram is to be processed: delay, throughput, reliability or cost.

Total length includes everything in the datagram, including header and payload.

Identification is a datagram ID. This unique 16-bit identifier is assigned to a datagram by the host that originates it. There is a single ID for each datagram the host transmits. These datagrams may be fragmented as they pass through different networks on their way to their destination. This ID makes it possible for a defragmentation to take part.

Some flags are included and the first of these flags is unused.

When the **DF** (Don't Fragment) flag is set to 1 it means that the datagram should not be fragmented on its way towards the destination. **MF**, More Fragments, is set to 1 if more fragments are on the way. When it is set to 0, it means that there are no more fragments or that the datagram was not fragmented. The Fragment offset tells where in the current

datagram this fragment belongs. All fragments except the last one in a datagram must be a multiple of 8 bytes, the elementary fragment unit.

The **TTL** is a counter used to limit packet lifetimes. It is supposed to count time in seconds, allowing a maximum lifetime of 255 sec.

The **Protocol** field tells which transport protocol to give it to, TCP, UDP or some others.

The **Header checksum** does not provide any reliability services, because this checksum is done on the header only.

Source address and **Destination address** indicates the network number and host number of the originating- and destination hosts.

The **Option field** is the last field in the header. It is possible to specify how secret the datagram is or to let each router place their IP-address. But as the name implies it is strictly optional and not often used, (the form they take in IPv6 is radically different). Available options relate mostly to routing. A brief description about the options you can find in appendix A.1.

2.2 Internet Protocol version 6, IPv6

This section introduces the Internet Protocol version 6 (IPv6), also known as IP next generation (IPng). We are going to describe the header and the extension headers. A short introduction is also done of the IPv6 addressing structure and the Internet Control Message Protocol version 6 (ICMPv6).

2.2.1 IPv6 header

When comparing IPv4 and IPv6 headers, some of the fields are entirely unchanged and some are deleted. The header length is not interesting any longer as the IPv6 header has a fixed size. The length of the IPv6 header without extension headers is 40 bytes.

The fragmentation field is no longer in the base header because fragmentation is no longer available in routers, just only at the source. Another field that also is eliminated is the Header Checksum field.

The IPv6 header (Figure 3) defined in RFC 2460 [5].

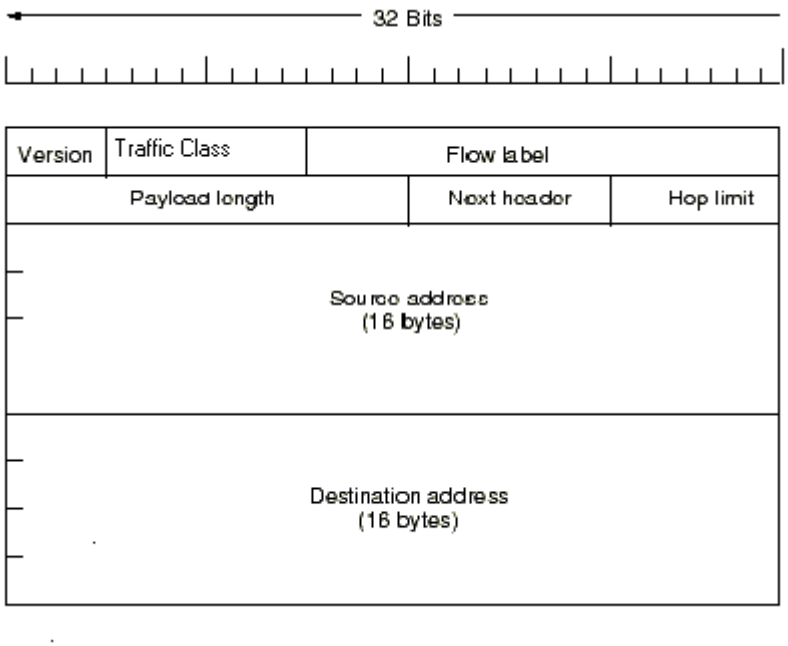

Figure 3: The IPv6 header

Version Field is four bits long, and identifies the version of the protocol. For IPv6 the version is equal to 6. The Version field is the only one that remains the same in both versions of the protocol, though its value changes. The reason for this is that during the transition period, IPv4 and IPv6 must coexist, and it must be possible to decode which version of the IP datagram it is dealing with.

The field for *Type of Service* is replaced to the similar field **Traffic Class** but positioned earlier in the header than before. The Type of Service field in IPv4 has never really been utilized and has been changed several times. In some books the field is not even mentioned, later on the name of it was Priority and 4 bits long, then it was renamed to Class, but in RFC 1883 it was renamed again to Traffic Class. In RFC 2373 published in July 1998 the name has

become Traffic Class and the length has changed to 8 bits, and is intended for originating nodes and/or forwarding routers to identify and distinguish between different classes or priorities of IPv6 packets. Values and precise use of the Traffic Class is not yet exactly determined [5].

The **Flow Label** field is 20 bits long, and may be used by a host to request special handling for certain packets, such as those with a none default or real-time QoS. This field is not yet determined [5].

The **Payload Length** field is a 16-bit unsigned integer that measures the length of the payload. Note that optional extension headers are considered part of the payload. The Payload Length field is similar to the IPv4 *Total Length* field, except that the two measurements operate on different fields. The Payload Length (IPv6) measures the data after the header, while the *Total Length* (IPv4) measures the data and the header. Payloads greater than 65536 are allowed and are called jumbo payloads. To indicate a jumbo payload, the value of Payload Length is set to zero and the actual payload length is specified within an option that is carried in a Hop-by-hop header.

The **Next Header** field in IPv6 has replaced the protocol field and is 8 bits long and identifies the header immediately following the IPv6 header. The field *Protocol* in IPv4 referred to the next-higher layer protocol encapsulated within the IPv4 packet. This protocol field has evolved to Next Header. Next Header can be one or more of the extension headers that are available in IPv6 or another layer protocol.

The **Hop Limit** field is 8 bits long and its value decrements by each node that forwards the packet. When the Hop Limit equals zero, the packet is discarded and an error message is returned. The *Time To Live* has become the Hop Limit, earlier it was meant that the packet lifetime should be measured in seconds. In practice the routers did not measure the time instead they just decrement the time by one second at each hop. Therefore a Hop Limit is more relevant in this field.

The **Source Address** field is a 128-bit field that identifies the originator of the packet and the **Destination Address** field is a 128-bit field that identifies the intended recipient of the packet. The space of the addresses has increased from previous 32 bits to 128 bits.

2.2.2 The IPv6 extension headers

The IPv4 header was designed by placing many of the existing fields as optional. In IPv6 options have been moved out of the base header, and specified as Extension Headers. Its

function is not eliminated but separated into extension headers with almost same function that IP options had, but with better performance than just as options (appendix B.3).

2.2.3 IPv6 address structure

Each IPv6 address consists of a 128-bit number. The way of writing the addresses will be different depending on the longer address space and a new way of representing it. Dots are exchanged with colons. They should be written in eight groups of hexadecimal digits separated by colons, with four digits in each group. Addresses will be represented like this; 14.2.69.4 will be compatible with IPv6 in the form: 0:0:0:0:0:0:14.2.69.4 or ::14.2.69.4. Compressed form excludes the repeated zeros in the address.

Precisely as in IPv4 some addresses are reserved according to a specific bit pattern to different uses (appendix B.1). Broadcast addresses are no longer available. The IPv6 addresses belong to one of three categories, which are unicast, multicast and anycast (appendix B.4).

2.2.4 ICMPv6

IP nodes need a special protocol to exchange messages that relate to IP conditions. The Internet Control Message Protocol (ICMP) fulfills this need. If a router is unable to process an IP packet for some reason an ICMP message is used to report it. ICMPv6 is a new version of the Internet Control Message Protocol and is documented in RFC 2463 [7]. ICMPv6 is considered an integral part of IPv6 and must be implemented by every IPv6 node. This protocol is used to report processing errors and the messages will be sent directly back to the packet source. Except for reporting ICMP messages (appendix B.7) for error it is useful to report informational conditions as well as diagnostic functions like ping and tracing route.

3 Driving forces behind a transition towards IPv6

In this chapter we will explain why a new Internet Protocol is needed, and who needs the new protocol. There will be a section about which vendor's supports IPv6 at this moment of time. We will also try to predict when the transition should be done.

3.1 Why a new Internet Protocol?

When it appeared that the existing IP address space would support continued Internet growth for only a relative short time, TCP/IP engineers and designers recognized the need for an upgrade of the IP protocol. This was as early as the late 1980s.

Up until 1994 there were a few different proposals that were presented as probable successors to IPv4. In 1992, three dominant proposals were considered (appendix B) by the Internet Engineering Task Force (IETF) [11]. The chosen solution was IP version 6, the next-generation Internet Protocol. IPv6 was recommended by the IETF seven years ago in July 1994, and the recommendation was approved and made as a proposed standard by the Internet Engineering Steering Group (IESG) on November 17, the same year 1994. Since then IPv6 has been in development with the intention of replacing today’s IPv4.

There are three main temporary solutions to get around the problem with the lack of addresses (appendix C). The most common solution today is NAT (appendix C.3), which gives IP addresses that is unique only internally in that network, not in the real Internet. This gives no possibility to address globally, which made people to do ad hoc solutions or application-specific solutions. It is impossible to find out the quantity of IP addresses that really is needed, because of the NAT algorithms. But with new Internet devices, like mobile phones, cars and other devices, the demand of more IP addresses will be very huge. The IPv4 address space is not big enough. Of course it is possible to make NAT a bit better but that includes more complicated protocols that might improve their functionality and increase their complexity, fragility, obscurity, and unmanageability.

3.2 Who needs IPv6?

The increase of the Internet connectivity is huge in many countries. In Asia, China and India both having over a billion of inhabitants, the demand for more IP addresses is huge. Even

Japan did not receive much IPv4 address space. In China a school system with 60000 schools recently (CY 2000) applied for IPv4 addresses and was awarded an entire Class C network. Just 254 actual IPv4 addresses for many millions of children and teachers [19]. When Asia requires unique IP addresses there is no chance of going around the problem any longer. Therefore Asia is a major force that wants IPv6.

In North America the crises of addresses is not as big as it is in the rest of the world, but even here the lack of addresses is a problem. On the other hand a small number of entities that got Class A IP addresses in the early days, like MIT and AT&T, each control over 16 million addresses [31]. Most companies now applying for IP addresses have to accept getting a fraction of the remaining Class C addresses.

Vendors of networked appliance points out that they will need IP addresses for millions of devices for data networking. The reason for this is that, in a near future people will start to use wireless and portable computers, such as Personal Digital Assistant (PDA), and mobile digital telephone services in a much larger scale than today. The huge increase of these devices, together with today's limits of addresses is definitely something that will enforce the expansion of IPv6.

UMTS have some requirements that IPv6 can solve like

- A great number of IP addresses are needed.
- The UMTS networks also have a stricter requirement for the security on the Internet services than IPv4 can provide.
- The QoS is an issue that is far more important in the UMTS networks than it has been in the Internet until now.

Operators that got a license to build the next generation mobile network based on the UMTS network will force the transition so they can fulfill their requirements.

When car manufacturers want IP for Tele-maintenance and mobile Internet services, there will be a great demand for addresses.

If you add to that all Internet appliances for home (refrigerators, ovens, washing machines, MP3 players, TVs) and industrial (sensors, weapons), there will be need for billions of address for global reachability.

3.3 Who supports IPv6?

In March 2000, almost six years after the first IPv6 RFC specification was published, the world biggest router company, Cisco, made a firm commitment to integrate IPv6 in their

products. At the same time as Cisco took their decision to integrate IPv6 in their products, Microsoft did the same. At that time other vendors including Sun, 3Com and Nortel already supported IPv6.

An aspect from IBM is, “IBM understands the importance of IPv6”, says Sue Horn [20], an IBM vice president tasked with leading the company’s IPv6 initiatives. “We understand it takes support across our operating systems, middleware and back-end systems. We are putting an end-to-end focus on IPv6.” Horn does not anticipate significant customer demand for IPv6 until 2002 or 2003, but she considers the technology a critical part of IBM’s e-business strategy.

