Accelerating Adoption of IPv6

LUDVIG AHLINDER
and
ANDERS ERIKSSON

KTH Information and
Communication Technology

Degree project in
Communication Systems
First level, 15.0 HEC
Stockholm, Sweden

Accelerating Adoption of IPv6

Ludvig Ahlinder
and
Anders Eriksson

2011.05.17

Mentor and Examiner: Prof. Gerald Q. Maguire Jr
School of Information and Communications Technology
Royal Institute of Technology (KTH)
Stockholm, Sweden

Abstract

It has long been known that the number of unique IPv4-addresses would be exhausted because of the rapid expansion of the Internet and because countries such as China and India are becoming more and more connected to the rest of the world.

IPv6 is a new version of the Internet Protocol which is supposed to succeed the old version, IPv4, in providing more addresses and new services. The biggest challenge of information and communication technology (ICT) today is to transition from IPv4 to IPv6. The purpose of this thesis is to accelerate the adoption of IPv6 by highlighting the benefits of it compared to IPv4.

Although the need for more IP-addresses is the most urgent incentive for the transition to IPv6, other factors also exist. IPv6 offers many improvements to IPv4 which are necessary for the continued expansion of Internet-based applications and services.

Some argue that we do not need to transition to IPv6 as the problems with IPv4, mainly the address-shortage, can be solved in other ways. One of the methods of doing this is by extending the use of Network Address Translators (NATs), but the majority of experts and specialists believe that NATs should not be seen as a long-term solution.

Another difficulty with the new protocol is explaining its benefits and areas of use to both the business world and the public. Understanding these benefits are necessary in order create awareness of these benefits, thus to accelerating the adoption of IPv6. This thesis aims to explain the incentives for both businesses and the public to adopt IPv6.

Sammanfattning

Det har länge varit känt att antalet unika IPv4-adresser kommer att ta slut på grund av Internets rapida utveckling och på grund av att länder såsom Kina och Indien blir allt mer uppkopplade mot resten av världen.

IPv6 är det nya Internetprotokollet som skall ersätta den nuvarande versionen, IPv4, genom att erbjuda fler IP-adresser och nya tjänster. Den största utmaningen inom ICT idag ligger i att påbörja övergången till det nya protokollet. Denna uppsats har som syfte att påskynda övergången till IPv6 genom att framhäva fördelarna med IPv6 jämfört med IPv4.

Även fast bristen på IP-adresser är den största anledningen till att IPv6 behövs så finns det andra faktorer som också spelar in. IPv6 innehåller en mängd förbättringar jämfört med IPv4 som kommer vara nödvändiga för att Internet och Internetbaserade applikationer och tjänster skall fortsätta att utvecklas.

Vissa menar att vi inte behöver byta till IPv6 och att problemen med IPv4, främst adressbristen, går att lösa på andra sätt. En sätt att göra detta på skulle vara att fortsätta att implementera användandet av Network Adress translators, men majoriteten av experter och specialister menar på att detta inte skall ses som någon långsiktig lösning.

En annan svårighet med det nya protokollet är att förklara dess nödvändighet för företag och privatpersoner. Detta är nödvändigt för att påskynda övergången och skapa medvetenhet om IPv6, vilket vi hoppas göra genom denna rapport.

Acknowledgment

This bachelor’s thesis would not have been possible without the help of many people. We would like to express our gratitude towards Professor Gerald Q. Maguire Jr. for providing us with help and feedback throughout the project. We would also like to thank Jan Östling who offered invaluable expertise about IPv6 as well as letting us use his Janoz Method for the purpose of our thesis.

Table of Contents

List of figures

List of Acronyms and Abbreviations

Acronym	Description
AS	Autonomous Systems
API	Application programming interface
ARP	Address Resolution Protocol
BOOTP	Bootstrap Protocol
CoA	Care-of-address
CoS	Class of service
DHCPv4	Dynamic Host Configuration Protocol version 4
DHCPv6	Dynamic Host Configuration Protocol version 6
DNS	Domain Name System
e2e	End-to-end
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
IP	Internet Protocol
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
ITS	Intelligent Transport Systems
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MTU	Maximum Transmission Unit
NAT	Network Address Translator
ND	Neighbor Discovery

P2P	Peer-to-Peer
RA	Router Advertisement
RARP	Reverse Address Resolution Protocol
RS	Router Solicitation
SCTP	Stream Control Transmission Protocol
SIP	Simple Network Protocol
SLAAC	Stateless Address Autoconfiguration
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
ToS	Type of service
TTL	Time to live
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
QoS	Quality of Service

1 Introduction

1.1 *Longer problem statement*

The purpose of the thesis is to look at solutions to enable a quick and smooth transition for Swedish corporations and private persons to IPv6, rather than continuing to be dependent upon IPv4, and thereby accelerate the adoption of IPv6. Prof. Gerald Q. Maguire Jr. suggested this topic and we liked the idea making an impact on companies, as well as private persons, by explaining why changing to IPv6 would prove very beneficial.

The central pool of IPv4 addresses officially ran out on Tuesday, first of February 2011 and this is expected to cause problems in several areas. We want to investigate what private persons and enterprises would gain from changing to IPv6 and how it should be done. We want to examine where the bottleneck is and find out what is causing the delay in the transition to IPv6. The main purpose of our project is to create awareness about IPv6 in order to accelerate the adoption of IPv6. We hope to achieve this by exposing this topic in the media.

This is a suitable bachelor thesis project because it requires us to apply our technical knowledge to investigate and evaluate the different benefits of IPv4 and IPv6. It also requires an understanding of how businesses, governments, and individuals will respond, both economically and politically to the transition to the newer version of the IP protocol.

1.2 Report Summary

Chapter 2 provides some basic background and the motivation for this thesis project. Chapter 3 explains what the Internet Protocol is and more specifically what IPv6 is, as well as the limitations of IPv4 and why a transition is needed. Chapter 4 compares both protocols and highlights the improvements that have been made leading to IPv6. Subsequently, Chapter 5 describes hardware, software, and appliances with regard to the transition to IPv6. IPv6-readienss of products is also discussed. Chapter 6 examines some of disadvantages of IPv6, mainly that the transition process will require a lot of effort & time and that there is no general transition plan (but rather than have to be specific transition plans by each network operator). Chapter 7 describes mechanisms, incentives, and procedures for the transition. Examples of implementation-cases are provided, as well as the business value for transitioning to IPv6. IPv6's future use in various industries is also discussed. In chapter 8 we reflect upon the status of IPv6 in Sweden – based upon discussion with employees of various companies and organizations. We ask them what they think about the upcoming switch to IPv6. We also include some global IPv6-statistics in terms of IPv6 traffic and the number of IPv6 enabled autonomous systems (ASs). Chapter 9 briefly discusses how to utilize IPv6 by setting up a tunnel through a tunnel broker (specifically, www.tunnelbroker.net).

2 Background

2.1 *What have others already done?*

IPv6 has been the topic for numerous theses and projects. However, most of these reports have focused on specific technically areas of the new protocol, such as its new features in comparison to IPv4. Many reports have focused on the need for businesses to realize the seriousness of the problem of needing to transition to IPv6 and suggest that business start to prepare for this migration by providing incentives for the transition to IPv6. However, few reports have focused on providing information about IPv6, especially by using examples to explain the everyday use of IPv6, in order to prepare both the business-world the general public to the transition.

Examples of previous theses with focus on how IPv6 can be used in our everyday life can be found in the bachelor's thesis *Virtually@home* by Anders Nilsson and Magnus Lindberg [1] and in the bachelor's thesis *IPv6 Home Automation* by Thor Hådén [2].

2.2 *About the text*

This thesis is intended for Professor Gerald Q. Maguire (our tutor and examiner), other students, and anyone with an interest in the subject at hand. The reader should have a moderate amount of knowledge about the different Internet Protocols, as well as about information and communication technology in general. We chose to write the thesis in English in order to reach a larger audience than only the Swedish-speaking audience. However, there was an interview largely in Swedish with one of us as part of the news program "SVT Rapport" on Swedish Television (SVT) [3].

3 Method

3.1 *Goals*

We want to perform research and help users to rapidly transition to IPv6 by providing information and education, both for private persons and companies. We want to educate the public about the benefits that IPv6 brings and why we need to change from IPv4 to IPv6 as soon as possible. We want to investigate what might be incentives for both companies and private users to migrating to IPv6.

3.2 *How are we going to meet our goals*

We began our project by collecting data about how the new IPv6 protocol differs from IPv4. This was done by reading books and consulting other sources. This chapter is rather long because there is a lot of information necessary to understand IPv6. The main reason for this chapter is to understand how the new protocol works. A good understanding of IPv6 is necessary to benefit from the remainder of this thesis.

After this we examine what needs to be done to migrate to IPv6 for both companies and private persons. Examples of areas that we will investigate are hardware, software, transition mechanisms, benefits, and costs. This investigation is based upon reading books, searching on the Internet, reading & viewing media reports, and by interviewing experts. This investigation enabled us to write an overview over what has to be done to transition to IPv6 and to investigate the complexity of this transition. We also wanted to find the main bottleneck hindering the transition to IPv6.

Finally we want to distribute the information that we have learned about IPv6 through the media in the hope of increasing customers' awareness of and demand for IPv6 in Sweden. During the course of this project we generated the following stories for distribution:

- An interview that became part of a report on SVT Aktuellt [3]
- A web blog: blog.wearestudents.se
- Survey
- Word of mouth

4 What is IPv6

The Internet operates by sending small packets of information, called datagrams, from a source to one or more destinations. These datagrams are independently routed through different networks in accordance with a communications protocol called the Internet Protocol.

Internet Protocol version six (IPv6) is the newest version of the Internet Protocol and it is supposed to succeed the current version of it; Internet Protocol version four (IPv4). IPv4 was first deployed in 1981 and spread across the world as the Internet grew. IPv4 has become well entrenched and is used by every internet service provider (ISP) to connect its users to the Internet. IPv4 has proven to be a very successful protocol. This has enabled the Internet to grow to its current size. IPv4 allows for interoperability with a wide range of device (ranging from appliances to very large servers). However, the biggest problem with IPv4 is the relatively small pool of IP-addresses that it provides. With its 32-bit address field IPv4 can support less four billion IP addresses for network interfaces (as some of these addresses are used for special purposes). This number of addresses is clearly insufficient when compared to the world's population — that as of mid-year 2010 was roughly *seven billion* people [4]. Thus the number of IPv4 addresses would not even permit half of the people to have a device with a public IPv4 address, let alone enable them to have several such devices active at one time.

In order to deal with the long-anticipated depletion of the IPv4-addreses, IPv6 was developed by the Internet Engineering Task Force (IETF) and deployed in 1999 [5] IPv6 represented the next step in the evolution of the IP. IPv6 was expected to improve IPv4's scalability, enable easy configuration of network attached devices, and enable end-to-end global networking. The main advantage with IPv6 is that it utilizes a 128-bit address field; this allows for approximately 3.4×10^{38} IP addresses. To put this in perspective, this means that every single person on the earth could be allocated about 50 000 000 000 000 000 000 000 000 000 IP-addresses each, which in itself already is $7.4\text{x}10^{18}$ times as many as the current *total* IPv4 pool. However, this is not the only improvement made with IPv6. Amongst other things, IPv6 brings more efficient routing, reduces management-requirements, offers greater support for mobile devices, supports multi-homing, and makes the features of IPSec mandatory to implement. The combined feature of IPv6 enable the Internet to further expand and paves the way for new and exciting scenarios with a multitude of new IP-based services. Some of these features enable entirely new ways of communicating.

Unfortunately, today the adoption of IPv6 is still in its infancy. Very few users have native IPv6 connectivity. According to Mike Leber's *Global IPv6 Deployment Progress Report*, as of 30 April 2011, a little less than 10% of the global Autonomous Systems have deployed IPv6 [6].

5 Advantages over IPv4

As mentioned above, IPv6 brings many new features and improvements over IPv4. In addition to providing more addresses, the IETF wanted to streamline and upgrade the new version of its internet protocol, whilst at the same time remove all of the “unnecessary” parts — in order to simply the processing of IP datagrams (thus reducing delay when forwarding packets).

5.1 *Larger address space*

In order for a device to be connected to the Internet it needs an interface. In order for this interface to be the destination for IP datagrams it needs to have an identifier. IP-addresses are numeric addresses that identify interfaces connected to the Internet. Both IPv4 and IPv6 addresses come from finite pools of numbers. As noted in the previous chapter the IPv6 address pool is substantially larger due to its 128-bit address space in comparison to IPv4 32-bit addresses. IPv6’s extremely large address space should provide a stable foundation to continue the development and expansion of the Internet.