Hewlett-Packard officially say they plan to be a lot more active in IPv6 development in the future. “I am seeing more requirements from my customers for IPv6”, says My Phan [20], technical director of HP’s Systems and Networking Solutions Lab. HP has offered an IPv6 developer’s kit for two years and will add IPv6 support into its Unix operating system core in 2001. HP also plans to offer IPv6 support in handhelds, printers and network management software.

Microsoft has also announced an upgrade to its IPv6 tool kit for Windows developers available as a free download since March 2000. Microsoft’s IPv6 Technology Preview now includes a browser, basic utilities such as telnet, FTP, and support for tunneling IPv6 traffic over an IPv4 backbone. However, Microsoft will not ship a commercial version of Windows 2000 with built-in IPv6 for another two years (2002), admits Tony Hain [20], program manager of IPv6 for Microsoft’s Windows Networking group. Hain says Microsoft is focused on getting application developer to support IPv6 first, so the technology will be useful to customers and business when it ships.

The Linux community will add other tunneling drivers to let IP transport data from other protocols, such as the ones Linux already supports (IPX, AppleTalk, SMB, and LLC). The Linux 2.2 kernel supports TCP/IP Version 6 (IPv6), the forthcoming upgrade to existing IPv4 [32]. Solaris 8 Operating Environment will satisfy support for IPv6. The software has an integrated a dual IPv4 and IPv6 stack [16], it means that unmodified IPv4 applications will continue to work unaffected.

3.4 When will the transition take place?

Optimists for IPv4 says that IPv4 still has a few good decades left, but pessimists say it is more likely a few years. If only the standard gets ready, most of the software developers will start to build systems that will support IPv6.

“Ericsson, is one of the driving forces toward a final standard” according to Sören Torstensson, Ericsson. "Ericsson's hope is to have a final standard in the end of this year." With a final standard the implementation of products with IPv6 can take speed, and for companies that will compete in the mobile Internet with the 3G-telephone networks, it requires that the work of IPv6 start right now. The natural thing is to start upgrading the routers in the kernel of Internet. If the final standard for IPv6 is ready in the end of 2001, it supposed to be implemented at these routers in 2004.

Since 3GPP has mandated IPv6 for next-wave wireless networks [18] it can result in an explosion of handheld devices that can talk Version 6 during the next few years.

The UMTS network in Sweden has the goal to be ready at 31 December 2003. Since, IPv6 will be one of the protocols in UMTS it is time to start to plan for a transit.

When products are ready for sale it probably increases the need of IPv6 addresses very quickly. How quick this will happened depends on what “killer-application” might come up.

3.4.1 Killer application makes the transition go faster

What the killer-applications will be for mobile Internet is what everyone wants to know, but none has the answer of it, at least not yet.

One opinion is that **mobile positioning** will be the killer. But this kind of service can on the other hand have the opposite influence to the users, which can feel too much supervised. To use it for knowing about new places, nearby services, and to know where the rest of the family is, will probably be services that we want to have. But it is not so good if anyone can follow every step you take. With some control of the privacy it can be the killer-application for the future.

Other says that **multiple services** will be the killer. That means that with many different services to choose between, it will be something for everyone.

Multimedia Messaging and **games** over the Internet could also be killers.

New applications using the **push technique**, where messages can be sent directly to the mobile phone using the always-on connection.

4 Features of IPv6

This chapter identifies what features IPv6 adds to the Internet Protocol in general. Some of the features are already proved and others do not have ready specifications and are still mentioned as features. Since no real decisions have been taken about QoS and the security in mobile Internet they are therefore described as they are expected to work.

Features that we have decided to mention are the larger address space, performance, hierarchical routing, mobility support, security, QoS, header compression and the effect of introducing IPv6 in a longer perspective.

4.1 Larger address space

The fact that the IP address space crises has grown further for each year is the prime motivating factor behind all the upgrade efforts. One of the biggest advantage is therefore that IPv6 solves the problem with lack of addresses, that otherwise will run out. IPv6 has 128-bit (16-byte) source and destination IP addresses. The **128-bit address** is divided into a prefix (appendix B.1) and a suffix, were the last part is a 64-bit identification of the individual interface.

The longer addresses make it possible to express over 3.4×10^{38} possible combinations [30], which is enough for a separate address for every grain of sand on the planet. This can be compared to IP version 4 with its 4 billions, which in practice had its limit to only a few billion devices.

Mobile IP requires a permanent global IP address for each device, and there is simply not enough address space in IPv4 to cover all the mobile terminals running through the public Internet. Mobile IPv6 will be easy to expand to handle large-scale mobility needs. In this way it can solve the problem of mobility between networks and access technologies on a global scale.

IPv6 supports **multicast** (appendix B.4) technology for distributing IP packets to a group of destination addresses.

4.2 Performance

Although IP performs remarkably well, some of the design decisions made twenty years ago in retrospect could need some improvements.

As a header in IPv4 can have various lengths it affects the routers different. IPv4 headers without options are always 5 bytes long and easy to process. Each IP-packet has a head that specifies a lot data about de packets contents. The various size of the header is the most obvious. With **fewer fields** and **fixed-length** the IPv6 header helps reduce the processing overhead and increase the performance at the routers.

Because the main issue for a router is to give high throughput of packets and to give optimal route, the majority of IPv4 packets are sent without options as the routers are optimized to handle these ones. Packets that were sent with options were set aside to be handled when more convenient for the router. That has the opposite result of using the options. Applications that need a lot of throughput can provide the opposite effect that was suspected.

Another thing that affect optimization for routers is that with IPv6 they no longer need to do **fragmentation**. Fragmentation will only be possible at source-nodes.

4.3 Hierarchical routing

Further is hierarchical routing a feature that has improved efficiency in mobile routing with IPv6. Hierarchical routing is accomplished by breaking the Internet into a hierarchy of networks, where each level is responsible for its own routing. IPv6 **hierarchical address structure** enables shorter routing tables than with IPv4. The growth of the routing tables has been a big problem for routers. Especially at routers that route near the Internet backbones, (default –free routing tables) and therefore must know all the routes the routing table has to list for every separate network. IPv6 is promoting major advantages to these backbone routers, enabling efficient routing hierarchies that limit the uncontrolled growth of them.

The growth of the Internet and the ability of Internet backbone routers to maintain large routing tables easier is a performance issue to strive for. The efficient of the routing algorithm is also affecting the QoS as it can minimize the delay for transmissions.

4.4 Mobility Support

This section handles autoconfiguration, mobility and some information of mobile IPv4 and what changes mobile IPv6 will offer. Mobility support is built into IPv6. IPv4 usually relies on a hierarchy of fixed address spaces (sub-networks) to route traffic. Mobility in IPv4 is handled by a two-phase routing first to a fixed address (so no updates to backbone routing tables are required) and then to a forwarding address that may change over time. When an IPv6 device connects to a network at any location, it can find any autoconfiguration server on the network and be automatically recognized by network routers. An IPv6 device can connect with the same address to any physical location in the network [21].

4.4.1 Autoconfiguration

IPv6 includes "**plug and play**" in the standard specification. It will therefore be easier for novice users to connect their machines to the network cause it will be done automatically. For mobile users, that always moving from one location to another the advantages with IPv6 is even greater. That is because IPv6 supports **autoconfiguration**. Thanks to autoconfiguration in foreign networks, no triangular communication via home agent is needed. Both IPv4 and IPv6 can use dynamic host configuration protocol (DHCP) for their configuration. Why IPv6 is smarter at solving problems than IPv4 is because IPv6 nodes automatically can configure themselves, only with DHCPv6 that requires the maintenance of state and is therefore called **stateful** configuration. IPv6 can also use **stateless** autoconfiguration. Using neighbor discovery, an IPv6 node can be plugged into any network, seek out a stateless autoconfiguration server, and be configured to interoperate all without human intervention. Computers assign themselves an IPv6 address. These features makes for true plug-and-play network access and through neighbor discoveries are able to automatically determine which routers on their links are available and reachable. IP address assignment on the organizational level is also simplified.

Most current IPv4 implementations must be either manually configured or use a stateful address configuration protocol such as DHCP. With more computers and devices using IP, there is a need for a simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure. Configuring IPv4 nodes has always been complex, but network administrators as well as users would prefer to be able to "plug and play".

4.4.2 Mobile IP

This section describes only in a brief way how mobile IPv4 (appendix F) and mobile IPv6 (appendix G) works. Mobile IPv4 and Mobile IPv6 have its major differences, though mobile IPv6 does not have Foreign Agents. The standard for mobile IPv6 is still under development.

In Mobile IPv6 (MIPv6), each mobile node is identified with a home address independent of its current point of attachment to the Internet. The IP address consists of two parts: the subnet identifier and the interface identifier. The interface identifier identifies a single interface within an IP subnet and does not take part in routing process. The subnet identifier, on the other hand, identifies an individual subnet within the internet work and is controlling the routing between different subnets. When the mobile node is situated away from its home, it can be associated with a care-of address that provides information about the current location of the mobile node. The home address and correspondent node are informed of the care-of address each time the mobile node changes location. For packets sent by a mobile node while away from home, the care-of address is typically used as the source address in the IPv6 header of the packet. By including a home address option in the packet, the correspondent node receiving the packet is able to substitute the node's home address for this care-of address when processing the packet. Therefore, IPv6 packets that are addressed to the mobile node are transparently routed to the node's care-of address.

4.5 Security in the Network Layer

Security is another advantage that speaks for IPv6 since it is an integrated part of the protocol. IPv6 will support the IETF [11] Internet Protocol Security (IPsec) [10] recommendations and standards for security. Different technologies allow secure, private communication independent of how the data is carried through various public networks. Private communications over a public medium like the Internet requires encryption service that protects the data being sent from viewing or modification. Although a standard now exists for providing security for IPv4 packets (known as Internet Protocol security or IPsec), this standard is optional in IPv4. IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH: Authentication Header). For end-users it is possible to run more secure intranets since IPv6 offer encryption and authentication services.

4.5.1 Security in IPv6

IPsec specified in RFC 2401 [10], is embedded and standardised as built in the stack in IPv6, which is a bonus of IPv6. The goal of IPsec is to provide interoperable, cryptographically based security for IPv4 and IPv6. Even though IPsec is available for IPv4 network, the NAT [C.3] gateways that sit at the edge of many large networks can slow down the encryption process.

Private communications over a public medium like the Internet requires encryption service that protects the data sent from being viewed or modified in transit. IPv6 includes security in the basic specification. It includes encryption of packets (ESP: Encapsulated Security Payload) and authentication of the sender of packets (AH: Authentication Header). For end-users it is possible to run more secure intranet since IPv6 offer encryption and authentication services.

The use of authentication and security features at the IP layer has been debated for years, and includes secure password transmission, encryption and digital signatures of datagrams. All data that follows an **authentication header (AH)** remains in plain text and may be intercepted by attackers. The **encapsulating security payload (ESP)** header makes it possible to encrypt the contents of a packet, (all data that follows an ESP header is encrypted).

Three goals are mentioned when talking about security and will be satisfied by IPv6 [3].

- **Authentication**. The ability to reliably determine that data has been received as it was sent and to verify that the entity that sent the data is what it claims to be.
- **Integrity**. The ability to reliably determine that the data has not been modified during transit from its source to its destination.
- **Confidentiality**. The ability to transmit data that can be used or reads only by its intended recipient and not by any other entity.

4.5.2 Security in mobile IPv6

The IP-based services will have strong impact on the mobile telecommunications business. As IPsec is built in the IPv6 stack it can enable seamless remote Intranet access, as well as corporate virtual networking. This is possible even when end users wants to stay always connected to their corporate Intranet. This “always-on” type of service is not readily achievable with IPv4 technology.

Destination options must be authenticated using AH or ESP. Both of the headers provide sender authentication, data integrity protection, and replay protection. In addition, the ESP

header provides encryption of the IPv6 packet payload, which addresses the threats concerning communications, privacy.

Mobile IPv6 creates a new class of messages called binding updates that confirm the identity of a device as it moves to a new location. Binding updates allows direct communication [22] but is unfortunately **slightly uncertain** (appendix H).

4.6 Quality of Service

This section discusses how QoS is expected to work when ready for use in IPv6. Internet traffic has not only increased, it has also changed in character. This has led to new application demands of the global Internet. Until now, IP has provided a “best-effort” service in which network resources are shared fairly.

Unless a decision about flow label specification is not taken, it seems there are no really benefits with using IPv6, than IPv4 to improve QoS mechanisms. Rename the field to "unspecified" is one opinion that we received from the mailing list at ipng@sunroof.eng.sun.com. When we have followed this discussion, it is obvious that there are different views of bringing a solution for quality of service. IPv6 provides same QoS as IPv4 today, with added advantages in the area of service differentiation. QoS is a combination of several issues, which are given from the two fields added to the IPv6 header. The fields are the **Traffic Class** and the **Flow Label**. IPv6 provides same QoS as IPv4 today, with added advantages in the area of service differentiation. These fields also make resource allocations available, which are defined as IntServ (appendix I.1) and DiffServ (appendix I.2).

Mobile users will have the benefit from having constant access to the Internet As no specification is ready for these fields we do not like saying that quality of service is a feature of IPv6, but everywhere we read it is. Probably the IETF will not stop developing these “reserved” fields until they fulfill the proposed benefits.

By enabling QoS it is possible to allow one user to get better service than another. QoS is for the ability of a network application to have some level of assurance that its traffic and service requirements can be satisfied. Packets can be set to different classes and let them have different priority.

- **Bandwidth** is needed, but it is not enough and any QoS assurances are only as good as the weakest link in the “chain” between sender and receiver. QoS does not create bandwidth. So, it is not possible for a network to give what it does not have.

- Services that can be done in the background such as file transfer and receiving mail does have its QoS of being transferred with **no error**.
- IP telephony is coming strong today and to this the bandwidth is not the big problem, **latency** is.
- To implement better support for real-time traffic (such as videoconference), which has high demands on **delays**, IPv6 includes a new field Flow Label in the specification. With Flow Label mechanism, routers can recognize to which end-to-end flow the packets belong. While standards for QoS exist for IPv4, real-time traffic support relies on the IPv4 Type of Service (TOS) field and the identification of the payload, typically using an UDP or TCP port. Unfortunately, the IPv4 TOS field has limited functionality and over time there were various local interpretations. In addition, payload identification, using a TCP and UDP port is not possible when the IPv4 packet payload is encrypted.

4.7 How other protocols are affected by IPv6

An interesting question to many companies, that starts to prepare for IPv6, is how IPv6 is going to influence their existing products.

Mobile IP is a proposed standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher-level protocols like TCP. IPv6 has the same support for upper layer as TCP and UDP as IPv4 has and will not be affected of a transition.

Today applications are practically nonexistent for IPv6 yet. But most applications will be easy to recompile to use 128-bit IPv6 addresses, but others might demand a bit more work. According to Sun Microsystems [28], the existing applications with IPv4 will not be affected when using the dual stack in the Solaris 8 Operating Environment.

4.8 Header Compression

The large header, which includes much information about the packets, is required to support a lot of functionality when routing through large networks of anonymous computers. The problem with wireless networks is that bandwidth is relatively limited, so every byte in the data stream must be used efficiently. A relatively small amount of data packets require a relatively large header to identify its contents, destination, sender, QoS parameters, and so on.

The last hop in a wireless network is the over-the-air interface. Servers in the Radio Access Network (RAN) know what data is being sent and knows exactly where to route it, so most of the header information is not required. Therefore is it possible to compress the IP header to improve the efficiency of the bandwidth [29].

Sun is actively engaged in efforts to address this problem through the IETF Robust Header Compression (ROHC) working group. Header compression will be defined by open standards so that every platform in the network can support those standards.

The saved bandwidth for computation due to header compression is a trade off which amounts must be paid for by compute-intensive compression or decompression of each packet's header. Each service may have different optimal header compression schemes and times, and the network has to support that. It may be that the header compression is best done at a gateway in the core network or in a server in the Radio Access Network (RAN). Open-standards, distributed-server computing model allow network operators to choose which node should be programmed to perform compression.

4.9 Affects of IPv6 in a longer perspective

As there is no compatibly between IPv6 and IPv4 without converting the addresses in some way, it will be quite a lot of work and investments during the transition period, to have them coexistence. This higher cost when introducing IPv6 will be compensated. Later on it will **save money** as the quantity that runs IPv6 will increase in time and finally take the leading position. In a long perspective the "life-holding" work of IPv4 will be much more expensive than the migration to IPv6.

5 Design impacts of IPv6

This chapter describes how the transition can be done. There are various strategies that will be possible when adopt IPv6. There are three main mechanisms that dominate the transition, **dual stack, tunnelling and translation,** and they works well together. Today, the network protocol used in the Internet is IPv4. IPv6 hosts in different locations need to communicate with each other over the existing IPv4 networks. The transition from IPv4 to IPv6 will be an evolutionary process rather than revolutionary, and IPv4 will be around for a long time.

How to plan the strategy for the transition varies. In some cases, entire networks could be upgraded to create small reservoirs of IPv6 support surrounded by oceans of IPv4. Alternatively, upgrading individual nodes to support both versions of IP, but there is no way getting around the fact that IPv6 is important to interoperate with.

Good news is that IPv6 creates no order dependencies. It is up to net architects to upgrade their hosts first and then the routers, or their routers first and then the hosts. It is even possible to upgrade some hosts, some routers and leave the rest alone.

5.1.1 Dual stack

There is no compatibly between IPv4 and IPv6, without modifications to let them coexist. Introducing IPv6, as a new protocol will be done gradually, mainly by introducing upgrades and new versions of existing operating systems with dual IP stacks. Dual stacks can therefore be used as a first step in a migration to IPv6 by deployment of systems that support IPv6.

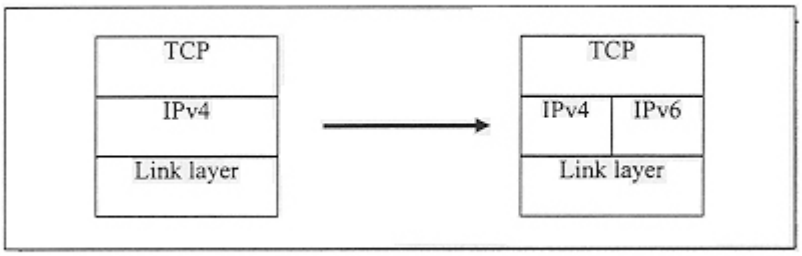

Figure 4: Dual Stack

A dual stack has both IPv4 and IPv6 protocols on the same system. This technique is providing complete support for both Internet protocols IPv4 and IPv6 in hosts and routers. A

host that support both of these protocols can communicate with an IPv4 node and an IPv6 node, and can identify packets as being IPv4 or IPv6. With a dual stack, existing IPv4 applications will continue to work seamlessly, and this is the main transition mechanism.

On the network side, the implementation of dual stacks in for an example GPRS, is vital to enable both IPv4 and IPv6 access. The edge routers in operator network should also be dual stack routers. Mobile terminals must use dual stacks in order to access both IPv4 and IPv6 services without translators in the network. This is the most straightforward procedure to satisfy the requirement of full intersystem compatibility and to include a complete IPv4 implementation to new IPv6 systems. This is what is called an IPv6/IPv4 node. When combined with protocol encapsulation, interaction of IPv6 applications will be possible between two IPv6/IPv4 nodes, even if the devices on the route have not yet been upgraded to IPv6. The dual stack approach does not necessarily imply that the system should contain two separate protocol implementations. It just should act as if it did. From the application point of view there are still two separate APIs and the true decision whether IPv4 or IPv6 is used is made on the application level.

5.1.2 Tunnelling

Tunneling enable IPssv6 packets to traverse IPv4 networks and vice versa.

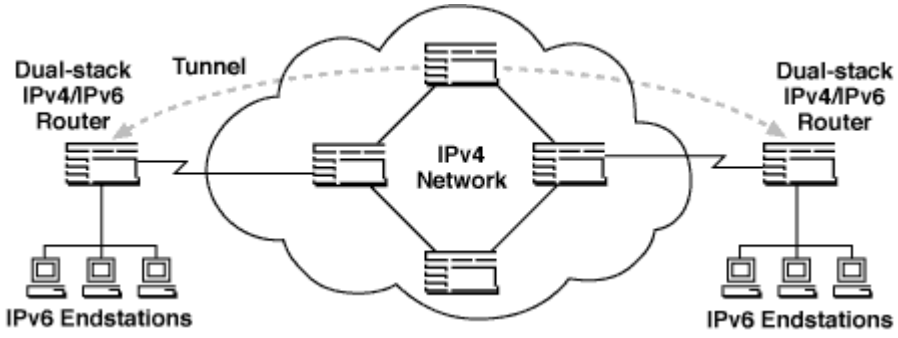

Figure 5: Tunneling

In the future the needs for IPv6 tunneling will decrease because it will be fewer IPv4-only clouds to traverse. IPv6 tends to be a more efficient protocol, so the performance degradation due to tunneling will be negligible. Tunnelling IPv6 over IPv4 is accomplished by encapsulating an IPv6 packet into the payload of an IPv4 packet. For a router to do the tunnelling, it must be upgraded to run IPv6.

Tunnelling of IPv4 packet can be done in different ways (appendix B.5).

5.1.3 Translation

Translation boxes are another approach for the transition. This method allows IPv6-only nodes to communicate with IPv4-only nodes through protocol translation. Except from IPv6 Fragment header the translator silently ignores all other IPv6 extension headers and IPv4 options. As there does not exist a semantic mapping between the IPv4 type-of-service and IPv6 traffic-class and flow-label fields the translator ignores even these.

The mechanism that includes these translations is included in separate translator boxes. Since, IPv4-to-IPv6 transition mechanisms still are under development it is suggested that more research are conducted for each network product to purchase to find out what each product manufacturer plans to support.

The drawback of translators is that they often cause breaks in end-to end services (end-to-end IP security), as happens with NAT in IPv4. They also introduce a single point of failure in the network. The use of translators must be carefully considered, and should be transparent from the terminals; otherwise they need to be updated accordingly. Translators allow IPv6-only nodes to communicate with IPv4-only nodes through protocol translation.

6 How Kipling is affected by IPv6

This section gives the result of the investigation of IPv6 in mobile Internet. The questions we got from Kipling about their transition and what consequences it has on their products, are based on the information found in previous chapters. In this section we set the focus on how Kipling is affected by these facts. For information about the status of the IP specification at this date the report is written, please see appendix D.

6.1 What are the driving forces for Kipling to transit to IPv6?

The Third Generation Partnership Project [12] (**3GPP**) is a cooperation of companies that works for producing technical specifications for Third Generation Mobile System. A decision has been taken by 3GPP to introduce IPv6 as one of the protocols of the future **3G** networks [8]. This decision may be the "killer-application" for IPv6 and will be the main driving force for companies involved with the future 3G networks, based on **UMTS**.

"Adoption for IPv6 by 3GPP is the first real business case and the biggest business case for IPv6"; says Latif Ladid, president of the IPv6 Forum, a consortium of 60 IT companies and research institutions. "IPv6 is practically what's needed for wireless applications because it provides true end-to-end security and true end-to-end voice over IP. 3GPP has provided the ice-breaking leadership that will pull the fixed networks to IPv6," Ladid adds [20].

6.1.1 The reason why mobile Internet is a driving force of IPv6

Mobile Internet in Europe and Japan is a big driving force for IPv6. The mobile Internet will use the majority of the IPv6 features, especially direct routing, "always-on" connections, security and quality of service, when introducing IPv6. The new protocol IPv6 enable all the IP-based services that are needed for the future wireless networks. The conclusion is that the mobile Internet has the major of the features of IPv6 in its networks. IPv6 enable all the IP-based services that have needs for the future wireless networks. We are now going to point out some of the needs that force an introducing IPv6these:

- **Wireless communications and Mobile IP.** The possibility to address the mobile devices uniquely and have always-on connection all through the world is a demand that comes further. New mobile services has also changed and requires that the Internet architecture has to evolve to accommodate new technologies as well as increasing

numbers of users, applications, and services. The demands of these products are a design of IPv6 that enable this. To meet the future with 3G networks for mobile phones it requires permanent global IP addresses for each device, and there is simply not enough address space in IPv4 to cover all the mobile terminals using the public Internet.