The main goal of IPv6 address space management is to ensure that the addresses are distributed in a hierarchical manner that should match the topology of the network infrastructure. This hierarchical addressing enables the aggregation of routing information by ISPs, hence limiting the size of Internet routing tables.

5.2 *New simpler header*

The first thing you notice when comparing IPv4 and IPv6 headers is that several elements, such as the options-field, no longer exist or have been replaced in the IPv6 header. The cluttered IPv4 header made it more difficult to ensure good routing-efficiency and reduced the over-all efficiency of IPv4 networks.

5.2.1 Version/IP version

The 4-bit version field is the only field in the IPv6 header that is the same as in the IPv4 header. In an IPv6 header the version field contains the number six, while in an IPv4 header this field contains the number four. However, this field has limited use as both IPv4 and IPv6 packets need not always be identified based on the number in the version-field. For example, in the case of an Ethernet the link layer uses two different link layer identifiers for these two types of link payloads.

5.2.2 Traffic class

In IPv4, the type of service (ToS) field which has had different purposes over the years. In fact, it has been redefined five times by the IETF. However, the original purpose of this field was to allow a source (a host sending a datagram) to specify how the packet should be handled, in terms of minimizing delay, minimizing cost, or maximizing reliability when the packet is forwarded. This allowed routers to determine which outgoing queue to use and where in this queue to place a given datagram. The new class of service (CoS) field is supposed to work in a similar fashion, hence service providers are working hard to establish a standard interpretation for the values in this CoS field.

5.2.3 Flow label

The flow label is used to identify packets belonging to a specific flow. If a packet flow requires a certain CoS, then this label allows routers to easily detect a specific flow and handle all of the datagrams in the same way.

5.2.4 Payload length

The total length-field in IPv4 has been replaced in IPv6 by the payload length-field. This field specifies the length of the IPv6 payload and differs from IPv4 by indicated the length of the data carried *after* the header, whereas in IPv4 this field included the header as well.

5.2.5 Next header

The next header-field is one of the most important additions to the IPv6 header, as it reflects the new organization of IP-packets in IPv6. The next header-field allows for the use of extension-headers and indicates the presence of an extension header, as well as identifying the next extension-header to be examined.

5.2.6 Hop limit

The time to live (TTL) of IPv4 is used to avoid datagrams being forwarded in infinite loops. However, this feature was expressed in seconds *or* hops. In contrast the hop limit-field in IPv6 is strictly based on the maximum number of hops the packet can be forwarded until it is dropped.

5.2.7 Source address &Destination address

The source address indicates where the datagram originated, whereas the destination address indicates the final destination of the datagram [8].

Figure 5-1 IPv6 header header (Adapted from figure provided by G. Q. Maguire Jr. in his IK1550 lecture note [7]) shows the IPv6 header, while Figure 5-2 IPv4 Header (Adapted from figured provided by Geoff Huston in his IPv4 Address Report [9])shows the IPv4 header to illustrate the difference between the two protocols.

<table>
<tr><td colspan="1">Version
4 bits</td><td colspan="2">Class
8 bits</td><td colspan="5">Flow label
20 bits</td></tr>
<tr><td colspan="4">Payload length
16 bits</td><td colspan="2">Next header
8 bits</td><td colspan="2">Hop limit
8 bits</td></tr>
<tr><td colspan="8">Source address
128 bits</td></tr>
<tr><td colspan="8">Destination address
128 bits</td></tr>
</table>

Figure 5-1 IPv6 header header (Adapted from figure provided by G. Q. Maguire Jr. in his IK1550 lecture note [7])

<table>
<tr><td colspan="1">Version
4 bits</td><td colspan="1">Header
length
4 bits</td><td colspan="2">Type of service (ToS)
or
Differentiated service
8 bits</td><td colspan="4">Total length
16 bits</td></tr>
<tr><td colspan="4">Identification
16 bits</td><td colspan="1">Flags
3 bits</td><td colspan="3">Fragment offset
13 bits</td></tr>
<tr><td colspan="2">Time to live (TTL)
8 bits</td><td colspan="2">Protocol</td><td colspan="4">Header checksum
16 bits</td></tr>
<tr><td colspan="8">Source address
32 bits</td></tr>
<tr><td colspan="8">Destination address
32 bits</td></tr>
<tr><td colspan="8">Options (padded to 32 bit length)</td></tr>
<tr><td colspan="8">Data</td></tr>
</table>

Figure 5-2 IPv4 Header (Adapted from figured provided by Geoff Huston in his IPv4 Address Report [9])

5.2.8 Extension headers

As mentioned earlier, one of the new exciting features of the IPv6 header is the ability to include one or several extension headers. The extension headers are included after the “main header” and before the IP data field and are supposed to offer both flexibility and efficiency.

Instead of having all of the different fields which only are used for special purposes in the main header, like in IPv4, these fields are now implemented only when needed, in the form of extension headers. The result is a cleaner, smaller and more streamlined main header that only needs to hold the information that must be present at all times.

The only field that is common to all of the extension headers is the Next Header field which is used to indicate if there is another extension header or if it is the last header before the IP data. In order to better understand the concept of extension headers compare the case of a simple TCP segment (shown in the upper half of Figure 5-3 Implementation of extension headers (Adapted from figured provided by TCPIPGUIDE.com) with the same TCP segment but with extra headers (shown in the lower half of Figure 5-3 Implementation of extension headers (Adapted from figured provided by TCPIPGUIDE.com)).

1. The main IP header has a Next Header value of zero, which indicates the presence of a Hop-By-Hop Options header.
2. The Hop-By-Hop header has a Next Header value of forty-four which indicates that there is a Fragment extension header following the Hop-By-Hop header.
3. The Fragment header has a Next Header value of six which indicates that this is the last extension header and that the following header is the TCP header.

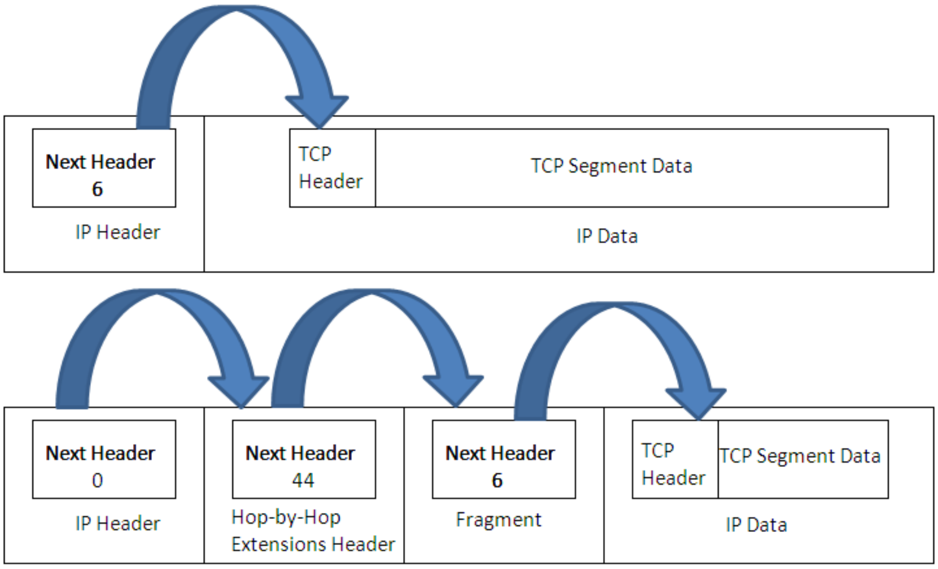


Figure 5-3 Implementation of extension headers (Adapted from figured provided by TCPIPGUIDE.com)

The extension headers in IPv6 can easily be confused with datagram options. IPv4 only had *one* header, but included a provision for options. This turned out to be very inefficient, so in IPv6 the IETF decided to introduce the concept of an extension header. IPv6 also supports the use of options, so one might wonder why included both? The short answer is to be able to provide *even* more flexibility with the ability to include options as a special form of extension header. These options supplement the existing extension headers and can provide almost limitless usability greatly decreasing the risk of the protocol becoming obsolete [10].

Examples of extension headers are the Routing header and the Hop-by-Hop Options header. The Routing header allows for a source to specify how it wants the datagram to be routed. The Hop-by-Hop Options header is as an extension header that includes the ability to send jumbograms of data. A jumbogram can be as large as 4 294 967 295 octets (roughly 4.3 gigabytes) and is suitable when large amounts of data, such as multimedia information, needs to be sent over a high speed link that supports large link layer frames.

5.3 *The Multihoming problem*

Multihoming is a technique that allows a host or network to be connected to more than one ISP at a time. The main purpose of multihoming is to increase the quality and robustness of the network connectivity. If the connection via one ISP fails, then traffic can be rerouted through another ISP. The single biggest reason multihoming is needed is to avoid a single point of failure. The existence of a single point of failure can have devastating effects on sites or networks that wish to maintain high availability, such as e-commerce sites, e.g., Amazon [11].

However, multihoming requires either (1) provider independent IP address spaces or (2) each host has to have an address from each provider **and** know when to use which address. Using provider independent addresses makes it possible for the end user to change which ISP they use *without* renumbering each of the hosts in their network. Provider independent addresses are addresses that do not belong to any ISP, but are assigned to users directly by a regional Internet registry. The drawback with these addresses is that every end user's address range will be visible in the *global* routing tables, instead of being aggregated under an ISP's range of addresses. This can increase substantially the burden on global routers.

Multihoming is something that many companies demand, but in IPv4 there is as of currently no good way of solving this problem for all protocols — although protocols such as the stream control transmission protocol (SCTP) supports multihoming. Several suggestions of how the problem should be solved have been proposed, but there is still not a clear solution.

5.4 *Multicast, Unicast, Anycast*

Ipv6 supports three main types of destination addresses: multicast, unicast, and anycast. The first and second of these types are the same as for IPv4, but anycast is a new type introduced by IPv6. A description of each of these types is given below.

5.4.1 Multicast

Multicast addresses are used to send IP packets to *a group of interfaces*. . If you send a packet to a multicast address every interface connected to it will process the packet ([12] , page 36). Multicast addresses exist in IPv4, but the concept has been modified and improved in IPv6. Note that the concept of a broadcast address from IPv4 does not exist in IPv6, but rather these use cases are subsumed by IPv6's multicast addresses.

One of the new concepts introduced in IPv6's multicast mechanism, is the concept of ***explicitly indicating the scope of a given multicast.*** The scope field in IPv6 delimits where the multicast traffic is intended to be sent. Routers use the multicast scope field to determine if the traffic *should be* forwarded. IPv6 multicast addresses can have one of 14 different scopes.

5.4.2 Unicast

A unicast address simply addresses a unique network interface of an IPv6 node. A packet sent to a unicast address is sent to the node's interface identified by that address ([12] , page 36).

5.4.3 Anycast

An anycast address is assigned to one or more nodes by a router. A packet send to an anycast address is sent to one node (usually the nearest one) ([12] , page 36). For example, there can be an anycast address to find an instance of a specific service.

5.4.4 Scoped addresses

One of the improvements to the addressing-scheme in IPv6 is the introduction of scoped addresses. The large pool of IPv6-addresses is divided into hierarchical routing domains to better reflect the

Internet topology of today. Because IPv6 uses 128-bits for the addresses, this means that several levels of hierarchy for addressing and routing can be designed. IPv4 lacks this ability and uses a mixture of flat and hierarchical addressing and routing.

Every IPv6 address has a reach ability scope. This means that the data sent to an IP-address is limited in how far it can be routed, depending on the scope of this address. Different addresses can share the same network interface, but can have different scopes.

Unicast and anycast have three different address scopes (as noted above, multicast already has its scope built-in): link-local, site-local, and global. Each of these is explained further below.

Link-local Link-local addresses are used by nodes when communicating with neighboring nodes on the same link. Unsurprisingly, the scope of a link-local address is simply the local link and an IPv6 router *never* forwards link-local traffic beyond the link.

Site-local Site-local addresses are used within private intranets, i.e., these packets are not to be forward to the IPv6 Internet. These addresses can be used without conflicting with global unicast addresses. Routers **must not** forward site-local traffic outside of the site; hence these addresses are not reachable from other sites. An example of a site could be an organization’s internal network.

Global IPv6 global unicast addresses are equivalent to public IPv4 addresses. These addresses can be reached on the IPv6 Internet and are globally routable. A goal for allocating these addresses is to be able to aggregate them in order to provide an efficient routing infrastructure. The scope of a global unicast address is the entire IPv6 Internet.