- The **telecom operators** that got a license to build the next generation mobile network based on the UMTS network force the transition, so they can fulfill their requirement and keep their promise, which is to have a complete UMTS network in Sweden at the end of 2003.
- **IP telephony** is a strong coming service and the SIP protocol has been developed to make telephony easier for both fixed and mobile data network to get through. SIP is a standard that should be used in the third generation mobile telephony, 3G (UMTS).
- **Real-time services** that requires better support for quality of service. Differentiation of priority and identifications of flows are some of the new needs for future services.

6.1.2 Why ought Kipling change from IPv4 to IPv6?

In a near future products will run pure IPv6 within the 3G telephones and to support this it must also be possible to have connections to IPv4 based networks. If Kipling has the goal to deliver products or giving support for the UMTS network, it will definitely be necessary to include IPv6 as one of the protocols in the near future. Therefore it is important for Kipling to change, or in other words, give support for both IPv4 and IPv6 to be an attractive software developer. It is no longer possible to force the problem further, if trying make profit by being among the first ones that deliver attractive services for applications to the 3G mobile network. To get the right timing of the support to IPv6 in their products or even better find out a killer-application for 3G, can give a leading role among competitors. That IPv4 is going to transit to IPv6 for mobile Internet is not longer a question, only a question of time.

Even if the goal is not to make purely, IPv6 products for the 3G networks, it is necessary to have knowledge about IPv6, as it has to coexist with IPv4 over a period of time. Products must have some strategies to make coexistence of both IPv4 and IPv6 in a first phase.

6.2 What are the greatest advantages of IPv6 that Kipling can make use of in their products?

The most obvious features that IPv6 adds is that it can provide support for products for the new generation of services such as IP telephony, mobile IP and push applications. **Push applications** assumes an **always-on connection**, which only is possible through IPv6. A benefit of this is that it is a tremendous moment to develop new products that fits to these new services. The push technique is a feature of being always connected, and the data is pushed directly to the mobile telephone from a content server.

When mobile IPv6, which is under development, is finished it will be possible to use direct routing. Mobile IPv6 route all traffic to the telephone without engagement to the home agent (appendix G).

6.2.1 Killer-application for 3G

When we did a small comparison between 3G and GPRS, and did not found any dramatically differences. The services are almost the same for both 3G- and GPRS telephones; indeed it will go a bit faster with 3G. The bandwidth that 3G are supposed to have is a theoretical value depending of where you send from and how heavy load the traffic is on the network. One difference that can give 3G a favor, except for the bandwidth, is that it can be built together with HiperLAN or other similar network technologies, which is a service that can be offered at airports for instance. GPRS has no support for this technical solution.

Products for the new generation mobile telephones such as IP telephony, mobile IP and push applications are aspects to be aware of, when trying to find out what products to develop in the future. We have mostly focused on what features the **push technique**, which assumes an always-on connection, can offer to products. These types of services are only available in use of IPv6. The push technique combined with the positioning or with HiperLAN is a strong alternative of future killer-application. A killer-application for 3G is what is needed to make it the alternative for users. If no real attractive products will be introduced there is nothing that says 3G are going to beat GPRS.

6.2.2 New products?

To provide automatically services based on their location are what we definitely think will be the killer-application. Probably, development of a new product, together with the existing positioning product Motion, will be attractive for users. Here we give some suggestions about

supposed products based on the benefit of the **always-on connections, push technique** and **location-based services**, enabled by IPv6.

- **Positioning** is still a candidate of killer-applications and modified with new services it can be an even stronger candidate. To get the real break-through of these products, the integrity aspects have to be solved to have the confidence solved in these applications. If it would be possible to be supervised of unauthorized persons it would not win anyone's trust.
- **Local information.** If this service is activated it could be possible to get information of current interest in the area. Every radio masts of an UMTS network that covers a town is intended to be a member of a multicast address. This service can be offered when passing the border to a town or maybe when it is a new date or new information. All depending of how important the messages is. Traffic warnings like accidents, queues and other traffic incidents included in this area, may have the priority to be sent more often, then for instance a message about happenings and events this day. With the push technique you get the latest news in this area and the current information in this area right in the phone. Preferable the message could be noticed in different ways depending on how you configure your telephone and if you do not want it, a possibility to turn it off. So, when driving the car it will maybe appear as a voice over IP. This is illustrated in figure 6.

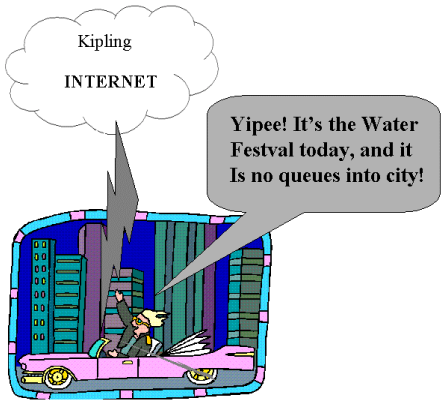

Figure 6: Killer-application with the push technique

- **Special directed advertisement.** Advertise all over a business chain and depending on which district you belong to, can be used to adapt advertise to fit the local stores. In this way some chains of food, radio and television shops even now distribute the advertise, so why not right into the mobile phones, which you probably have with you, and not a lot off advertise like papers or coupons at home?

To join this service it may be by an agreement to the store as a member, and the store registers the mobile telephone to a multicast address to get the messages. When the mobile telephone changes place to some other area the messages also will be different. Figure 7 illustrates the illusion of this.

Figure 7: Special directed reclaim

- **Occasional services**: Have the push service occasional as long as you need it. Call a number to see what services are available, easiest would be to have a distributed database to hold the updated information. As a member of something you are interesting of, you get the most resent information. Say, you are interested of something special for a short while, for instance a ticket for a travel, time tables, joining an advertisement site to get all the advertise in the telephone to see directly when something new appears, this could be an alternative and instead of searching the result by yourself the offer comes to you. Figure 8 illustrates how this message could appear.

Figure 8: Occasional service

6.2.3 Are there any disadvantages with a transition towards IPv6?

There is no compatibility between IPv6 only stations and IPv4 only stations without some converting, so different strategies for the transition have to be done. As stated earlier, the standards are still not stable. Many RFCs and Internet drafts have replaced each other for about a decade now, and it is easy to understand the confusion when starting to learn the IPv6 and mobile IPv6. In other ways it seems that IPv6 has so much to add to the Internet protocol that this can be overseen.

6.2.4 What can IPv6 offer in a security aspect?

As Kipling is not affected directly by the IP protocol, mostly by the addresses, we cannot see what security features IPv6 can add for their existing products. Security with embedded IPsec is added to the IPv6 protocol, but for mobile IPv6 this has turned up as a security hole in the security architecture (appendix H).

6.3 When should Kipling transit to be competitive towards their competitors?

When to transit is the big question, the computer communication is a fast changing environment and it is necessary to have updated information to get the right timing. The initiative of this bachelor's project is a good start of planning the transition to IPv6. Today Kipling is using IPv4 in all their products they are developing for Mobile Internet and they must know in advance when it is recommended making support for both IPv4 and IPv6 to have a leading role within the development of Mobile Internet products.

Today it is a hard work to get the standard of IPv6 so stable that it is worth starting building products from it. Ericsson hopes on a final standard in the end of this year, 2001. After having this final specification of IPv6 the implementation of products with IPv6 can take speed, and for companies that will compete in the mobile Internet with the 3G networks, it requires that the work of IPv6 start.

A transition to IPv6 may be just round the corner as the decision to use IPv6 as one of the protocols in the UMTS network is done. If the operators can hold their vision to build it in time, 31 December 2003 in Sweden, it is necessarily to start the planning of introducing IPv6 immediately. Indications give us the feeling that this time is not going to be satisfied.

Sun Microsystems Inc, is also actively involved in the process of setting standards for mobile IP. Greg Papadoulos, chief technology officer at Sun says in an article written Oct 23 2000 [20], "We are in the middle of a complete transition of our product line, and the core of

it is Solaris 8, which has IPv6 built in". He says further that, "IPv6 is not optional. Every piece of equipment we ship will come with IPv6 within nine moths".

The natural thing is to start upgrading the routers in the kernel of Internet. If the final standard for IPv6 is ready in the end of 2001, it supposed to be implemented at these routers in 2004. These routers must have a dual stack that supports both versions of IP.

It is important to have updated information of happenings within the UMTS network, to get the right timing for the transition and to be a good competitor. What we might expect for the coming transition is defined in a scale over ten years with start at this date, May 2001. Figure 9 gives our opinion of when the time is ready.

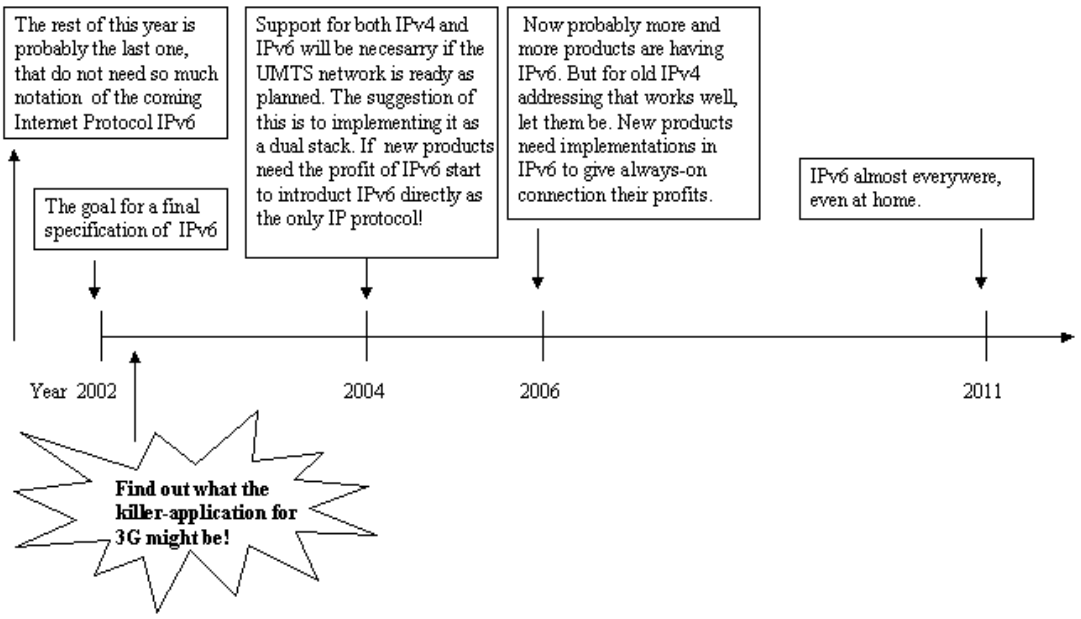

Figure 9: Transition strategy for Kipling

6.4 What strategy will be used at the transition?

Kiplings products are implemented in JAVA (Figure 10). Sun Microsystems, Inc, has announced plans to ship an IPv6-compliant version of Java in fall 2001, with beta software due next spring. The coming version JVM for**,** Solaris 8 has an integrated, dual IPv4 and IPv6 stack. IPv4 is the default Internet Protocol in the operating system upon installation of

Solaris 8. To get IPv6 you must enable it during the installation process. Solaris 8 software cannot be configured as an IPv6-only node. It can, however, be configured as an IPv4-only node or as a dual stack. When the work of the transition is done at lower level in the stack it is already mandated how to be treated when coming up to the application level. With a dual stack that Solaris 8 offers, the JVM will handle the rest. With support to dual stack in the JVM, no big changes are needed to the existing code. There are different transition mechanisms available. Dual stack is one alternative, which allows running both IPv4 and IPv6 on the same machine. Our proposal strategy for Kipling is to do their transition to IPv6 with the dual stack, included in the Sun Solaris 8.

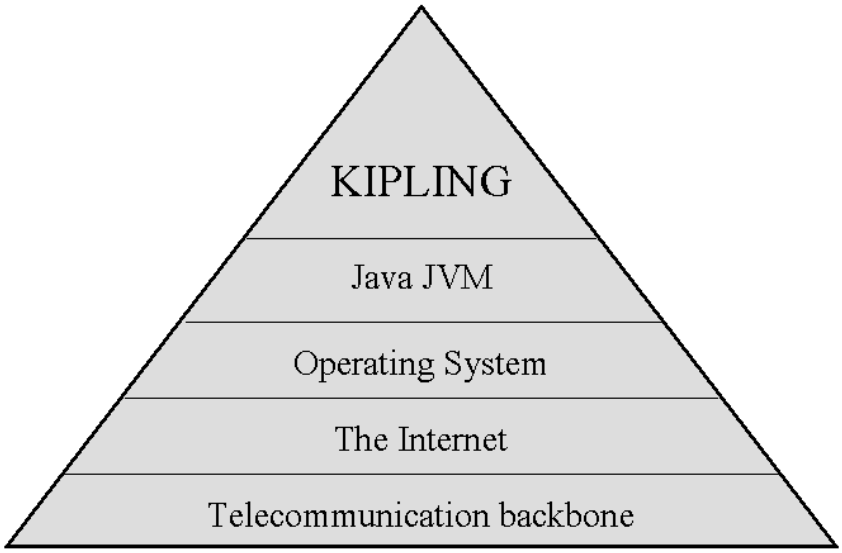

Figure 10: Hierarchy of levels concerned by Kipling's products

6.4.1 What are the consequences for Kipling and their products?

An effect of 3GPP decision, to introduce IPv6 as one of the protocol in the future 3G networks, is that it naturally influencing the actors on this market. Therefore Kipling will also be affected. Probably the 3G telephones will be implemented with pure IPv6 from the beginning. The consequence is that Kipling has to give support for these telephones by introducing support for IPv6. If Kipling solves this by introducing a dual stack, there are no consequences for their products. Since, Kipling's products not directly works at the IP level, they are not involved to all different services that have support in the new protocol, IPv6, which also makes the consequences limited to the addressing.

6.4.2 Is a transition leading to great changes?

The most obviously change is to get support for IPv6. The products must be able to handle the new format of the addresses. If Kipling's products works on an operating system (OS) that supports dual stack, the products will work transparently to the applications and no changes are needed. In a near future, several OS will give support for dual stack.

6.4.3 Do the products need to run both versions at the same time, or just change everything over a night?

It is not realistic to think that Internet will be "shut down" and then to be restarted with the new protocol. It will probably be a gradually transition where some run IPv4 and other run IPv6. When developing new products it will be a proper time to do an upgrade to IPv6.

7 Approach

In this section we will describe the specification of the task. We will also tell about how the work was done, and the experience it gave us.

7.1 Specification of the task

The task was to do a technical investigation in mobile Internet, with a focus on IPv6. After half the time the work should be presented at Kipling, to let them know what we had found out so far. When we have finished the entire project we will give another presentation at Kipling to give them our conclusions. The task was split into three different phases (appendix J).

7.2 How the work was done

First, we made up a project plan over the entire work. That plan was so detailed that we almost had every hour of the project documented.

Every phase started with collecting material. This collecting phase did not only consist of collecting; it was a mixture of collecting, reading and writing.

We created the structure of this report and inserted the headlines. Below these headlines it was just to fill in the information that we got. In the writing phase we formulated the text.

After the structure was done, we started to read several books, but soon we recognize that there were contradictions between them. For an example the fields in the IPv6 header did have different names and the fields did not even have the same length. We were forced to go to the specification for IPv6 [5] to get the right answer. After that we concentrated on more resent RFC’s and Internet Drafts, because it is from those documents the standard will be set.

To get a notice how the discussion of the not yet specified fields in the header of IPv6 was going, we joined a mailing list, ipng@sunroof.eng.sun.com.

Our conclusions are made from information that we have read in books, RFC's, reports on the Internet and other daily updated information. We also got some information from software developer by interviews and contacts. Some questions were sent to telephone operators in Sweden to get their opinion about IPv6. Europolitan was the only telephone operator that gave us some answers. Tele2 answered that the information we were asking for was too

sensible to give answers to. Telia did not even reply. These questions did not give us any new information and are therefore not used in the report.

In the learning phase about Kipling's products we found out that it was a minimal amount of documentation on the right level of their products. To help us to learn about Kipling's products we have had the benefit of having access to product developers at a workshop. The result of the workshop did unfortunately not give what we had expected. To get a real understanding of Kipling's products, we should have had knowledge about the GSM network.

7.3 Experiences of the bachelors project

When we have done this investigation about IPv6 it is easy to understand why IPv6 has taken so long time to become accepted. It is confusing reading and contradictions everywhere. New Internet Drafts are replacing each other like an assemble line, where some are developed to a RFC, some as standards and others become nothing at all. Reports, books and article are often based on not recently updated information.

That no stable standard is ready, not even after ten years of developing, is a big drawback for IPv6. Because IPv6 inconsistently it is easy to understand why it does not have had the high priority and why most companies has been waiting for a final standard. Why spend a lot of work and money on something that already works fine and cannot offer some real visible features to their products immediately? There are several experiences that we have made during this project:

- You should not believe everything that you read. The information can be old or the author maybe misunderstood the information that he/she got. The best thing to do is to read information from different sources to make confirmation to what you have read.
- This project gave us also a deeper knowledge about how the IP protocol works and the need for a new protocol.
- Since IPv6 is not a final standard, and all the detailed information about the new protocol is to be found on the IETF's home page, it also gave us knowledge of how IETF works when they are developing a new standard.
- The Bachelor's project made us understand the importance of making a projectplan, with breakpoints. It is very easy to get on to a sidetrack and therefore miss the target.
- Documentation with references is another thing that is important during the project.

It has been a challenge for us to write the report in English, when having no experience of it before.

7.3.1 Problems

Without the knowledge about how the GSM is working it was hard to understand Kipling's products in a deeper technical way. We had a workshop to learn about Kipling's products, this gave us a chance to ask questions and have an insight in how they use IP. At this workshop it had been useful to have knowledge about how the GSM network to get the real understanding of the discussion. Many new words, which did not have the same terms in mobile IPv6, made it difficult for us to follow the discussion.

IPv6 has been under development for about 10 years now. Since, the standards for IPv6 are not yet ready, it has aggravated our work.

The daily coming problem have been that we did not get an own workstation at Kipling as promised. Time had been waste of sitting two persons in front of one computer. In the beginning, when we still had the hope of getting one computer for each person, time was wasted for travelling to the university or home to have an own computer.

Probably the projects had to high ambitions on this short time to give any deeper analyze. A basic knowledge about how the mobile IP and the GSM net works would have been a requirement. Also to have documentations of Kiplings products available at right level have had been valuable.

7.3.2 For further studies

Since the standard for IPv6 are not ready, we suggest that Kipling should keep in touch with the IETF home page, to be up-to-date with the further development of IPv6. Also to follow the 3GPPs discussions, were Kipling is one of the members, can be very useful.

References

[1] Tanenbaum, Andrew S, *Computer Networks, 3:rd Ed*, Prentice-Hall, 1996

[2] Postel. J, *Internet Protocol - DARPA Internet Program Protocol Specification*, USC/Information Sciences Institute, 1981, RFC 791

[3] Loshin, Pete, *Ipv6 Clearly Explained*, Morgan Kaufmann Publisher Inc, 1999

[4] Hinden. R, Deering. S, *IP Version 6 Addressing Architecture*, RFC 2373, July 1998

[5] Deering. S, Hinden. R, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 2460, December 1998.

[6] Hinden. R, Deering. S, "IP Version 6 Addressing Architecture", INTERNET-DRAFT, March 2 2001

[7] Conta. A, Deering. S, *Internet Control Message Protocol for IPv6*, RFC 2463, December 1998.

[8] Internet.com, *3G IndustryGroupSupportsIPv6*, http://www.allnetdevices.com/news/0005/000526ipv6.htm, May 26, 2000

[9] David B. Johnson, Charles Perkins, "Mobility Support in IPv6", http://www.ietf.org/internet-drafts/draft-ietf-mobileip-ipv6-13.txt 17 November 2000

[10] Kent.S, "Security Architecture for the Internet Protocol", RFC2401, 1998

[11] IETF Secretariat, *IETF Home Page*, http://www.ietf.org/, Mars 2001

[12] *3GPP*, http://www.3gpp.org, April 2001

[13] Deering. S, *IPv6: Why, What, When, How?*, http://www.cisco.com/warp/public/732/ipv6/cisco_ipv6_talk_public.pdf, April 2001

[14] Kivisaari. Sami, *A comparison Between Mobile IPv4 and Mobile IPv6*, http://www.niksula.cs.hut.fi/~skivisaa/iwork/internetworking_seminar.html#chap1.1, 2 April 2001

[15] Stardust.com, Inc., *White Paper –Introduction to QoS Policies*, http://www.qosforum.com/white-papers/qospol_v11.pdf , April 2001

[16] Sun Microsystems, Inc, *Solaris IPv6*, http://www.sun.com/software/solaris/ipv6/faqs.html#15, May 2001

[17] Duffy Marsan, Carolyn, *Mobile security flaw delivers yet another blow to IPv6*, http://www.nwfusion.com/news/2001/0402mobileip.html, April 2001

[18] Loshin Pete, *America's Dangerous Apathy For (Yawn) Ipv6* http://www.ispworld.com/src/Ipv6.htm 30 April 2001

[19] Castelli, Florence 3gpp-ipv6 http://www.etsi.org/press/3gpp-ipv6.htm 8 May 2001

[20] Duffy Marsan, Carolyn, *Wireless boosting IPv6*, http://www.nwfusion.com/news/2000/1023ipv6.html 13 February 2001

[21] Sun Microsystems, Inc, *Enabling The Wireless Net Effect*, http://www.sun.com/sp/supplements/wireless_whitepaper.pdf, May 2001

[22] *IPv6 and Multimedia*, http://www.6init.org/public/ibc_mm03.pdf, May 2001

[23] Perkins C, *IP Mobility Support*, http://www.ietf.org/rfc/rfc2002.txt, 17 May 2001

[24] Wegner J D, Rockell Robert, *IP Addressing and Subnetting including IPv6*, Syngress, 2000

[25] Narten T, Nordmark E, Simson W, *Neighbor discovery for IP Version 6 (IPv6)*, http://www.ietf.org/rfc/rfc2461.txt, 18 May 2001

[26] Thomson S, Narten T, *Stateless Address Autoconfiguration*, http://www.ietf.org/rfc/rfc2462.txt, 18 May 2001

[27] *6bone Home Page*, http://www.6bone.net/, May 2001

[28] Sun Microsystems, *Solaris Ipv6*, http://www.sun.com/software/solaris/ipv6/faqs.html#15, 17 May 2001

[29] Degermark. M, Nordgren. B, Pink. S, *IP Header Compression*, http://www.ietf.org/rfc/rfc2507.txt, 21 May 2001

[30] Nokia, IPv6- *Enabling the Mobile Internet*, *White Paper*, http://www.nokia.com, April 2001

[31] Loshin. Pete, *IPv6 over everything*, http://www.data.com/issue/991021/ipv6.html, 15 mars 2001

[32] Randall. Neal, *Linux 2.2 Gives NT a Run for its Money – for Free*, http://linux.dbw.org/articles/linux22vsNT.html, 10 May 2001

Abbreviations

3G	Third Generation
3GPP	Third Generation Partnership Project
ARP	Address Resolution Protocol
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
CIDR	Classless Inter Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control and Message Protocol
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IHL	Internet Header Length
IP	Internet Protocol
IPng	Internet Protocol Next Generation
IPsec	Secure Internet Protocol
IPX	Internetwork Packet Exchange
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
JVM	Java Virtual Machine
LAN	Local Area Network
MAC	Medium Access Control
MIG	Mobile Internet Gateway (MOTION Mobile Location System)
MTU	Maximum Transmission Unit
NAT	Network Address Translator
NIC	Network Information Center
NSAP	Network Service Access Point
OSI	Open System Interconnection
PING	Packet Internet Grouper
RFC	Request For Comments
SIM	Subscriber Identity Module (SIM-card)
SIP	Session Initiation Protocol
SMS	Short Message Service
TCP	Transmission Control Protocol
TOS	Type of Service
TTL	Time To Live
TWG	Trinity WAP Gateway
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLSM	Variable Length Subnet Mask
WAP	Wireless Application Protocol

APPENDIX

A Internet

The Internet, a network that was born in 1969 as the Advanced Research Projects Agency Network (ARPAnet), from the beginning sponsored with U.S. Governments grants. As the Internet made the transition from a government sponsored to a commercially driven communications environment, the users connected to the ARPAnet grew rapidly, almost exponential.