5.5 *ICMP in IPv6*

The internet control message protocol for version IPv6 (ICMPv6) is a part of the IPv6, and must be implemented by every IPv6 node. ICMPv6 delivers messages about the network status and error reports (for example: Destination Unreachable, Packet Too big, Time Exceeded, and Parameter Problem). It also can provide diagnostic features (for example: Ping – using an ICMP echo request). An ICMPv6 redirect message can be sent if a node is sending all of its traffic through one router but another router offers a better route. The change in ICMPv6 introduces new functionalities for example IGMP has been absorbed in ICMPv6 and ND uses ICMPv6 messages to learn the link-layer addresses for host attached to the same link find routers, get information about which nodes are accessible, and discover changes in link-layer addresses..

5.5.1 Router advertisement

When individual networks are connected an Internet is created. This internet is formed by routers in the network. Neighbor discovery is essential for learning which interfaces are connected to which network link. The host needs to learn about the local router and what network it is attached to. A router advertisement (RA) is sent by the router to inform hosts about this router and the network. If a host wants to proactively get this information from a router it sends a router solicitation (RS) message. Both RA and RS messages are optional

RA is a host-router discovery mechanism provided by routers. RA uses link-local addresses to identify routers. A router sends out RAs periodically or when special events occur (i.e., when a host requests a RA by sending an RS). A router advertisement enables the nodes to automatically configure the interface to connect to the network. In IPv6, RAs contain a source link-layer address and a maximum transmission unit (MTU) value. The sending interface link MTU is used as the value in the MTU option field. In the RA message there is a suggestion of whether stateful address configuration should to be used. RA messages can also be used by routers to advertise preferred and explicit routes, thus giving the host an opportunity to select the best router— if it receives get more than one RA. This is also good for multihome routers (which are a key feature in an IPv6 network). RAs are used also in Stateless Address Autoconfiguration (SLAAC). In SLAAC, RAs provide information about the subnet mask and what gateways must be configured; hence there is no need to manually configure a subnet mask as this information can be learned from the RA ([12] , pages 74-75).

5.5.2 Stateless Address Autoconfiguration and DHCPv6

There are two major methods for configuring clients with an IP address in IPv6: SLAAC and DHCPv6. DHCPv6 is essentially an upgrade of IPv4's DHCP and is used for the same reasons. SLAAC is a new feature in IPv6 and allows nodes in an IPv6 network to auto-configure themselves, thus creating a "plug-and-play"-scenario that is highly desired by network administrators. There are, however, a growing number of IPv6 experts that are worried about the adoption of SLAAC as it does not configure all the network parameters—unlike DHCPv6 which allows the administrator to control many of the network parameters.

SLAAC allows various devices in an IPv6 network connect to the Internet without having to rely on DHCP. SLAAC makes life simpler for a network administrator since it automates IP address configuration of network devices using ICPMv6 router discovery messages. When a node first connects to an IPv6 network it sends out a link-local RS multicast request to learn the configuration parameters. If configured properly, one or more of the routers in the network will then respond with a RA containing the network configuration parameters.

Before SLAAC, configuration had to be done manually or with the help of DHCP. However, SLAAC has one big disadvantage as compared to DHCP: it only provides IP address configuration and does not configure the other networking parameters, such as the DNS domain, DNS server, etc. This means that this information has to be added with another protocol. Here is where DHCPv6 has an advantage as it can provide all of these other parameters. Another pitfall of SLAAC is that it does not provide control over which addresses are allocated. This might seem superfluous, but knowing when a given host is assigned a given address can be useful for auditing purposes.

DHCPv6 works much like its IPv4 predecessor, DHCPv4, and the protocol is basically the same. What greatly differs are the details of DHCPv6. DHCPv4 is based on the BOOTP protocol which has a wasteful packet layout, with space allocated for various options that may not be used. However, in the case of DHCPv4 it is also hard to change a protocol that is so widely used. As a new protocol, DHCPv6 leaves this entire legacy behind.

A feature of IPv6 that greatly improves DHCPv6 is the fact that IPv6 interfaces can have link-local addresses. This makes it possible for IPv6 to send requests for "real" addresses using these link-local addresses, whereas IPv4 hosts have to use a system-specific hack to get an IPv4 address. Another feature is that all IPv6 systems support multicast, hence all DHCPv6 servers can register to receive DHCPv6 multicast packets, thus the network will thus know where to send these packets. In IPv4 clients have to broadcast their requests and the networks do not know how far to forward these requests. Another feature of DHCPv6 is that a single request can be used to configure all of the interfaces on a device.

There is an ongoing debate over which of the two configuration protocols to use, or if a combination of them is the best solution. Some claim that SLAAC should be used for configuring an initial IP address; while DHCPv6 should be used to configure the rest of the network parameters. Others say that SLAAC is unnecessary, as DHCPv6 can be used for both functions. Despite this, SLAAC is thought of to be the best long-term solution if it can be rebuilt to provide the other parameters as well. Alternatively many of the other parameters need not be statically configured as the host can use anycast addresses to find a DNS server (see for example RFC 4339 [36]), printer server, etc. The question of using DHCPv6 or SLAAC is something that every network administrator is bound to face sooner or later [13].

5.6 *IPv6 and DNS*

DNS is used to mapping a name to an address (in both IPv4 and IPv6) and vice versa. In IPv6, DNS takes an even larger and more necessary role due to the length of IPv6 addresses. When hosts utilize both protocols there is a need for multiple entries in the DNS. A new DNS record has been defined for IPv6 hosts. This DNS record is called AAAA or quad-A instead of A in IPv4. RFC 3596 [37] defines the quad-A type record ([12], pages 242-243).

5.7 *Avoiding NATs*

Network address translation (NAT) is a function that can be implemented in a router, firewall, or proxy server which interconnects a group of hosts to another network. A NAT can be used to enable several hosts to share one or more IP addresses. NAT was invented due to the lack of available IP addresses and was thought by many to be a good *short term* solution. However, today there are a number of reasons why we should avoid NATs and instead use IPv6 (see for example RFC 4966 [38]). NATs hold back peer-to-peer services, by introducing additional complexity to the systems due to having to work around NAT. NAT causes problems for applications requiring quality of service (QoS), such as IP-TV, VoIP, and real-time video — because of the need for end to end connectivity between end points.[14] Additionally, NAT requires additional processing by the NAT device, slowing packet forwarding.

5.8 *IPv6 Security*

In IPv6 the security is built-in as part of the protocol suite, i.e. the protocol includes header extensions to support authentication, data integrity (encryption), and optional data. IPv6 was built with security in mind unlike IPv4, therefore a lot of mechanisms needed to be added to IPv4 to secure IP traffic. One of the key capabilities of IPv6 is the increased address space allowing each interface to have a unique public IP address, thus enabling end-to-end IP security – rather than only providing network-to-network security.

5.8.1 IPSec

It is clear that the Internet needs to be able to provide a secure environment to support the success of Internet. IPv4 utilizes protocols such as SSL under the HTTP protocol or SSH to make IPv4 safer. IPSec differs from SSL and other security add-ons by implementing security at the network layer, thus making secure end-to-end communication possible for all the services on top of IP *by default*.

A new study on IPv6 security shows that IPv6 and IPv4 use the same IPSec-based protocols. However, in IPv6 IPSec is built-in. IPSec was initially designed for IPv6, but later was successfully implemented for IPv4 (when there were no NATs on the path). IPv6 implements some new policies for firewalls, for example, ICMPv6 and multicast traffic should **not** be blocked by default. Another aspect of IPv6 is that some operating systems may enable IPv6 by default, i.e., without the administrator’s knowledge which can cause security problems, thus leaving hosts unprotected from attacks.

IPSec is supported by a variety of operating system platforms. IPSec makes it possible to implement a secure virtual private network (VPN). IPSec provide open standard which enables interoperability between different devices [15].

5.8.2 Possible threats to networked services

Some of the most common threats to network services today are:

Denial of service A denial of service attack’s main purpose to prevent normal usage of the service. The most common attacks are overload attacks. This type of attack frequently targets business sectors such as banking and financial institutions. These kinds of attacks are easily detected because they have a noticeable impact on the system.

Fabrication, Modification, Deletion attacks These types of attacks are hard to detect. Examples of such attacks are modifications/infiltration of false information in e-mail, payment systems, or other trusted communications.

Eavesdropping Eavesdropping is almost impossible to detect, as IP sniffing software is readily available and many switches have support for port replication, making it easy to get a copy of all of the traffic passing through one or more ports of the switch.

5.9 *Mobile IPv6*

One of the features of IPv6 is built-in support for mobile IP. Mobile IP allows for mobile nodes, such as laptops, cell phones, and other wireless devices to maintain a constant IP address while connecting via different networks. This allows for seamless IP mobility, which means that the node does not have to re-establish any upper-layer connections after any network transition.

However, Mobile IP has not been widely used for a number of reasons. For one, mobile IP was not built into IPv4, which made using it more troublesome. Mobile IP in IPv4 also had flaws regarding security. Some of these issues have been resolved in IPv6, but Mobile IP still remains unused. Jan Östling, Systems Engineer at Cisco Systems Sweden, suggest that a possible explanation for this is that there is actually very little need for this kind of portability [11]. One could think that all of the billions of wireless devices around the world could make great use of this feature, but this is not the case. As an example, when it comes to 3G/4G connectivity the mobile operators have avoided the need for mobile IP by implementing their own tunneling mechanisms. Also, very few users need to be connected *all* the time. An example of this can be when you are streaming video content from the web. What will happen if you move from one network to another and the connection is disrupted? Well, most likely you will experience latency issues and the streaming might stop for a brief moment. However, once the connection has been reestablished the video will continue to buffer and you can carry on watching the video. The few instances when Mobile IP is suitable is when it is absolutely vital that the connection is not disrupted, which for example could be the case within the military. Due to the limited use of Mobile IP we will not consider it further in this thesis.

6 IPv6 Hardware and Software

Fortunately, the change from IPv4 to IPv6 will not require much work for home users [11]. As most modern operating systems already support IPv6, most end users will simply buy a new router that supports IPv6 as well as IPv4. However, this is easier said than done. While physically replacing your old router with a new one is not a very complex task, this can only be done if your network hardware and connection *actually* support IPv6.

6.1 *Software support for IPv6*

6.1.1 Operating Systems

Most modern operating systems are shipped with support for IPv6. The table below summaries this support for three of the most widely used operating systems.. For a more extensive list of operating systems with support for IPv6 please refer to appendix II.

Table 6-1: Operating System support for IPv6

Apple Computer	All versions of Apple Computer's OS X later than, and including, 10.2 have support for IPv6 [16].
Microsoft	Microsoft has done a good job in incorporating support and transition mechanisms into their different versions of Microsoft Windows [11]. Windows 7, Windows Server 2008 R2, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP with Service Pack 2, Windows XP with Service Pack 1, Windows XP Embedded SP1, and Windows CE .NET all have in-built support for IPv6 [17].
Linux	Linux has had support for IPv6 since the 2.2.x kernels and 6to4 tunneling has been there for almost as long.

6.1.2 Applications

It will take some time until all applications support transport over IPv6. Some applications have no direct dependency on the IP layer and will run equally well without modification in IPv4 and IPv6 environments. However, some applications have dependencies and will have to be modified. These modifications should be made so that the application will be as protocol-independent as possible, so that the application can be used in both IPv4 and IPv6 environments. Tests indicate that many applications behave well in a dual-stacked or tunneled environment ([12] , page 305).

The challenge for developers lies in building applications that works well in all situations. The following are some of the most important IP dependencies in applications:

- Format of the IP-address (32-bit dotted decimal or 128-bit hexadecimal with colons),
- Application programming interface (API) functions for the establishment of connections and data exchange,
- DNS to resolve host names to IP addresses and vice versa,
- IP address selection and caching/storage of addresses,
- Multicast applications, depending on situation; correspondence of IPv4 and IPv6 multicast addresses and selection of correct socket configuration options.

The optimal approach is to make all applications independent of the version of IP that is used. This means that the source code should not have any IP dependencies and the communication library should provide APIs without IP dependencies. Many popular Internet applications have support for IPv6, this includes web-browsers such as Google Chrome, Internet Explorer, Mozilla Firefox; Apache Web Server; and so on. Applications such as Apple Mail and Microsoft Outlook Windows Live Mail also have IPv6 support [18]. For a more extensive list of popular Internet applications with support for IPv6 please refer to appendix II.

6.1.3 IPv6-Ready Hardware

When investigating how much of the consumer home network gear which has IPv6 support it is sad to find that IPv6 support lags far behind enterprise equipment and operating systems. Experts say that a lot of the products that are supposed to run IPv6 are full of implementation bugs [19]. However, a positive view of this is that many equipment vendors are aware of this and they are trying to fix their software as fast as they can.

There is a large number of network-related products that claim to be “IPv6 Ready”. One might think that this means that these products fully support IPv6 and that once you install them in your IPv6-network that IPv6 should run smoothly. Unfortunately, this is *not* the case. The term “IPv6 Ready” is used much like the term “HD-ready” was used in the early stages of HD-TV. It is commonly known that HD-ready is not the same thing as full HD, and in the same manner, IPv6 Ready is not the same thing as fully supporting IPv6.

If you purchase an IPv4 firewall you do not have to worry about whether it supports services such as DNS or not because you know it will. As of autumn 2010, there are no firewalls that support IPv6 in the same way that you would expect an IPv4 firewall to support IPv4 [20]. The “IPv6 Ready” logotype (shown in Figure 6-1 IPv6 Ready Logo (Provided by IPv6ready.org)) is owned by the IPv6 forum group — which is endorsed by the EU-commission.

Figure 6-1 IPv6 Ready Logo (Provided by IPv6ready.org)

The website ipv6ready.org offers a search-tool where you can look for products that are IPv6 Ready. There you will find that there are a lot of products that supports the core protocol, which is often referred to as Phase-1. However, only a small fraction of these devices support Phase-2-services, such as DNS and DHCPv6.

It is relatively easy to find a firewall that supports Phase-1, but if you are looking for Phase-2 support in your firewall, then you might as well stop looking. It is currently impossible to find a firewall that supports all of the functions for IPv6 that you might need. This requires complementary services outside of the firewall a must.

It is also difficult to know what routers to choose. Even if a router is Phase-1-certified it might still not work with your ISP, as your router might not be compatible with your ISP’s tunneling-mechanisms. In order to find out what router is most suitable for you it is advisable to contact your ISP and ask them answer which router suits your needs best. ISPs who offer IPv6 are aware of this and expect that through 2012 they will have to address this matter by providing customers with lists of tested products and configuration instructions. We tried to find such a list provided by an ISP but were unsuccessful in doing so. However, information about IPv6 compatible products and applications can be found on a variety of sites, including https://www.ipv6ready.org/db/index.php/public/ and http://www.ipv6-to-standard.org/.

Even though equipment vendors may be working on providing more and better products with support for IPv6, time is starting to run out. If we want the transition to IPv6 to happen as quick and smooth as possible, there must be suitable hardware and software to support this transition. Unfortunately, this is not the case today, thus giving both users and ISP even more of an incentive to continue to use NATs to prolong this transition.

7 Disadvantages of IPv6 compared to IPv4

The main advantage of IPv4 over IPv6 is that it is well proven and we know what to expect of it. The biggest disadvantage is that we actually need to make a large change in order to shift to IPv6, as a result the transition from IPv4 to IPv6 is most likely going to take a long time and require a lot of effort and resources, which is not seen as a very positive thing in the eyes of many. There is also a problem with the lack of applications and services that are currently available over IPv6. Very few new services have been developed as there are few users in the IPv6 Internet; hence without users there is no incentive for developers to write applications or service providers to implement services.

It is also important to remember that IPv6 still has flaws that need to be addressed in order for the protocol to work as it was intended when it was designed. One noticeable disadvantage is that it is much harder to remember IPv6 addresses. While IPv4 addresses are relatively easy to remember because they are only 32-bits in length (hence leading to at most 12 decimal digits that you must remember), as we migrate to IPv6 this will be increasingly difficult because of the 128-bit address field (which could lead to a maximum of 32 hex digits that must be remembered).

There is also no clear plan for how this transition is supposed to actually take place. While recent versions of all major operating systems have support for IPv6, it is less clear how ISPs should make the transition. The degree of backwards-compatibility is limited between the two protocols and if we continue to use up all of the limited number of unallocated addresses as quickly as we are, there is soon going to be very little time left for an orderly transition. While it is unlikely that the transition will end in chaos, it is quite conceivable that the transition will require a lot of painful, and possibly buggy, workarounds. Hopefully most of this will be handled “behind the curtains” so that the average end user will be affected as little as possible. Still, as the complexity of the transition increases, so will the risk of end users being affected.

8 IPv6 transition

There are a number of different transition mechanisms that could be used. This chapter begins with a review of these mechanisms and then examines the transition process. The chapter concludes with some suggestions of how to prepare for and successfully carry out a transition to IPv6.

8.1 *Transition Mechanisms*

The change from IPv6 to IPv4 cannot, and will not, happen overnight. It will take a long time before all organizations, corporations, governments, private end-users, etc. have shifted to IPv6; hence both protocols will have to be run simultaneously. In order to run both IPv4 and IPv6 at the same time, different technologies called transition mechanisms are going to have to be used. These technologies allow hosts connected only via IPv4 or IPv6 to reach content available only using the other protocol.

These transition mechanisms can be classified into two large groups: tunneling mechanisms and dual stack. Running a dual stack allows IPv4 and IPv6 to coexist in a host (or other node) and enables concurrent communication with IPv4-only or IPv6-only nodes. Tunneling is a set of methods that allows IPv6 islands, or single nodes, to communicate over an IPv4 network. There are several types of tunneling:

- (manually) configured tunneling
- automatic tunneling
  - IPv4 compatible IPv6 (deprecated)
  - IPv6 over IPv4 (deprecated)
  - IPv6 to IPv4
  - 6rd
  - ISATAP
  - Teredo
  - Tunnel Broker

8.1.1 Dual IP-Layer

A dual stack (illustrated in Figure 8-1 Dual stack (Adapted from figured provided by www.ntt.net)) makes it possible to combine implementations of both IPv6 and IPv4 protocols. This means a full implementation can support both protocols. A node with this capability is often referred to as an IPv6/IPv4 node. When communicating with an IPv4 node it behaves as an IPv4-only node and when communicating with an IPv6 node it behaves as an IPv6-only node. Every IPv6/IPv4 node has at least one IPv6 address and at least one IPv4 address. Both end nodes and routers run both protocols and the IPv6 protocol is preferred when possible. When a dual stack client wants to connect to a server two requests are sent to the DNS asking for IPv4- and IPv6 addresses for this server. Most DNS servers support both IPv6 and IPv4 requests. If the DNS sends back both an IPv4 and IPv6 address it is up to the client to decide whether to use one or the other address in order to connect to the server. Generally the host picks the IPv6 destination address by default.

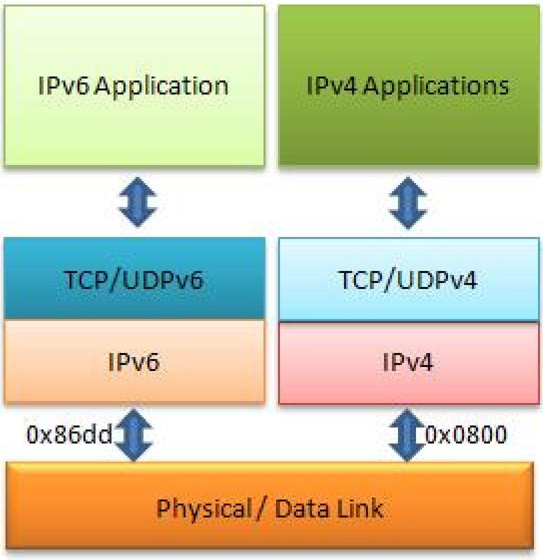


Figure 8-1 Dual stack (Adapted from figured provided by www.ntt.net)

One of the problems with a dual-stack is that you need to perform a full network upgrade to run the two different protocol stacks. All the routing protocols need to be configured for both protocols. This can in some cases, depending on the operating system in use, require using two different commands and it requires more memory and CPU power ([12] , page 255).

One of the strategies to implement a dual stack is to make the transition from the core to the edge. This means that you first enable both IP protocols stacks on the network's core routers, then on the edge routers and firewalls, then on server cluster routers and finally on the home access routers.

A dual stack is a key function in the transition to IPv6, because IPv6 nodes and routers will have to be able to interoperate with IPv4 hosts and use IPv4 routing for a long time to come. Additionally, this is a very flexible method and when we do not need the IPv4 nodes anymore the IPv4 stack can easily be disabled or removed ([12] , pages 255-256).

8.1.2 Tunneling

Some of the tunneling techniques have grown old and more modern techniques have been introduced, hence these old techniques have been deprecated.

8.1.3 Manual Tunneling

This method allows IPv6 traffic to be carried over IPv4 networks. However, the tunnel's destination address is determined by the tunnel's configuration to create a peer-to-peer (P2P) topology. The tunnel will appear to be a single hop for the IPv6 packets; however, the IPv4 packet which encapsulates the IPv6 packets may make several hops. This technique is simple to deploy and is available on most platforms. The drawback of this approach is that each tunnel needs to be manually configured, thus it is not suitable for large-scale tunneling and should only be used for permanent links [21]. If changes are made to the network, then the manually configured tunnel will not change — hence this approach has a rather high maintenance cost.

8.1.4 6to4

The 6to4 tunneling mechanism allows IPv6 sites to communicate with each other over an IPv4 network without explicitly setting up a tunnel. This is often the method of choice for users who wish to connect to the IPv6 Internet using an IPv4 connection.

The IPv6 sites communicate with each via 6to4 routers, which also are called 6to4 gateways. It is important to note that only the gateway needs to be configured to support 6to4 and no changes need to be made to the hosts within the 6to4 network. This is possible because the IPv6 packets are encapsulated in IPv4 packets at the 6to4 gateway and not at the host. There must be a minimum of at least one globally unique IPv4 unicast address available to the 6to4 gateway in order for this configuration to work.

If a node in the 6to4 network wishes to communicate with a node in a different 6to4 network there is no extra tunnel configuration required. The tunnel entry point takes the IPv4 address of the tunnel exit point from the IPv6 address of the destination. However, if the node wishes to communicate with a node in the IPv6 Internet, a 6to4 relay router is needed. This is a router which is configured for both 6to4 and IPv6 and it connects your IPv6 network to the IPv6 Internet.

Figure 8-2 A 6to4 Network and how the components play together. (Adapted from figured provided by “IPv6 Essentials”, Siliva Hagen) shows a hypothetical 6to4 network with various communication paths. Host A and B can communicate within site 1 using IPv6. In order to communicate with host C at site 2, the IPv6 packets are sent to router R1. At R1 the IPv6 packets are encapsulated in IPv4 and forwarded to router R2 at site 2. R1 has learned the IPv4 address of R2 from the IPv6 destination address. R2 decapsulates the packet and forwards it to Host C. To communicate with Host D, any of the others hosts sends their packets to their 6to4 router which encapsulates the packet and forwards it to the R3 6to4 relay router. This relay router decapsulates the packets and forwards the original IPv6 packet to Host D ([12] , pages 264-265).

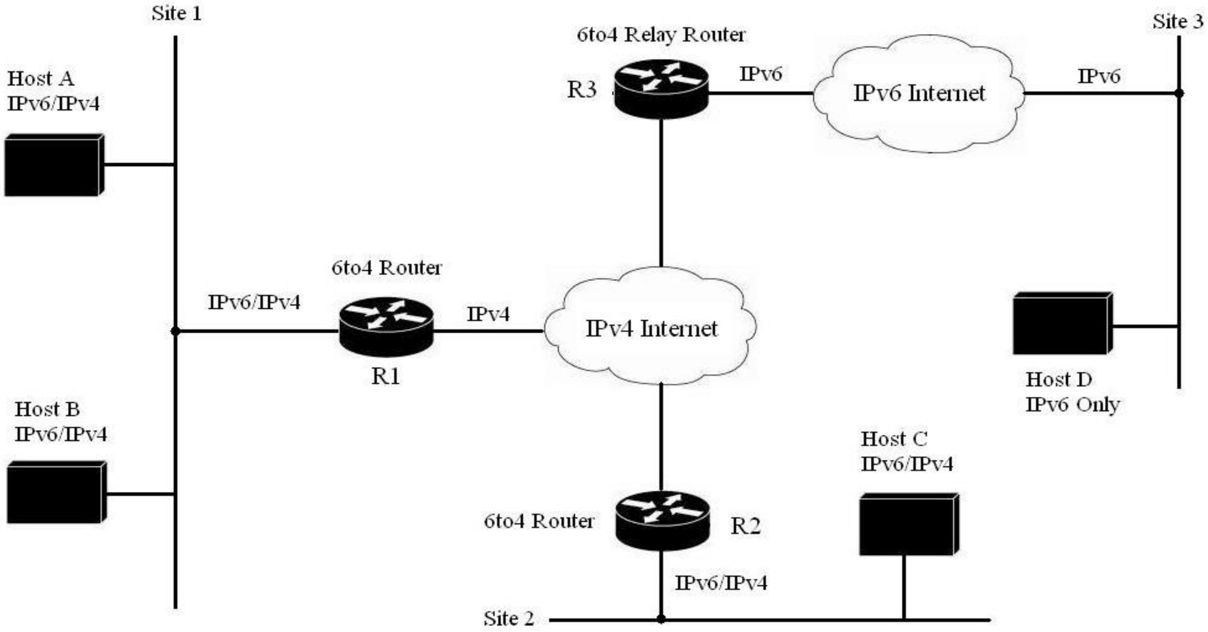


Figure 8-2 A 6to4 Network and how the components play together. (Adapted from figured provided by “IPv6 Essentials”, Siliva Hagen)

Hurricane Electrics is the world’s most interconnected IPv6 network and provides a global 6to4 relay service, as well as a relay service for Teredo (see section 8.1.7). According to Hurricane Electrics, their IPv6 traffic doubled in 2009 thanks to the free IPv6 tunnel broker that they opened in April 2009 [22].