The glue that holds the Internet together is the TCP/IP reference model and TCP/IP protocol stack. TCP/IP became the only official protocol on Jan.1, 1983. The current version of IP, known as Version 4 or IPv4, has not been substantially changed since RFC 791 [2] was published in 1981.

A.1 Options in IPv4

Table 1 describes the options in IPv4

Option	**Description**
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Table 1: IPv4 options

B Internet Protocol Next Generation (IPng)

Sometimes Internet Protocol version 6 is called IP Next Generation (IPng), but they are not the same. IPng is not a special protocol, just a name for the successor of the new revised IP. IPv6 was the one that was chosen in the competition between the proposals made as probably successors to IPv4. Proposals of the IPng

TUBA, TCP and UDP with bigger Addresses were some of the suggestions. Other possibilities to solve the address space problem were CATNIP and SIPP. SIPP was a result of several groups that worked together, but SIPP didn't have any good solution for the transition or acceptable mechanism for auto configuration. But with some modifications, was the specification recommended to and accepted by IESGs as the basis of IPng.

B.1 Prefix for addressing with IPv6 addresses

Prefix Format (PF) allocation

PF = 0000 0000 : Reserved

PF = 0000 001 : Reserved for OSI NSAP allocation

PF = 0000 010 : Reserved for IPX allocation

PF = 001 : Aggregatable Global Unicast Address

PF = 1111 1110 10 : Link Local Use Addresses

PF = 1111 1110 11 : Site Local Use Addresses

PF = 1111 1111 : Multicast Addresses

Other values are currently unassigned (approx. 7/8th of total) [13]

All addresses starting with 80 zeros (80bits) is reserved for IPv4 addresses to be backward compatible. These are included in larger block where every address starting with eight zeros is reserved. An address that starts with 010 is to be distributed so it is possible to se who has distributed the address. The five following bits shows exactly which company who gave it. The addresses that starts with 100 are imagine having a geographical committed, similar as CIDR. Another addressing type is the unspecified address, or the all-zero address. This type of address is used when there is no valid address. An example when this occurs is when a host boots from the network first starts up and has not yet been assigned an IPv6 address. It might

use this address to the source field of the IPv6 header when sending out a request for configuration information.

B.2 IPv6 addresses and autoconfiguration

An IPv6 address enables autoconfiguration of different type of addresses for host interfaces [30]. An aggregatable global unicast address is the default IPv6 address type.

Globally	**On-site**	**Broadcast**	**Mobility**
Global unicast address	Link local address	Multicast group address	Home address
	Site local address	Anycast address	Care-of address

Table 2: IPv6 addressing type

B.3 Extension headers for IPv6

RFC 2460 [5] recommends that the extension headers be placed in the IPv6 packet in a particular order:

- **Hop-by-Hop Options** header must always appear just after the IPv6 header. It contains optional data that every node on the packet's path must examine. It is the only header that every router looks at.
- **Destination Options**, this header contains options that must be processed by the final destination node only.
- **Routing header** indicates that the packet has to visit specific nodes on its route.
- **Fragment header** is some different than its predecessor. Fragmentations of IPv6 packets are only possible for the source node. If a packet is too large for the path MTU between the source and the destination, an ICMPv6 packet arrives and indicates this. An advantage of this is that the routers do not have to handle with fragmentation any more.
- **Authentication header is** used to ensure data integrity.
- **Encapsulating header** is used to ensure data confidentiality and data integrity.
- **Destination Options header** carries optional information that need to be examined only by a packet's destination node(s).
- **Upper Layer Protocol header**, which can be the transport layers.

B.4 IP Version 6 Addressing Architecture

IP Version 6 Addressing Architecture is defined in RFC 2373 [4].

Unicast. This is an identifier for a single interface. For unicast the address is divided in a network part and a host part. The prefix number (appendix B.1) shows the length of the network part of the address. There are several forms of unicast address assignments in IPv6, including the global provider based unicast address, the geographic based unicast address, the NSAP address, the IPX hierarchical address, the site-local-use address, the link-local-use address, and the IPv4-capable host address. Link local addresses are guaranteed to be unique within the link in which they are formed, they are used for communicating with neighbor machines and are not routed to foreign networks. Site local addresses are unique within a given site whereas global addresses are globally unique. For further information, see [4] and [6]. A packet sent to a unicast address is delivered to the interface identified by that address (one-to-one).

The loop back address is used to let packets pass down through the protocol stack to the network interface. This is useful for testing software as well as configurations, but never to be transmitted on the network link. In IPv4 the loop back address is defined as 127.0.0.1. The IPv6 loop back address is all zeros, except for the lowest-order bit. The address is represented as 0:0:0:0:0:0:0:1, or just as ::1.

Multicast. Another possible way to send is as a multicast (one- to- many). A multicast address identifies a group of interfaces and the addresses must be used as destination addresses. No datagram should ever be originated with a multicast address as its source. Nodes that wants to subscribe to a multicast address announces that it wants to be a member, and any local routers will subscribe on behalf of that node.

IPv4 is already using multicast for applications that requires a high bandwidth to send the same data to multiple nodes, such as video conferencing or distribution of financial news. The first octet in the address identifies the address as a multicast address. All nodes that are member of a multicast address expect to receive all packets sent to that address. It is possible for a node to belong to any number of multicast groups. Non-permanently-assigned multicast addresses are meaningful only within a given scope. There are also pre-defined well-known multicast addresses. They are used for; All Nodes Addresses, All Routers Addresses, DHCP Server/relay-Agent, and Solicited-Node Address.

Anycast. The third way of addressing is as an anycast. Multiple nodes may be sharing the anycast address, like a multicast address, but with anycast only one of those nodes can expect to receive a datagram sent to an anycast address. The difference between multicast and anycast is in the transmission process. A packet sent to an anycast address is delivered to one of the interfaces identified by that address (the "nearest" one, according to the routing protocols' measure of distance). An anycast address may only be assigned to an IPv6 router. Anycast addresses are allocated from the unicast address space, using any of the defined unicast address formats.

B.5 Different ways of tunnelling packets through different networks

IPv4-compatible IPv6 addresses

Automatic tunnelling of IPv6 over IPv4 is a mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks. In automatic tunnelling, the encapsulation is done automatically in the encapsulating router/host, and the tunnel endpoint IPv4 address is included in the packet's IPv6 destination address. An example of such a tunnelling mechanism is '6to4' tunnelling.

This method is built on "Reserved space for old addresses" as it makes it possible for an IPv6 address format to employ embedded IPv4 addresses. There are two types of special addresses that IPv6 provides that embed addresses. In both these cases the beginning starts with 80 high order bits set to zero; the 32 low order bits contain the IPv4 address. In the middle of these there are 16 bits, that when set to zero (0000), indicates that the address is called an IPv4 compatible address. This type of address is for use when two IPv6 devices need to communicate via an IPv4 routing infrastructure. This process is called automatic tunneling.

IPv4 mapped IPv6 address

The other case is when the 16 bits in the middle are set to ones (FFFF). This type of address is called an IPv4 mapped IPv6 address. It is used when an IPv6 host would use an IPv4 mapped IPv6 address to communicate with other hosts, which only supports IPv4. Some think that an IPv6 address format that employs embedded IPv4 addresses will be most common for enterprise routers and switches.

B.6 Experimental network for IPv6

IETF has taken the initiative to establish a Wide Area experimental IPv6 network infrastructure, termed “6bone”, where the word "6bone" stands for "IPv6 backbone".

The 6bone is an IPv6 testbed set-up to assist in the evolution and deployment of IPv6 in the Internet. The 6bone is a virtual network layered on top of portions of the physical IPv4-based Internet to support routing of IPv6 packets, as that functionality has not yet been integrated into many production routers; the network is composed of islands that can directly support IPv6 packets, linked by virtual point-to-point links called “tunnels”; The tunnel endpoints are typically workstation-class machines having operating system support for IPv6.

Registry, maps and other information may be found on the 6-bone link [27]. The 6bone is an experimental worldwide network for testing interconnectivity of IPv6 implementations, checking if IPv6 really works well or not in actual situations, and so forth. To achieve 6bone connectivity, it is necessary to use unique 6bone addresses. The world 6bone is made up by several regional 6bones. Pete Loshin who is involved in the development of IPv6 says [18], that in America the experimental 6bones mostly has been used for router updates and pings. The lack of enthusiasm for using IPv6 has generated a general lack of enthusiasm throughout the networking and computing industries. Although it is possible to use IPv6 support in Linux, BSDI and other OS, and in routers from Nortel, as well as Ericsson/Telebit, customers in North America has not yet been interested. The key is the application; there is none. Some IPv6 enabled applications are available but common IPv4 can handle that just as well. Early implementers could apply for 6bone addresses, but no registries are yet assigning real IPv6 addresses.

B.7 ICMP messages

Common problems that the router reports are:

- Destination Unreachable, for this error messages there are five different codes.
- Packet Too Big, the error message includes a field containing the value of the MTU of the link that causes the problem.
- Time Exceeded, when the hop limit of an IP packet is one and will be decremented to zero, the router must discard the packet and send Time Exceeded in an ICMPv6 message. This procedure is also useful to find out trace routes. When incrementing the hop limit one by one it is possible to identify all routers along the path that a packet takes between source and destination.

- Parameter Problem is used when there is problem with some part of the IPv6 header or some extension header.

Echo Request. When a node receives an echo request it respond with sending an echo reply. Echo Reply must contain the same request identifier, sequence number and data that were contained in the original request message.

C Temporary solutions of the address space shortage

In the 1970s, the architects of the Internet envisioned an internetwork with dozens of networks and hundred of nodes. They developed a design where any node on the internetwork was reachable by any other node. On the Internet today, there are tens of thousands of networks and millions of nodes. Unfortunately, the original design has not scaled well. The increased number of networks joining the Internet has strained router technology, and the sheer number of participants has strained the limits of IP addressing as it was originally designed. Some compromises had to be made to allow the Internet to continue its growth. Several strategies have been developed and implemented to help the Internet community cope with its growing pains. They help reduce the load on the Internet routers and help us use globally unique IP addresses more efficiently. These strategies are explained in [24]:

- CIDR
- VLSM
- NAT

C.1 CIDR

CIDR (Classless Inter Domain Routing) is an addressing consolidation and routing plan for the Internet, which reduces the pressure on the Internet's core and provides a more efficient allocation of IP addresses than the old Class A, B, and C address scheme can do.

CIDR provides for:

Hierarchically allocating IP address assignment by delegating control of segments of the IP address space to the various network service providers.

Hierarchically routing aggregation to minimize route table entries.

Implementing CIDR assumes the use of VLSM, routing technology for interior (intranet) routing, and CIDR-capable routing technology for exterior routing. Organizations that operate as Internet Service Provider (ISP) are expected to be able to support VLSM- and CIDR-capable routing protocols. A CIDR IP address looks like a normal IP address except that it ends with a slash followed by a number. This is called the IP prefix. An IP prefix consists of an IP address and a mask length. The mask length specifies the number of leftmost contiguous significant bits in the corresponding IP address. The mask length also indicates how many addresses the CIDR address covers. The lower prefix number, the more addresses it covers.

For example, consider CIDR address 200.25.0.0/16; the /16 indicates that the first 16 bits identifies the unique network number that in turn indicates the size of the address space. This allows a single routing table entry to specify how to route traffic to many individual networks addresses. Without the rapid deployment of CIDR in 1994 and 1995, the Internet routing tables would have to manage 70,000 routes (instead of the current 30,000+) and the Internet would probably not be functioning today! It is a temporary solution that improves the efficiency of network address allocation; it does not do anything to increase the total number of host addresses possible under IPv4 and should be considered purely a short-term tool rather than a long-term solution. A negative aspect to CIDR is that with an arbitrary address, we cannot determine the network and host numbers unless we know the network mask. Even though CIDR has extended the lifetime for IPv4 because it buys us some more years, the effort to manage the routing will continue to increase. There is no question that an IPv6 is needed, but only a question of when.

C.2 Variable Length Subnet Masks (VLSM)

CIDR and VLSM is essentially the same thing since they both allow a portion of the IP address space to be recursively divided into subsequently smaller pieces. The difference is that with VLSM, the recursion is performed on the address space previously assigned to an organization and is invisible to the global Internet. CIDR, on the other hand, permits the recursive allocation of an address block by an Internet Registry to a high-level ISP, to a mid-level ISP, to a low-level ISP, and finally to a private organization's network.

Just like CIDR, the successful deployment of VLSM has three prerequisites:

- The routing protocols must carry network-prefix information with each route advertisement.
- All routers must implement a consistent forwarding algorithm based on the "longest match."
- For route aggregation to occur, addresses must be assigned so that they are topologically significant.

C.3 NAT

NAT (Network Address Translator) translates addresses from one IP network to another; it allows network administrators to use a set of reserved addresses that never meant to be routed in the public Internet. NAT promote reuse of the private address space, they do not support standards-based network layer security or the correct mapping of all higher layer protocols and can create problems when connecting two organizations that use the private address space. It breaks end-to-end networking, and shifts control of the datagram away from the endpoints and into the network, that disables something that experts see as a requirement for security. On the positive side is that NAT in that way can hide entire networks behind a single IP address. NAT may be appropriate in some organizations, particularly if full connectivity with the outside world is not desired. But for enterprises that require robust interaction with the Internet, NAT devices are not always desirable. The technique of substituting address fields in each and every packet that leaves and enters the enterprise is very demanding, and can lead to a bottleneck between the enterprise and the Internet. NAT works well enough for Web and e-mail transmissions, they do not work well with newer network applications, like VoIP, IPsec, and real-time video and audio. QoS also becomes a big issue because NAT adds a process burden.

D IPv6 specification status

The current Request for Comments (RFC) and Internet Drafts that this report is based on, written in May 2001.

Number	Description	Status	Author	Date
2460	Internet Protocol, Version 6 (IPv6) Specification	Standards Track	S. Deering, R. Hinden	December 1998
2002	IPv4 Mobility Support	Standards Track	C.E.Perkins IETF	October 1996
	Mobility Support in IPv6	INTERNET-DRAFT	David B. Johnson, Charles Perkins	November 2000
2373	IP Version 6 Addressing Architecture	Standards Track	R. Hinden, S. Deering	July 1998
	IP Version 6 Addressing Architecture	INTERNET-DRAFT	R. Hinden, S. Deering	March 2 2001
2401	Security Architecture for the Internet Protocol	Standards Track	S. Kent R. Atkinson	November 1998
2463	Internet Control Message Protocol for IPv6			December 1998

Table 3: Table of specifications of IPv6

E Differences between IPv4 and IPv6

This table gives an overview of differences between IPv4 and IPv6.

IP Service	IPv4 Solution	IPv6 Solution
IP header	Variable header length, from 5 to 15 bytes.	The header has a fix size and fewer fields, which affects the performance at the routers. The length of the IPv6 header without extension headers is 40 bytes.
Addressing range	Addresses are 32-bits, that theoretical give about 4 billion addresses but in practice only a few billions.	Addresses are 128 bits long and can give $3.4x10^{38}$ bits possible combinations. Hierarchical routing makes the routes more effective and limits the size of the routing tables.
Autoconfiguration	DHCP servers are required to get the configuration.	Mobile devices are able to get their own addresses. Both stateless and stateful configuration is possible.
Security	IPsec	Embedded security, IPsec
Mobility	Mobile IP	Mobile IP with direct routing
Quality of Service	Differentiated Service (DiffServ), Integrated Service (IntServ)	Differentiated Service, DiffServ, Integrated Service, IntServ. Flow Label can identify different flows between source and destination. Special handling of packets will be possible with use of the Traffic class

Table 4: Differences between IPv4 and IPv6

F Mobile IPv4

In Mobile IPv4 a mobile node can move from network to network and still be reachable at the same address. That can be done because the mobile node can have two different addresses, a home address and a care-of address.

The home address is an address assigned for an extended period of time by the home agent of its home network. When a mobile node receives an Agent Advertisement [23] it determines if it is on its home network or a foreign network. If it is on its home network, it operates without mobility services. If the mobile node detects that it has moved to a foreign network, it obtains a care-of address on the foreign network. This temporary address could be a foreign agent care-of address that is shared in between several visited mobile terminals or be a unique co-located care-of address. The mobile node registers its new care-of address with its home agent through exchange of a Registration Request and Registration Reply message with it, probably via a foreign agent. Datagram sent to the mobile node's home address are intercepted and tunneled by the home agent to the mobile node's care-of address. When the packet arrives at the care-of address, the reverse transformation is applied so that the packet once again appears to have the mobile node's home address as the destination IP address (Figure 11, [14]). TCP or UDP will process a packet that arrives to the mobile node properly. Higher-level protocol logically receives it from the mobile node's IP processing layer.

When the mobile node sends a datagram, it is generally delivered to the destination using standard IP routing mechanisms. It does not necessarily pass through the home agent. Whenever the mobile node moves, it registers its new care-of address with its home agent. The mobile IPv4 protocol specification is described in RFC 2002 [23].

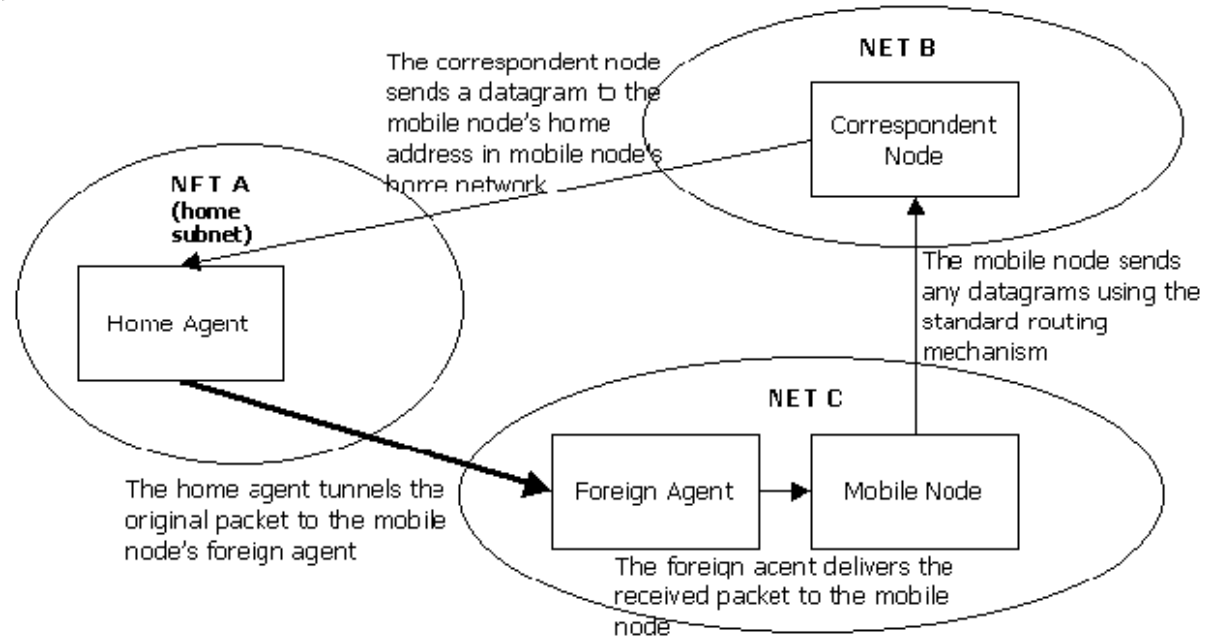

Figure 11: Mobile IPv4 routing.

G Mobile IPv6

Mobile IPv6 shares many features with Mobile IPv4, but the protocol is now fully integrated into IP and provides many improvements over Mobile IPv4. Route Optimization is now integrated in the protocol rather than as an option. This integration allows direct routing from any correspondent node to any mobile node, without needing to pass through the mobile node's home network and be forwarded by its home agent (Figure 12, [14]).

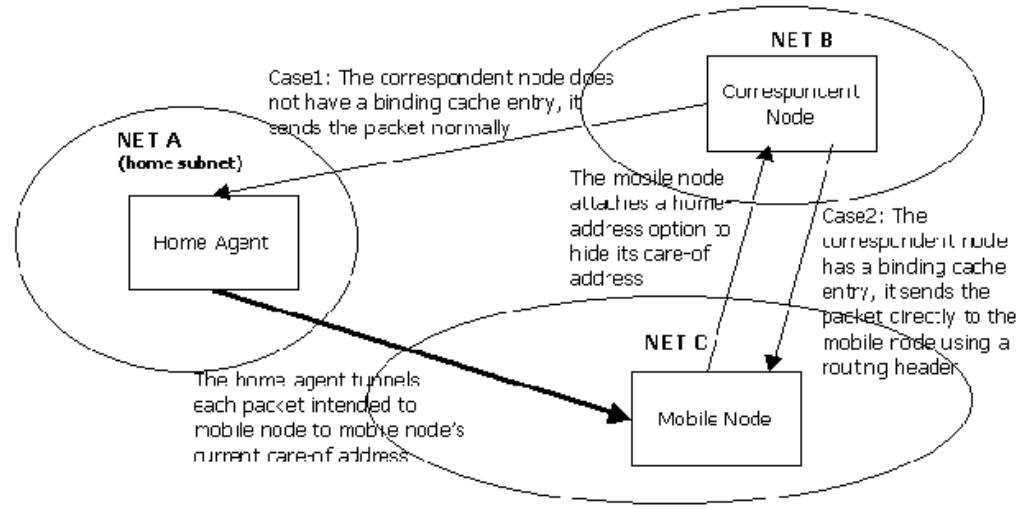

Figure 12: Mobile IPv6 data delivery.

The home agent and the correspondent node are informed of the care-of address each time the mobile node changes location. For packets sent by a mobile node while away from home, the care-of address is typically used as the source address in the IPv6 header of the packet. By including a home address option in the packet, the correspondent node receiving the packet is able to substitute the node's home address for this care-of address when processing the packet. Therefore, IPv6 packets that are addressed to the mobile node are transparently routed to the node's care-of address. The use of care-of address as the Source Address in each packet's IP header also simplifies routing of multicast packets to its home agent in order to transparently use its home address as the source of the multicast packets. There is no longer a need to deploy special routers as foreign agents as are used in Mobile IPv4. In Mobile IPv6,

mobile nodes make use of IPv6 features, such as Neighbor Discovery [25] and Address Autoconfiguration [26], to operate in any location away from the home network without any special support required from its local router. Unlike Mobile IPv4, Mobile IPv6 utilizes IP Security (IPsec) for all security requirements (sender authentication, data integrity protection, and replay protection) for Binding Updates (which serve the role of both registration and Route Optimization in Mobile IPv4). The optimized route between the correspondent node and care-of address results in more effective usage of the network. The integrated IP layer mobility enabled by the Mobile IPv6 protocol will offer crucial advantages, especially as the number of mobile terminals continues to grow. Although a similar mobile protocol exists in the IPv4 world, there is one fundamental difference; mobile IPv4 cannot cope with a large number of terminals. Mobile IPv4 relies on its own security mechanisms for these functions. The mobile IPv6 protocol specification is described in draft-ietf-mobileip-ipv6-13.txt [9].

H Mobile IPv6 security

A binding update is a shortcut designed to speed up wireless communications that use IPv6. Once the binding update is authenticated, communications go straight to the new location without passing through the home address. Originally, the Mobile IP working group planned to use the existing protocol IP Security (IPSec) to secure binding update messages. But the IETF's security experts recently announced that IPsec would not work for these messages for two reasons [17]:

- IPSec depends on a public-key infrastructure that has not yet been deployed.
- The key management component of IPsec requires heavy processing by end devices.

Because of these findings, the IETF leadership asked the Mobile IP working group to find an alternative approach for securing binding updates. As late as 2 April 2001, an article in Network World discussed the security, with the headline, Mobile security flaw delivers yet another blow to IPv6 [17]. “IPv6 has suffered another setback”, Carolyn Duffy Marsan writes. She continues that, “Security experts punched holes in their planned strategy for supporting mobile communications. The discovery of security flaws in the proposed Mobile IPv6 protocol means the IETF will have to develop a new method for authenticating roaming devices that use IPv6 addresses. This development means delays of months for Mobile IPv6, which was conceived a decade ago and thought to be in its final form.”