8.1.5 6rd

IPv6 rapid deployment (6rd) is another technique to deploy IPv6 connectivity as an overlay on the underlying IPv4 infrastructure. It is an improvement of 6to4 with the major difference that it solely operates within an ISP's network.

In 6to4, the native IPv6 hosts need access to a 6to4 relay server which uses a common IPv6 prefix in order to communicate with the 6to4 hosts. There is no guarantee, however, that the native IPv6 hosts have a route to such a relay. This is no longer an obstacle in 6rd as the ISP uses one of its own prefixes and does not require a relay server to be used since everything is taken care of within the ISP's network. This guarantees that *all* 6rd hosts can be reached by native IPv6 hosts [23]. However, this technique requires that the end-users' routers support 6rd and the encapsulation process.

8.1.6 ISATAP

The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) enables connectivity for dual-stack nodes in an IPv4 network. ISATAP can encapsulate and transmit both IPv6 and IPv4 packets over an IPv4 network. It is specifically targeted for IPv6 deployment in large enterprises [22].

ISATAP creates an overlay on the IPv4 network making it possible for dual-stack nodes to automatically tunnel between each other. There is no need for global or private IPv4 addresses in order for this tunneling method to work.

If the IPv6 hosts within the site network wishes to communicate with IPv6 hosts on the Internet a configured boarder router is needed ([12] , pages 266-267).

8.1.7 Teredo

Teredo was designed in order to make IPv6 available to hosts who reside behind one or several layers of NAT devices.NAT devices are very common in the Internet today, especially for home users accessing the Internet. There are two major drawbacks with NATS when utilizing IPv6 tunneling over IPv4 networks:

1. NAT users have a *private* IPv4 address
2. NATs usually have many different filters enabled which prohibits forwarding of many types of payloads

Mechanisms such as 6to4 often fail when being routed through NATs because of the need for a public IPv4 address. There are ways to avoid this problem, but it requires a 6to4 router to be run in the same device as the NAT. In the future we will no longer need NATs because of the large number of available addresses that IPv6 offers, bur for the duration of the transition we are still going to need them. Developers are therefore working on methods that allow connectivity for users behind NATs. Teredo is one of these methods. However, its design adds some overhead that could be avoided if more direct access to the Internet were available ([12] , pages 267-270).

8.1.8 Tunnel Broker

Tunnel Brokers are virtual IPv6 providers. They offer IPv6 Internet connectivity to users who already have an IPv4 connection to the Internet. If a user wants IPv6 connectivity they register with the Tunnel Broker who manages the establishment, maintenance, and deletion of a tunnel for this user ([12] , page 27). Since 2009, Hurricane Electrics has offered a free IPv6 Tunnel Broker services on their website www.tunnelbroker.net .

8.1.9 Implementation cases

In this section we will examine a number of cases of users transitioning to IPv6.

8.1.9.1 Dual-stack

Company: Betchel
Industry: Construction

In 2005, Betchel[1] started to upgrade their Internet infrastructure to IPv6 in collaboration with Cisco and Microsoft. They used Cisco hardware and Microsoft software to perform the transition. The transition process was planned in 3 steps: go from IPv4 only to IPv6 capable, go to IPv6 dominant, and finally go to only IPv6. The method used was Dual-stack. As of June 2007, Betchel had succeeded in having over 20% of their servers and clients running IPv6. Regarding the process of migrating to IPv6 Betchel is so far happy with the results even though much work remains to be done. They managed to migrate without interrupting the activities of their end users. [24]

8.1.9.2 6rd

Company: Free
Industry: ISP

A rapid deployment of IPv6 was implemented by FREE (a French ISP) in 2007. In only 5 weeks they succeeded in delivering IPv6 to over 1,500,000 customers. If the customer had an IPv6-capable host they only needed to activate IPv6 in their Freebox home-gateway (the customer premises equipment provided by the ISP).

The deployment was completed in a few steps. First they obtained an IPv6 prefix from their regional Internet registry (RIR). Second they added 6rd software support to their Freebox home-gateway. Third they provisioned a PC - platform with 6to4 gateway software. After that they tested the functionality and operation using different operating systems and applications. Finally they finished the operational deployment with the help of the new downloadable software version for their Freeboxes.

If IPS provide customers with IPv6 free of charge (i.e., as part of the customer’s Internet connectivity) there will be a potential market for developers and companies to create services and applications that can be accessed over IPv6. This could trigger the demand for IPv6 among end users.[25]

8.1.9.3 The Swedish government

Post och Telesstyrelsen (PTS) are investigating the transition to IPv6. Their goal is to produce a manual for how IPv6 can be introduced in government and other public organizations in terms of accessibility, safety, and economy. Their report is going to contain concrete descriptions of how the agencies should practically and technically proceed to make e-services available. In 2010, E-deligationen presented a comprehensive guide about how the transition to IPv6 should be made by the government authorities in Sweden. [26]

We tried to contact Anna-Karin Hatt (IT and Regional Minister) to interview her regarding this topic, but were referred to their homepage for more information. They have started to plan for the deployment of IPv6, but there are still some uncertainties about when it is going to happen. Whether it is going to be this year or next, we will have to wait and see.

[1] Betchel is a global enterprise leader in engineering, construction, and project management.

8.2 *Transition phase*

Two of the key questions in planning a transition from IPv4 to IPv6 are: (1) What is the benefit? (2) When is it worthwhile to make the transition? The following subsections will give some example of answers to these questions.

8.2.1 Situations where corporate and private person benefit from IPv6

In what situations do corporate and private persons benefit from using IPv6? We will consider this for general government networking, public safety, end-to-end communication, vehicles, and corporate networks. These situations and descriptions are based on [27].

Government
A government network must be able to provide services to internal clients as well as private citizens. Example of services include: voting, filing tax declarations, and other applications. Using IPv6 (and avoiding NATs) makes it possible to provide safe and secure e-government services.

Public Safety
Organizations dealing with public safety could use broadband IP based communication in their daily work. Two major benefits from using IPv6 is auto-configuration and improved mobility. Together these two facilitate rapid deployment of communication networks when there are natural disasters or major accidents.

End-to-end communication
With increased usage of mobile devices people expect to be able to access to their corporation’s network and/or work from a remote location. Mobile IPv6 can be used to provide direct end-to-end communication between peers while avoiding triangular routing via a mobility anchor point, thus reducing delays and costs.

Vehicle communication
Increasingly vehicles not only have a network within the vehicle, bur increasingly vehicles can communicate with each other and with road-side infrastructure. For example, the vehicle can send sensor data to the car manufacturer to determine if maintenance should be performed *before* there is a fault or failure. IPv6 necessary as each vehicle will need to have at least one IP address and a mobile vehicle will change where it attaches to the Internet.

Corporate networks
Because of the shortage of IP addresses in IPv4 corporate networks need IPv6 to evolve from border-protected groups of in-house resources to an extended enterprise with wide communications infrastructure.

8.2.2 General incentives for enterprises

IPv6 is here to stay and if enterprises have not yet started to plan their transition into IPv6, they had better start. Planning for IPv6 is important because it has a fundamental impact on how the enterprise connects to the rest of the world. It affects everything from desktops, to phones, to laptops, to hardware and software. In other words, IPv6 will have direct affects on everything that the enterprise does on a daily basis.

Enterprises should be asking themselves how a proof of concept of transition should be done. How will the IT personnel be trained in the new protocol? How much will it cost? What benefits or drawbacks are there? From the enterprise’s infrastructural perspective, IPv6 is likely to dominate planning meetings and budgets for the next couple of years.

IPv6 offers significant opportunities for companies with original and innovative business models to realize these models. The main advantage is the possibility to embed IPv6-addresses in almost everything; from dishwashers to cars and houses. IPv6 will enable a new generation of applications and appliances exploiting enhanced support for machine-to-machine communications, as well as human-to-machine communications. Improvements in these areas will result in major improvements in operational automation and productivity for the connected enterprise [28].

Enterprises will be able to benefits from transitioning into IPv6 because of its improvements in routing, security, and auto-configuration. Enterprises will also find that IPv6 networks will lower costs for deployment, maintenance, and day-to day operations. This will eventually lead to large savings for the company in the long run.

However, the transition to IPv6 will cause some short term implementation expenditures and lead to some difficult challenges. Investments may be needed in order to upgrade the existing network infrastructure, as well as requiring investments for staff training and system enhancements.

8.2.3 Benefits for the connected enterprises

Some ways in which IPv6 can reduce internal enterprise IT and networking operational costs are [28]:

- Investing in IPv6-enabled software and hardware is seen as a secure investment because the entire world is moving towards using IPv6. In contrast, investing in IPv4-only software and hardware may lead to additional expenditures.
- NAT devices will no longer need to be deployed and maintained, thus eliminating the capital and operating costs associated with NATs.
- IPv6 eliminates the need for private addresses, because the abundance of addresses will enable devices to have and retain a globally routable IP address. When using private IP-addresses conflicts can occur when companies merge because companies have used the same block of private IP addresses. This consequently leads to hidden costs in a merger and acquisition transaction because the issue of overlapping and duplicate addresses needs to be resolved. This will no longer be an issue, thus simplifying IT and network policies.
- The enterprise’s carbon footprint can be reduced by taking advantage of IPv6-enabled multimedia services to minimize the need for travel.
- Auto-configuration will reduce network management costs.
- “The Internet of things” is considered to be an important value proposition due to the ability to connect everyday devices to the Internet with each device having its own individual IP address. It has been speculated that the Internet of things could lead to one of the largest transformations of human civilization, perhaps even greater than the industrial revolution.
- There is basically an unbound market space for machine-to-machine communications because of the abundance of addresses. This will result in a paradigm shift for the telecommunication sector and huge effects on other industries.

8.2.4 World IPv6 Day

The World IPv6 day will be held on the 8th of June 2011. Participating companies (including Google, Yahoo!, and Limelight Networks) will be distributing their content over IPv6 for a 24 hour “test flight”. The goal for this test flight is to motivate other companies to enable their services over IPv6, leading to a successful global transition to IPv6.

8.2.5 IPv6 in industries

Two major industries that are expected to be radically changed by the transition to Ipv6 are the automotive industry and medicine. In both cases there are advantages to connecting devices to the Internet (both for reasons of cost savings and for improved services). The following subsections describe in more detail these industry's opportunities when using IPv6.

8.2.5.1 Auto Industry

An increasing number of automobile manufacturers are integrating solutions into their vehicles for maintaining connectivity while on the move. More and motorists are demanding support for e-mail, entertainment, browsing, navigation, and dynamic traffic-congestion updates. IPv6 can be used to make all of this possible on a large scale, thus initiating the era of smart transportation, or the era of Intelligent Transport Systems (ITS).

ITS is an initiative taken by Europe, China, the US, and Japan to reduce traffic congestion in order to lower fuel consumption, as well as reduce air and noise pollution caused by vehicles. Vehicles would be equipped with a set of sensors that transmit data such as the vehicle's speed, direction, and outside air temperature to a control center which analyzes this data and sends back optimized plans for the vehicle to use in order to increase its efficiency. Embedding IPv6 technology in vehicles could also provide a framework for new serial numbers. Today American car manufacturers are working on implementing features such as theft recovery, driver monitoring, and system tracking to learn where the vehicle is, how the driver is acting, and estimating when the vehicle needs maintenance. An example of such a system has already been implemented in China with taxis being equipped with sensors to monitor outside air temperature and rainfall. This enables taxi dispatchers to know when to send extra taxis to areas with unpleasant weather.

However, vehicles communicating with an owner/operator/dispatcher are not the only possible approaches, as different parts of the same vehicle might exchange data; two different vehicles could warning each other about road jams; roadside sensors could warn the driver if the velocity is too high for an upcoming turn; and so on. In order for all of this to work, each vehicle might need several hundreds of IP addresses making IPv6 a requirement [29].

8.2.5.2 Medical industry

Another industry that can leverage the large numbers of newly available IP addresses is the medical industry. A biosensor is a small device which can be used to transmit biological data over a wired or wireless network. This data can be used in many ways, but one of the major areas of use is in personalized medicine and real-time monitoring of patients. In order for this communication to be possible, the biosensors need to have direct access to the Internet (or they need to go through a gateway). These sensors can only be made directly addressable with the help of the large pool of IPv6 addresses. The alternative, communicating through gateways leads to problems of privacy, loss of personal integrity, and increased overhead & delay.

Using biosensors medical professionals can monitor the patient's biological data in real-time without needing to be located right next to the patient. Biosensors connected to the Internet make it possible for specialists all around the world to analyze the data. With a constant flow of data from the patients, specialists will be able to take proactive measures instead of simply reacting to problems.

Another requirement for this is high-speed networks, which IPv6 supports. IPv6 has been tested to reach speeds of as high as 40 Gbps which is necessary for real-time monitoring of the aggregated data from a very large number of patients. Another feature that makes IPv6 suitable for this purpose is the built-in security mechanisms that can be used to provide confidentiality and authentication of the sensor data [30].

8.2.6 The Internet of things

The only thing limiting the future growth of IPv6 Internet-enabled devices and appliances is our imagination. Uses of IPv6 can be found in the most unexpected places. We have already seen examples of taxis being equipped with IPv6-enabled sensors, but what about microwaves, cattle at a ranch, or even an entire house? Some of these examples have already becoming reality in Japan. Some microwaves are able to download new software updates and cattle have been equipped with sensors to measure body temperature for breeding purposes. In 2005, the Toyota Dream House was built as an experimental intelligent home embedded with network computing technologies. The house can, amongst other things, adjust the climate in the house based on the present occupants in it.

Another example can be found in a convenient store in Japan where IPv6 technology is used to send advertisements and updates to the mobile devices used by both customers and employees.

Other applications of IPv6-enabled technology:

- Logistics and transportation (smart packages, container tracking, container monitoring, …)
- Smart grids and energy control systems
- Animal tracking and precision agriculture

8.3 *How to prepare*

Key requirements for successful IPv6 implementation are leadership, skills, and collaborations [31]. The starting point should be in determining a company-wide implementation strategy. It is inadvisable to implement IPv6 in one segment of the company at a time, since competences and organizational assets cannot be leveraged effectively. A phased transition is optimal because it reduces incremental costs and decreases risk. After a strategy has been decided, then the company should perform a gap analysis to determine the internal impediments regarding IPv6 deployment. This analysis should also include estimated costs and a timeframe for removing these impediments.

The following sections describe some of the actions enterprises can take in order to prepare for the transition.

8.3.1 The Janoz-Method

Jan Östling (Cisco Systems) provided us with information about the “The-Janoz” method used by Cisco System’s in their daily work. The general idea of this method is to facilitate a discussion between costumers and Cisco regarding how to enable IPv6 on the customer’s network(s). Instead of using complicated terms, the “Janoz-method” simplifies the description of the transition process to a basic level enabling better understanding of what actually needs to be done. The method is based on a general model of how most organizations networks are currently configured.

In Appendix II the Janoz method is implemented in several different types of situations, each of which requires a different implementation strategy.

What makes this method so effective is its simplicity. If you are trying to help a costumer to transitioning to IPv6 it is important to keep the process simple so that you can understand what the customer is asking for and then you can provide the customer with what they actually need [11].

8.3.2 Product lifecycle replacement

One way for enterprises to reduce IPv6 migration costs is to add it into the planned product procurements of their existing technology budget. If the IT-staff upgrades their equipment to equipment that already supports IPv6 by default, then they can gradually implementing the IPv6 in their network.

8.3.3 IPv6 in requests for proposals

In addition to adding IPv6 support as a requirement in their upcoming core network procurements, enterprises can further accelerate IPv6 adoption by demanding support for IPv6 in their IT requests for proposals. Including IPv6 procurement planning and training into the enterprise’s planned and existing IT processes will result in a more moderate transition cost (and effort). By doing this the enterprise has more time to adapt to the new protocol, which should limit the number of mistakes that otherwise could occur if the transition is rushed, potentially avoiding unexpected and unnecessary costs.

8.3.4 IPv6 training

Enterprises should try to include IPv6 training costs into their IT budget. Training costs might in some cases be very high; hence enterprises can avoid high unexpected costs by spreading these costs out over time. This will lead to a smoother and more secure transition. However, is important to remember that IPv6 is, and needs to be treated as, an entirely new protocol that will require training and workshops in order for IT-personnel to become familiar with it.

9 IPv6 and Sweden

This chapter will examine the state of knowledge about IPv6 in Sweden today. The chapter begins by looking at IPv6 in the largest ISP, the goes on to look at IPv6 in a large housing association. Following this we examine the knowledge of IPv6 in a company providing networking equipment and in a company buying and using network equipment and services. The chapter ends with the description of a survey conducted of private persons regarding their knowledge of IPv6.

9.1 *TeliaSonera*

An essential element of the adoption and use IPv6 in Sweden is whether ISPs can provide IPv6 connectivity to their customers. We focused on one of Sweden's largest ISPs, TeliaSonera, to see what their strategy is for adopting IPv6. TeliaSonera was allocated a /20 block of IPv6 addresses in May 2004. We interviewed Leif Bengtsson, Vice President of Product Development TV at Telia Sonera, regarding TeliaSonera's IPv6 status. He said they had several ongoing IPv6 projects. Telia Sonera recognize that IPv6 is the networking protocol of the future and they need to start working on making applications and services available for IPv6 to promote the further success of Internet (and their own success as an ISP). According to TeliaSonera's customer service today they offer IPv6 to specific business clients and are planning to IPv6 to private end-users after summer 2011. However, this last statement could not be confirmed by Leif Bengtsson [32].

TeliaSonera has several ongoing IPv6 projects, and they are trying to resolve what other applications might needing IPv6. Today Telia does not have a complete plan to move to IPv6, but they are definitely looking at a number of different solutions. Their aim is to create and deploy new IPv6 applications as quickly as possible. Whether NATs create a problem for TeliaSonera's current applications seems to only be a problem when the client does not have the right equipment installed.

At the moment TeliaSonera is working on different solutions to the upcoming shortage of IPv4 addresses. One solution is to reorganize the distribution of IPv4 addresses to hosts. They will try to use NAT where it is possible in order to save IPv4 addresses. They do recognize that this is just a short term solution and this is increasing the incentive to move to IPv6 as soon as possible for TeliaSonera.

The biggest reason for enabling IPv6 in their network is the risk that all their existing and new mobile customers will start using smartphones. This will probably be a problem for **all** mobile operators as they will need to allocate IP addresses to **all** their users. However, there are not addresses for all of the mobile operators to allocate public IPv4 addresses to their customers; potentially this means that the operators will be unable to signup new subscribers who wish to use a smartphone. This makes IPv6 very important for ISPs that want to have smartphone users as their customers.

There is still a problem due to the lack of demand for IPv6 by customers, mainly due to the lack of attractive IPv6 applications and because Sweden is not, at the moment, affected by the shortage of IP addresses. However, TeliaSonera is aware of these facts and are trying to create applications that will generate demand for IPv6 by their customers. Additionally, it is clear that ISPs need to start offering IPv6 solutions because it is inevitable that the existing pool of available IPv4 addresses will be exhausted.

Some details of the plans for TeliaSonera's deployment of IPv6 in Finland are described in a thesis by Tero Maaniemi [39].

9.2 *HSB- Hyresgästernas sparkasse- och byggnadsförening*

One of our objectives was to influence large cooperatives that alone could force the rapid adoption of IPv6. We contacted HSB, Sweden's largest housing cooperative with over 500 000 tenants, for an interview regarding whether they had start thinking about migrating to IPv6. The main reason for pursuing this interview was to see if there was an interest by HSB.

The HSB networking planning is outsourced to Tieto [33] and employees are not allowed to talk about ongoing projects with customers due to company policies. However, when ask what their general plans for introducing IPv6 to customers was their answer was: Yes we are planning a couple of transition strategies for customers but we cannot discuss it any further. One of the problems highlighted during the investigation is that HSB is divided into 31 regional associations. Each regional association has to decide for themselves if they want to adopt and start using IPv6.

We learned that in general companies are starting to take an interest in adopting IPv6, but they are generally still in the planning phase.

9.3 *Cisco Systems*

We conducted an interview with Jan Östling [11], a System Engineer at Cisco, to examine the current situation of IPv6 from the perspective of a network equipment vendor and to examine whether they had any ongoing IPv6 projects with customers. The goal of this interview was to talk to an expert to see how Cisco as a company might facilitate the introduction of IPv6 to customers. First and foremost IPv6 and IPv4 create two totally separated Internets. IPv6 adds a number of new functionalities as compared to IPv4. This makes the transition even more complex because you need to implement a whole lot of new features.

Some of the features in IPv6 still do not work satisfactorily. Jan specifically mention SLAAC. The problem with SLAAC is that it was designed without considering the need for networks parameters other than an IP address (e.g. DNS server address). This is a problem, because at the moment SLAAC only supports allocation of an IP Address and nothing more, hence some other protocol is required to configure these other parameters.

According to Jan, the companies who will be leading the change to IPv6 will be the telephone operators. This is because they are in the most need for new IP addresses in order to provide Internet connectivity to their smartphone subscribers. Every smart phone needs at least one IP address, hence this leads to a major problem for operators who wish to add new subscribers because their pool of IPv4 addresses is running out.

Additionally, he also indicated that compelling new applications are needed to motivate the migration. Today's IPv6 bottleneck is due to the vicious circle of no enterprises deploying IPv6 services or applications because there are no customers and the customers do not use IPv6 because there are no applications or services. The current solution requires providing services via both protocols at the same time for some period of time. Today only a few companies, such as Telia and Google [40], provide their services via both IPv6 and IPv4.

There is a large interest in IPv6 among Cisco's customers. Many companies are starting to plan for the new protocol. Mostly they are interested in how the transition to IPv6 is going to affect them. According to Jan we will definitely see more and more companies moving to IPv6 in the near future.

9.4 *Forsen Projekt*

We interviewed Simon Edström, IT, Telecom, and Security Manager of Forsen Projekt a construction consulting company, to find out how they are planning for the migration to IPv6. We wanted to see what companies do in order to prepare for IPv6 and to understand why they might be waiting.

What Forsen has done so far is that they have investigated their current IT situation. They have educated their IT-staff and looked at what equipment needs to be changed in order make the transition. Their plan is to start to migrate while using IPv4 and IPv6 at the same time. According to Simon, the problem with IPv6 today is that there are not many services supporting IPv6 right now. Forsen sees a big incentive to change because it brings new possibilities to increase the efficiency of their communications and can create new features for their business.

Simon thinks that it is important for Forsen to be at the forefront in IT technology in order to be able to meet the technical requirements from their customers and projects. They focus on trying new techniques to improve their services and to be more effective in their daily business. However, Simon knows by experience that it is dangerous to jump on the train too early— because of the risk of infancy problems. This does not mean that Forsen will not support IPv6 in the future only that they want to be sure that the new protocol works to their satisfaction *before* implementing

Regarding when they are going to migrate they are consciously waiting and will make their transition one step at the time, but they definitely consider that a transition to IPv6 is inevitable and that IPv6 represents the future Internet [34].

9.5 *IPv6 survey*

We conducted a survey among ordinary Internet users to find out what they knew about IP addresses and IPv6. By ordinary Internet users, we are referring to users using the Internet for social media, banking, mail, school, and work. The aim of the survey was to investigate what people actually know about IPv6 and to find out if there was anyone asking for it. This survey does not reflect the general awareness of IPv6 in Sweden, as it was only used to see if some people were aware of the new protocol at all. The participants were randomly selected without regard to age or gender. The survey was Internet-based and distributed via www.facebook.com and www.wearestudents.se as we expected that the number of respondents would we large due to the large use of social media.

9.5.1 Hypothesis

We think that the average person's knowledge about IP addresses should be a lot higher than knowledge of IPv6 in Sweden. We expect that the majority of the participants do not know what IPv6 is and that this could reflect the demand for IPv6 in Sweden.

9.5.2 Results

As of the 29th of April 2011, a total of 182 participants completed the survey. Of these there were 72 female participants and 110 male participants. The ages ranged from the youngest participants with an age of 15-20 years to the oldest at the age of 61. Figure 9-1 Total respondents knowledge about IPv6 (IPv6 Survey) shows that 27% of the respondents know what IPv6 is, but that 73% did **not** know what IPv6 is. Further results are shown in Appendix I.