The problems with Mobile IPv6 are frustrating for IPv6 proponents, who view wireless applications as the likely first adopters of IPv6. This frustration was according to the same article evident at a meeting of the IETF's Mobile IP working group, which was held in Minneapolis on March 22.

Steve Deering, Cisco engineer also says [17] "It's a setback for those who are eager to get IPv6 out there". Deering says the Mobile IP working group was blindsided by the security problems. "The IETF's security people were not paying close attention to Mobile IPv6, and then they discovered a significant problem," Deering says.

"This is a real kink in IPv6 deployment," adds Jim Bound [17], a principal software architect at Nokia Networks and chair of the IPv6 Forum's technical directorate. "We need a spec in the market."

On the bright side, Mobile IPv6 problems are not expected to delay the European wireless community's 3GPP, which plans to use IPv6 but has its own security architecture. "3GPP mandates IPv6 but not Mobile IPv6", Deering says [17]. “This will not slow down 3GPP", he continues.

In an article in Network World in October 2000 Steve Deering says [17]: "The major difference between mobile communications in IPv4 and IPv6 is the improved efficiency in mobile routing with IPv6. Communications should be much faster". He continue to say: "We also thought it was going to be more secure. But now it doesn't look like it's going to be more secure."

I Quality of Service

There are two types of resource allocations that are available, IntServ and DiffServ.

I.1 The 20- bit Flow label field

Integrated services, (IntServ): Resource Reservation RSVP is being developed as a resource reservation (dynamic QoS setup) protocol. No service if no resources are available, admissions control.

The most convincing requirement was to add a flow identifier to the original IP protocol. A flow is the set of packets that comes from the same source to the same destination and bears the same flow label. Flow labels will be used when the transmission mandates some special treatment, for example, for applications with strict real-time constraints. The flow label is used to distinguish packets that require the same treatment. This can happen when packets are sent by a given source to a given destination with a given set of options.

For an example, this can be used when someone talks in a mobile telephone and at the same time downloading a file in the background. When using the flow label it is possible to identify which flow identification the speech and the data have and give them the QoS they need.

I.2 The 8- bit Traffic Class

Differentiated Service, (DiffServ) is a service that helps IPv6 to improve the quality of service, which may appear in several ways, mainly by enabling always-on connections, preventing service breaks and enhancing network performance.

The essential three support services that are essential to the success of QoS are Policy Management, Authentication and Accounting/Billing [15].

J The phases

Phase 1 Forces

- Collect material about Ipv4
- Collecting material about Ipv6
- Analyze the material
- Try to answer the following questions:
  - What are the driving forces for transition towards IPv6?
  - When should Kipling transit to be competitive towards their competitors?
- Documentation

Phase 2 Transition strategy

- Collecting scholarly dissertations
- Analyze the material
- Try to answer the following questions:
  - What strategy will be used at the transition?
  - Do the products need to run both versions at the same time, or just change everything over a night?
- Documentation

Phase 3 Implementation-strategy

- Collecting material about Kiplings products.
- Analyze the material.
- Answer the following questions:
  - Why ought Kipling change from IPv4 to IPv6?
  - What are the consequences for the company and their products?
  - What are the greatest advantages they can make use of in there products?
  - Are there any disadvantages against a transition towards IPv6?
  - Is a transition leading to great changes?
  - What can IPv6 offer in a security aspect?
- Documentation

K The IETF IPng interim meeting in Seattle

From: **Thomas Narten <narten@raleigh.ibm.com> Save Address - Block Sender**
To: ipng@sunroof.eng.sun.com **Save Address**
Subject: **IPng interim meeting and 3GPP**
Date: Thu, 24 May 2001 14:08:56 -0400

Reply Reply All Forward Delete Previous Next Close

As you know, the first day of the upcoming interim meeting in Seattle has been set aside for discussions with 3GPP on matters of IPv6. In preparation for this, The IETF IPv6 directorate put together a number of questions for 3GPP (appended below). Those questions were discussed at a recent 3GPP meeting and I'm including a response from Stephen Hayes, one of the 3GPP TSG chairs.

I'm looking forward to a productive meeting in Seattle.

Thomas

From: Thomas Narten <narten@hygro.adsl.duke.edu>
To: 3GPP_TSG_SA_WG2@LIST.ETSI.FR
cc: Mikko Puuskari <mikko.puuskari@nokia.com>,
"Stephen Hayes (EUS)" <Stephen.Hayes@am1.ericsson.se>
Date: Sun, 13 May 2001 15:29:32 -0400
Subject: IPv6 Questions on 3GPP [Joint IETF-IPv6 / 3GPP meeting]

The following set of questions was put together by the IPv6 Directorate after an initial study of some 3GPP documents. This note is intended to start a dialog between the 3GPP & IETF communities on IPv6.

Thomas Narten

3GPP is including IPv6 in its Release 5 specifications, an action that excites the IETF IPv6 community greatly. The 3GPP work will be an important driver for IPv6 deployment. Having said that, the IPv6 community has only a very limited understanding of how IPv6 will be used by 3GPP, e.g., which RFCs will be used, in what parts of the system they will be used, which parts are required and which are optional, etc. We believe that it is in our mutual interest to understand and educate each other on our perspectives on how IPv6 can

best be used to your advantage, which components (e.g., which RFCs) are needed, whether there are any missing pieces, etc.

The IETF IPng WG will be holding an interim meeting in Seattle, WA starting May 30. The first day of meeting has been reserved for a joint meeting with members from 3GPP. It is our hope that such a meeting will facilitate direct technical interactions between 3GPP and IETF engineers on IPv6 issues.

The following describes some general areas where we have some specific questions. These questions were put together after looking at some 3GPP documents that make reference to IPv6, including 23.060 and 23.221.

- What is the addressing model for the network and handsets? Will each handset be given a single 128-bit address and no more? Or will each handset be given its own /64 (e.g. an entire network) so that it can connect additional devices, say through a bluetooth or 802.11 interface?

  A related question is how many additional devices (e.g., a laptop) will be able to connect to a handset (e.g., via bluetooth) and use IP. Doing so would suggest each device would need an IPv6 address and both the handset and the device being on the same subnet. One way of providing such a capability would be to have each handset be a router for a /64 subnet. Is such a configuration envisioned now, or in the future?

- What parts of Neighbor Discovery (RFC 2461) will be implemented on handsets? All of it? How will handsets using IPv6 communicate with each other when on the same subnetwork (or link in IPv6 terminology)? Is ND needed to resolve addresses or does the handset view its connection to the network as a point-to-point link with a router on the other end (i.e., the GGSN)?

- What is the scope of problem for which IPv6 is viewed as a solution? I.e., what features of IPv6 are needed immediately, and which are assumed to be of interest at some later point in the future?

- How permanent are the IPv6 addresses that are assigned to handsets? From our understanding, interface identifiers are assigned by the

GGSN, and handsets then form addresses by combining the interface identifier with a prefix learned through Router Advertisements (RAs). Is it envisioned that information specific to the mobile will be used to form the interface identifier (e.g., IMSI)? Or will the interface identifier assigned to a handset change over time (e.g., if it is power cycled or moves)? This question is important as it will determine whether addresses are effectively permanent in the sense that it will be stable for weeks or more.

In the case that addresses remain stable for weeks or longer, are any of the concerns raised in RFC 3041 viewed as applicable?

- Will handsets be dual stack (i.e., support both IPv4 and IPv6) or will they support only IPv6? Some of the documents suggest that in the IM domain, IPv6 will be used "exclusively". Does that specifically mean that IPv6 must be supported and the IPv4 doesn't apply?

- Where will IPsec (RFC 2401) be used? Will IPsec be implemented on the handset (to provide true end-to-end encryption) or will IPsec terminate at the GGSN, with the remainder of the path (from the GGSN to the handset) protected by link-layer encryption?

  Note that it is our understanding that in the current specs MN to SGSN communication is protected by GSM privacy but there is nothing specified between the SGSN and the GGSN. Will the tunnel between the SGSN and the GGSN will be carried over the Internet?

  Finally, are there any plans to implement IKE? If not, how will IPsec security associations be created?

- Are there any requirements in the area of QOS? Are diffserv and/or RSVP being looked at as something that is important?

- What transition schemes will be used in communicating with IPv4 sites? Some of the 3GPP documents make mention of NAT-PT as well as automatic and configured tunnels. However, automatic tunnels only make sense if address numbering is done in a certain way. It is not clear that the use of automatical tunnels makes sense in the 3GPP environment. Has there been any study of schemes, in addition to NAT-PT, that allow IPv6-only and IPv4-only nodes to communicate?

- Which IPv6 RFCs does 3GPP consider to be part of IPv6, in the sense that they must be implemented as part of the 3GPP Release 5 specification? Are all of these RFCs to be implented in their entirety, or are only subsets of (some of) them needed? Is there any intention to take parts of the IETF protocols and modify or extend them?

- Are there any plans or needs with regards to compression? For example, the IETF has existing standards (e.g., RFC 2507) and on-going efforts to compress IP traffic over link layers. Is it anticipated that 3GPP will have needs here?

- What DNS components will be used? For example, IPv6 addresses can reside in either AAAA or A6 records. Will resolvers in handsets be implementing A6 records? Or both AAAA & A6?

Many of the above questions are somewhat open-ended and would probably benefit from face-to-face discussion. It is our hope that this will occur at the Seattle meeting and/or through e-mail followups. In addition, we would welcome any questions you might have on IPv6 issues.

Overall, we would like to understand the overall 3GPP architecture and how IPv6 fits into it. 3GPP documents are organized and structured very differently from IETF documents, so for us it has been difficult to understand where and how IPv6 is being used and whether its usage will bring any unexpected surprises (e.g., are there any shortcomings or missing components?). We believe a technical discussion between the IETF and 3GPP communities on the topic of IPv6 would be mutually beneficial to both communities.

From: "Stephen Hayes (EUS)" <Stephen.Hayes@am1.ericsson.se>
To: deering@cisco.com, mikko.puuskari@nokia.com, narten@raleigh.ibm.com,
Erik.Nordmark@eng.sun.com, hinden@iprg.nokia.com
Cc: tech@ipv6forum.com
Date: Mon, 21 May 2001 09:27:09 -0500
Subject: Additional info on May 30 IPnG/3GPP meeting

Dear Colleagues,

The 3GPP has been invited by the IETF IPng WG to a one day discussion of how 3GPP will use IPv6. The meeting will be held on May 30, 2001 at Redmond, WA. Please see (http://research.microsoft.com/ietf-ipv6-meeting) for info about the meeting. At the 3GPP SA2 meeting held on May 14-18 there was a discussion of what should be presented by the 3GPP at the IPng meeting. Hopefully this quick synopsis of those discussions will help in preparation of the meetings.

Based upon the discussions I would expect the following at the meeting from the 3GPP side:

1. A presentation of the 3GPP architecture. This will include a discussion of:
   - the reference models
   - 3GPP protocol stacks (involving IPv4/IPv6)
   - 3GPP packet concepts (PDP context, APN, GTP)
   - IP address allocation

2. A high level presentation on the 3GPP QoS architecture

3. Verbal answers to the questions posted previously(the list of questions is attached at the end for convenience). The IETF may find the answers unsatisfying as most of the answers are "it is an implementation decision" (Questions 2,4,5,8,11) or "for further study" (Questions 6,9,10). Some concrete answers are given below:

- Q 1 - There is currently no capability defined to allocate a subnetwork
- Q 3 - The main need is the address space
- Q 7 - Yes there are requirements - to be discussed in QoS presentation

Of course, these quick answers and the terms "implementation decision" and "for further study" leave lots of degrees of freedom, so I would not recommend waiting for the answers delivered by the 3GPP delegates to get the full flavor of the answers.

4. Verbal guidelines for what 3GPP documents are relevant and how they fit together.

There will be several 3GPP experts at the meeting, so I would expect a lively discussion. The presentations will be being refined this week on the 3GPP SA2 mailing list. The latest copies of the presentations should be available on the mailing list.

Best regards, Stephen Hayes
3GPP CN Chair

IETF IPng Working Group Mailing List
IPng Home Page: http://playground.sun.com/ipng
FTP archive: ftp://playground.sun.com/pub/ipng
Direct all administrative requests to majordomo@sunroof.eng.sun.com

---