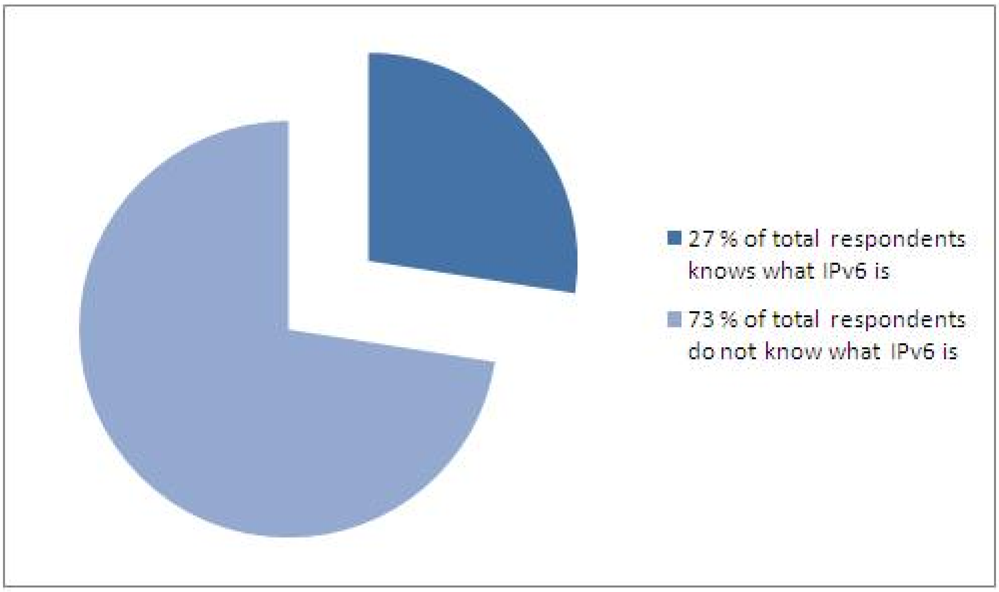


Figure 9-1 Total respondents knowledge about IPv6 (IPv6 Survey)

9.5.3 Confounding factors

Since the survey was distributed through social media, the conclusions could be questioned since we could not verify the participant's background, interest, or education. These factors could have affected the results, but as we did not aim to get an exact measure we think that this approximation fits the purpose of the survey.

9.5.4 Conclusions

According to the survey the knowledge about IPv6 is moderate with only about 30% of the respondents knowing what IPv6 is, while roughly 75% of respondents did know about IPv4 addresses. This could be because we are not yet affected by a shortage of IP addresses and that the current IPv4 Internet works to our satisfaction. However, it reflects the poor flow of information about IPv6 via the media. These results could indicate one of the bottlenecks further delaying the adoption of IPv6.

9.6 *IPv6 statistics*

IPv6 is still in its infancy, but adoption is growing day by day. However, as of March 2010 only 1% of the Internet traffic was IPv6 based, with roughly 90% of the IPv6 traffic native IPv6 and 10% through tunnels [35].

9.6.1 Current global IPv6 statistics

RIPE has made available some statistics about current IPv6 usage. Figure 9-2 Graph showing the progress of IPv6-enabled ASes in all countries, Sweden and the United States. (Provided by RIPE NCCshows the growth in the global number of AS supporting IPv6. As of XX XXX 2011 some of these statistics are:

Percentage of Top Level Domains with IPv6 name servers: 83.7%

Percentage of registered domains with both A and AAAA records: 1.21%

Percentage of ASes in the world (IPv4 or IPv6) running IPv6: 9.9%

Percentage of ASes in Sweden (IPv4 or IPv6) running IPv6: 22.9%

Percentage of ASes in the United States (IPv4 or IPv6) running IPv6: 6.44%

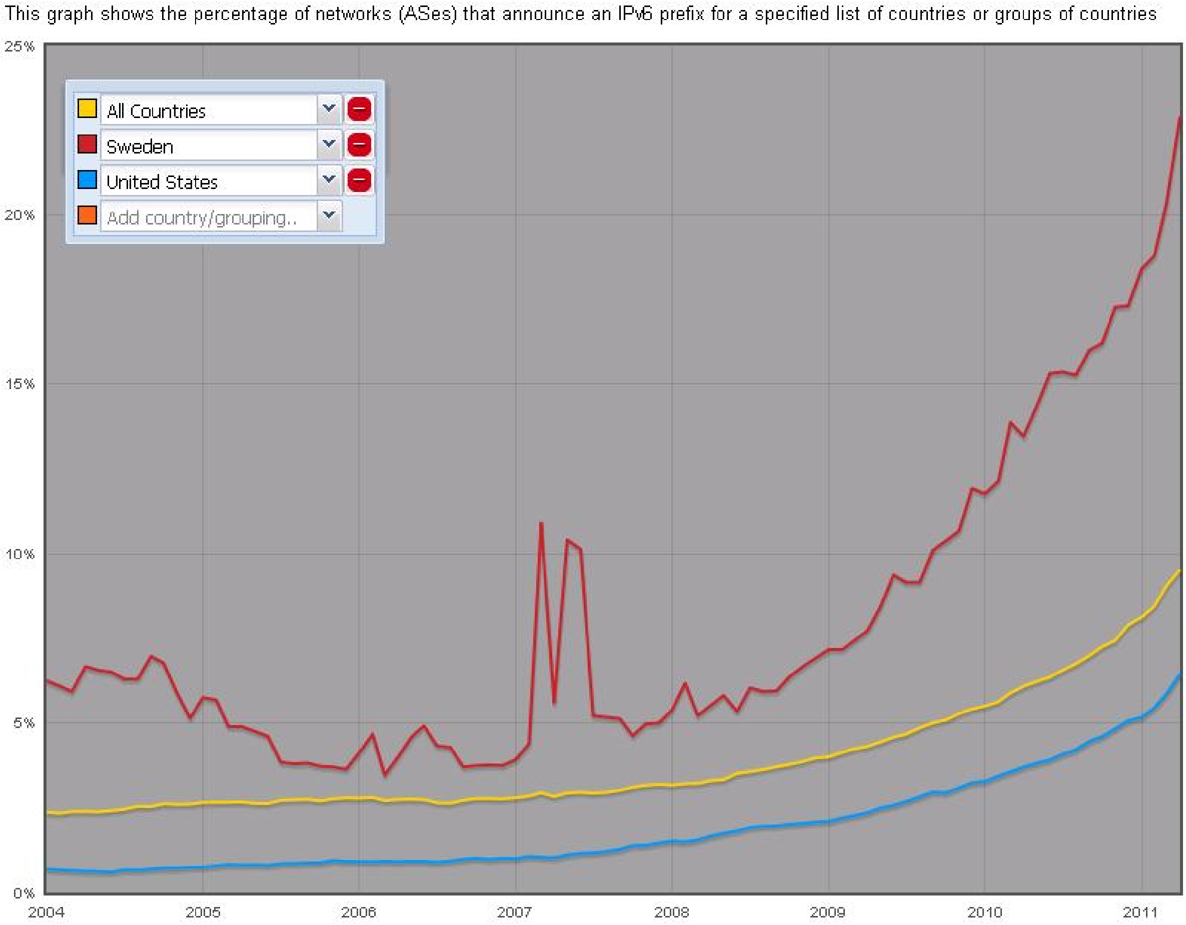


Figure 9-2 Graph showing the progress of IPv6-enabled ASes in all countries, Sweden and the United States. (Provided by RIPE NCC)

9.7 *IPv6 Test using www.tunnelbroker.net*

We wanted to investigate the complexity for a private person to use IPv6 over IPv4. We decided to use Hurricane Electric IPv6 Tunnel Broker (www.tunnelbroker.net) to perform this test. To be able to use this tunnel platform service you need to have an IPv6 capable host or router with IPv4 connectivity.

9.7.1 Hypothesis

We expect to be able to access IPv6 without stumbling on any major problems which cannot be solved by ourselves.

9.7.2 Equipment

Computer	**Operating system**
IMB ThinkPad	Windows XP Home
Alienware M15x	Windows 7 Home Premium
MacBook (2007)	Mac OSX 10.3 Panther

Tunneling Platform
Hurricane Electric IPv6 Tunnel Broker

9.7.3 Method

In order to use Hurricane Electrics IPv6 tunneling services you need to register as a user on their website. Once a member, you can create tunnels up to five regular tunnels. To set up a tunnel, we performed the following steps:

1. Enter www.tunnelbroker.net
2. Sign up for an account.
3. Login in and click: “ Create Regular Tunnel”
4. Enter your IPv4 endpoint Address which is provided for you in the browsing window.
5. Choose the recommended tunnel server (usually the closest to your location).
6. Then press create tunnel and follow the instructions for configuring your tunnel for your current operating system and then the tunnel should be running.

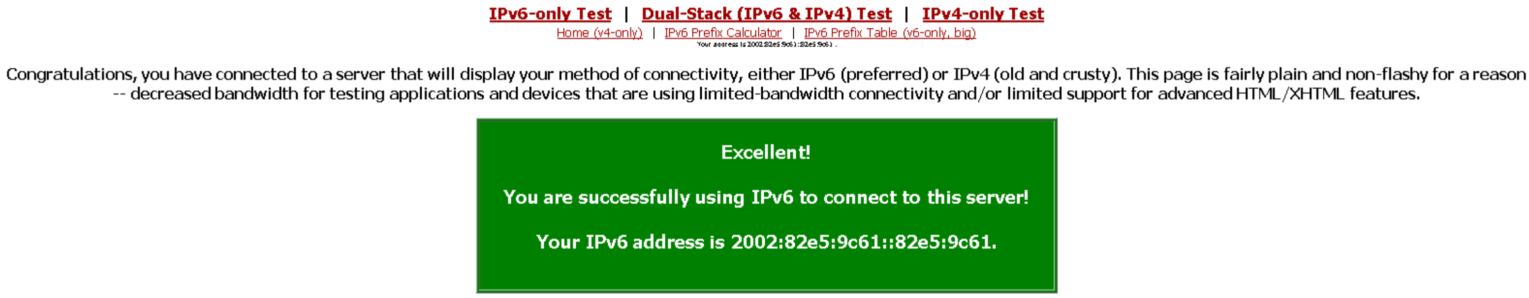
   For a computer running Windows 7, the configuration parameters can look as follows:

```
netsh interface teredo set state disabled
netsh interface ipv6 add v6v4tunnel IP6Tunnel 130.237.17.115 216.66.80.90
netsh interface ipv6 add address IP6Tunnel 2001:470:27:804::2
netsh interface ipv6 add route ::/0 IP6Tunnel 2001:470:27:804::1
```

9.7.4 Results

The tunnel worked on the Alienware M15X computer running Windows 7 Home Premium without any major complications. We did however end up with a total of 72 different tunnel connections to local networks after following the configurations provided by www.tunnelbroker.net.

After setting up the tunnel we controlled our IPv6 connectivity by visiting the following site: http://v6.testmyipv6.com which provided the following results:


IPv6-only Test | Dual-Stack (IPv6 & IPv4) Test | IPv4-only Test
Home (v4-only) | IPv6 Prefix Calculator | IPv6 Prefix Table (v6-only, big)

Your address is 2002:82e5:9c61::82e5:9c61 .

Congratulations, you have connected to a server that will display your method of connectivity, either IPv6 (preferred) or IPv4 (old and crusty). This page is fairly plain and non-flashy for a reason -- decreased bandwidth for testing applications and devices that are using limited-bandwidth connectivity and/or limited support for advanced HTML/XHTML features.

Excellent!

You are successfully using IPv6 to connect to this server!

Your IPv6 address is 2002:82e5:9c61::82e5:9c61.

Figure 9-3 Picture showing IPv6 connectivity (Provided by http://v6.testmyipv6.com)

9.7.5 Conclusions

Setting up a 6to4 tunnel through www.tunnelbroker.net is fairly easy if you have access to a computer with a modern operating system (preferably not Windows XP) such as Windows 7 or Windows Vista. Even though previous experience with configuring IP-connections might help, it is not needed. As long as you can follow the instructions and use a search engine to provide further information if needed, the process is quite straightforward.

10 Results

Clearly the IPv6 transition is a complex matter that will require a lot of time and effort. Outside of people who are familiar of IT, very few people know what IPv6 is and why the transition to it is necessary. Among the employees of the different companies we have spoken to, knowledge of IPv6 is strictly limited to IT staff. These staff members are often aware of the upcoming transition, but lack a clear plan on how to move forward. The main cause of inactivity seems to be the lack of a concrete plan and the fear of moving too fast forward — leading to wasteful investments in IT infrastructure.

The survey that we performed indicates that most people know what an IP-address, but only one in three knows what IPv6 is. This suggests that improved education and media coverage of these issues is warranted.

The main bottleneck in terms of a large scale transition by companies and organizations seems to be the lack of services that would be available only over the IPv6 Internet. This is a so called “chicken and egg” problem as very few services are being developed for IPv6 as there are no users, and there are no users because of the lack of services. On June 8th 2011 several large companies, such as Google and Facebook, will participate in what is called “IPv6-day” where they will offer their services over native IPv6. This is a step in the right direction to introduce more services to the IPv6 Internet.

Another bottleneck is the lack of ISP-support for IPv6. Very few ISPs are currently providing IPv6 to their customers and many are lagging behind in implementing IPv6, making it even harder for end users to connect via IPv6. It seems that telephone operators will be one of the major players pushing for the rapid adoption of IPv6. The largest reason for this is because of the need for unique IP-addresses to be able to provide smartphones and other devices with Internet connectivity.

There is some ambiguity regarding the support for IPv6 in hardware and software. Almost all of the major operating systems of today have support for IPv6, but home routers and modems have very limited support for IPv6. A result of this lack of IPv6 support in home routers and modems is that users will have to implement their own IPv6 firewalls. Many of the most widely used applications, such as web-browsers and email-programs, already have support for IPv6 and more applications are continuously being added.

It is a fact that IPv6 will be needed for the continued development and growth of the Internet. The main reason why IPv6 is needed is the lack of available globally IPv4-addresses. The abundance of new addresses will enable countries such as China and India to continue to connect to the Internet. Another exciting feature is the possibility of embedding IP-addresses into everyday objects and remotely controlling these objects through the Internet.

IPv6 brings a lot of other new features to the Internet Protocol as well, but as of today, they are, not as important in comparison to the need of new addresses.

We managed to get our topic featured on (Swedish) national television where a four minute long feature was shown and where the benefits and needs of IPv6 were discussed [3]. This hopefully resulted in informing the general public more about the issue at hand.

Our attempt to gain IPv6 connectivity through tunneling via www.tunnelbroker.net turned out successfully and proves that almost anyone can gain access to the IPv6 Internet today.

11 Conclusions and Future Work

The lack of knowledge about IPv6 among people makes it hard to influence people to adopt IPv6. The goal of informing the public about the role of IP addresses and the importance of the transition to IPv6 through the media was met to a certain point. We had the ambition to contribute articles to newspapers as well, but failed due mainly because of the lack of interest on their part. However, we think that the media coverage we got from the news feature on national television is a good start in informing Swedish citizens about IPv6. The goal of educating companies about IPv6 was not completed in this thesis because it turned out to be a more complex of a task than we first thought. However, with help from Jan Östling of Cisco Systems, we did find a convenient method for defining what strategy a company should use for implementing IPv6 using the "Janoz-method" (Appendix III). We also managed to identify to some extent what the situation looks like in Sweden regarding the knowledge and expectation of IPv6.

Regarding the benefits of the new protocol we were surprised to see that *absolutely* the biggest advantage is the increased number of addresses. The remaining features included in IPv6 turned out to not be as important as we first thought, while the need for unique addresses was more important that we had originally anticipated. However, in the future, the other improvements made to IPv6 might turn out to be very attractive.

At the beginning of the thesis project we expected the new protocol to be superior in every aspect, but as it turns out there is still much work to be done to IPv6 before it completely can replace IPv4. Nevertheless, it is our firm belief that the future of the Internet lies with IPv6.

One of the big question marks of IPv6 is whether or not the new protocol will work when widely deployed between millions of nodes. A first test with this magnitude will be made on June 8th 2011 on the World IPv6 Day.

There are also many uncertainties for both companies and private persons as to when to begin the transition to IPv6 and which strategy to choose. Every client and company is most likely going to need their own strategy. One thing that is certain is that the full implementation of IPv6 will not happen overnight, the process will most likely span over a ten to fifteen year period where both protocols will have to be run at the same time.

If we had to it all over again with the same goal of accelerating the adoption of IPv6 we would have focused more on reaching out to people explaining why they should change instead of putting so much effort in comparing the two protocols and examining incentives for businesses to change.

It is very hard to determine what impact our work will have on the adoption of IPv6. We think our thesis project has already increased the awareness about IPv6 in Sweden, but our study clearly shows that much work remains to be done before we will successfully fully migrate to IPv6.

11.1 *Future work*

Future work includes the need for continued education about IPv6 to the general public and why IPv6 is needed in practice — rather than focusing on the technical differences between the two protocols. Instead the focus should be to make more services available over both protocols, as this is most likely the most powerful driver of increased demand for IPv6 by customers.

References

[1] Anders Nilsson and Magnus Lindberg, Virtually@Home, , Bachelors' thesis, School of Information and Communication Technology, Royal Institute of Technology (KTH), Stockholm, Sweden, TRITA-ICT-EX-2009:219, December 2009, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/091202-Ander_Nilsson_och_Magnus_Lindberg-with-cover.pdf

[2] Thor Hådén, IPv6 Home Automation, Bachelors' thesis, School of Information and Communication Technology, Royal Institute of Technology (KTH), Stockholm, Sweden, TRITA-ICT-EX-2009:28, June 2009, http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/090601-Thor_Haaden.pdf

[3] Susan Ritzén, Sverige har släpat efter som IT-nation, SVT Rapport, Swedish Television (SVT), telecast at 19:30 on 20 April 2012, duration 3:23, http://svtplay.se/v/2403774/sverige_har_slapat_efter_som_it-nation

[4] About.com website, Current World Population, as accessed on 12-Feb-2011 13:00 UTC, http://geography.about.com/od/obtainpopulationdata/a/worldpopulation.htm

[5] ARIN (2010) IPv4 Depletion, IPv6 Depletion, [PowerPoint Slides], as accessed on 15-Feb-2011 14:40 UTC, http://www.teamarin.net/

[6] Mike Leber, Global IPv6 Deployment Progress Report, as accessed on 19-Feb-2011 15:41 UTC, http://bgp.he.net/ipv6-progress-report.cgi

[7] Gerald Q. Maguire Jr., Lecture notes for IK1550 Internetworking/Internetteknik Spring 2010, Period 4, 21 March 2010, http://www.ict.kth.se/courses/IK1550/Internetworking-2010b.pdf

[8] Juniper Networks Techpub, IPv6 Packet Headers, as accessed on 23-Feb-2011 18:34 UTC, http://www.juniper.net/techpubs/software/erx/erx50x/swconfig-routing-vol1/html/ipv6-config4.html

[9] Geoff Huston, IPv4 Address Report, as accessed on 09-Feb-2011 07:58 UTC, http://www.potaroo.net/tools/ipv4/

[10] TCP IP Guide, IPv6 Datagram Options, as accessed on 21-Feb-2011 15:33 UTC, http://www.tcpipguide.com/free/t_IPv6DatagramOptions.htm

[11] Interview with Jan Östling, Systems Engineer at Cisco Systems Sweden, 7-Apr-2011

[12] Silvia Hagen, IPv6 Essentials, Integrating IPv6 to your IPv4 Network, 2nd Edition , O'Reilly Media, Sebastopol, California, U.S.A., May 2006, ISBN-13: 978-0596100582

[13] IPv6.com, IPv6 – Auto Configuration vs. DHCPv6, as accessed on 20-Apr-2011 21:05 UTC, http://blog.ipv6.com/articles/general/Auto-Configuration-vs-DHCPv6.htm

[14] Wikipedia, Network Address Translation, as accessed 3-Mar-2011 12.00 UTC http://sv.wikipedia.org/wiki/Network_Address_Translation

[15] Kaushik Das, IPv6.com website, IPSec & IPv6 - Securing the NextGen Internet, as accessed on 22-April-2011 11.42,UTC http://ipv6.com/articles/security/IPsec.htm

[16] IPv6.com, IPv6 – Hardware Vendor Support, as accessed on 21-Apr-2011 16:33 UTC, http://ipv6.com/articles/hardware/IPv6-Vendor-Support.htm

[17] Microsoft Technet Network and Access Technologies, Ipv6, as accessed on 20-Apr-2011 09:44 http://technet.microsoft.com/en-us/network/bb530961

[18] Wikipedia, Comparison of IPv6 application support, as accessed on 20-Apr-2011 13:46 UTC, http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support

[19] Julie Bort, IPv6 on home routers and DSL/cable: FAIL, as accessed on Apr-20-2011 23:17 UTC http://www.networkworld.com/news/2011/030411-ipv6-home-routers.html?hpg1=bn

[20] Lars Dobos, IPv6 Ready är inte IPV6-färdigt, as accessed on Apr-20-2011 23:48 UTC http://www.idg.se/2.1085/1.369029/ipv6-ready-ar-inte-ipv6-fardigt

[21] IPv6vsIPv4.net, IPv6 Manual Tunneling, as accessed 25-April 2011 18:34 UTC http://www.ipv6vsipv4.com/manual.html

[22] Carolyn Duffy Marsan, IPv6 Tunnel basics, as accessed 26-April-2011 09:44 UTC http://www.networkworld.com/news/2010/050610-ipv6-tunnel-basics.html?page=1

[23] Wikipedia, IPv6 Rapid Deployment, as accessed 26-April-2011 10:54 UTC, http://en.wikipedia.org/wiki/IPv6_rapid_deployment

[24] Cisco Case Study, Bechtel Well Positioned to Serve Customers by Using Microsoft and Cisco IPv6 Solution, as accessed 26th-April-2011 UTC http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/prod_case_study0900aecd806d89d5.pdf

[25] R. Despres, RFC 5569 IPv6 Rapid Deployment on IPv4 Infrastructures(6rd) as accessed 15th-April-2011, UTC http://tools.ietf.org/html/rfc5569

[26] Näringsdepartementet, Press release, Ett viktigt steg mot införande av IPv6, as accessed 5th-April-2011, UTC http://www.regeringen.se/sb/d/13722/nocache/true/a/157018/dictionary/true

[27] Karl Mayer and Wolfgang Fritsche, IABG ,IPv6 security models and dual stack (IPv6/IPv4) implications, as accessed 3-April-2011, UTC http://ec.europa.eu/information_society/policy/ipv6/docs/studies/executive_summary_v1.3_en.pdf

[28] Daniel O. Awduche, Benefits of IPv6 for Enterprises, as accessed on 28-April-2011 17:55 UTC http://www.verizonbusiness.com/resources/whitepapers/wp_benefits-of-ipv6-for-enterprises_en_xg.pdf

[29] IPv6.com, IPv6 and the Auto Industry, as accessed 28-Apr 16:20 UTC http://www.ipv6.com/articles/mobile/IPv6-and-the-Auto-Industry.htm

[30] IPv6.com, Medical Industry IPv6 Sensors http://www.ipv6.com/articles/applications/Medical-Industry-v6-Sensors.htm

[31] Khaled Al Twergi, Business aspects of IPv6, as accessed on Apr-28 18:51 UTC http://www.menog.net/sites/default/files/Business%20aspects%20of%20IPv6.pdf

[32] Interview with Leif Bengtsson Vice President of Product Development TV at Telia Sonera, 15-April-2011

[33] Interview with Rieza Abbasi, Director Connectivity Services, TietoEnator, 5-April-2011

[34] Interview with Simon Edström, IT, Telecom and Security Manager of Forsen Projekt, 25-Feb 2011.

[35] Carolyn Duffy Marsan, IPv6 Tunnel basics, as accessed 29-April-2011 01:40 UTC http://www.networkworld.com/news/2010/050610-ipv6-tunnel-basics.html?page=1

[36] J. Jeong, IPv6 Host Configuration of DNS Server Information Approaches, Internet Request for Comments, RFC Editor, ISSN 2070-1721, RFC 4339, February 2006, http://www.rfc-editor.org/rfc/rfc4339.txt

[37] S. Thomson, C. Huitema,V. Ksinant, and M. Souissi, DNS Extensions to Support IP Version 6, RFC Editor, Internet Request for Comments, ISSN 2070-1721, RFC 3596, October 2003, http://www.rfc-editor.org/rfc/rfc3596.txt

[38] C. Aoun and E. Davies, Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status, RFC Editor, Internet Request for Comments, ISSN 2070-1721, RFC 4966, July 2007, http://www.rfc-editor.org/rfc/rfc4966.txt

[39] Tero Maaniemi, IPv6 Rollout To TeliaSonera's Finnish IPNetwork, December 2010, Master Thesis, Information Technology Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland, http://publications.theseus.fi/bitstream/handle/10024/26485/IPv6%20Rollout %20To%20TeliaSoneras%20Finnish%20IP-Network.pdf

[40] Google, Access Google services over IPv6, Google, Last modified 2 January 2011, http://www.google.com/intl/en/ipv6/

Appendix I – IPv6 Survey results

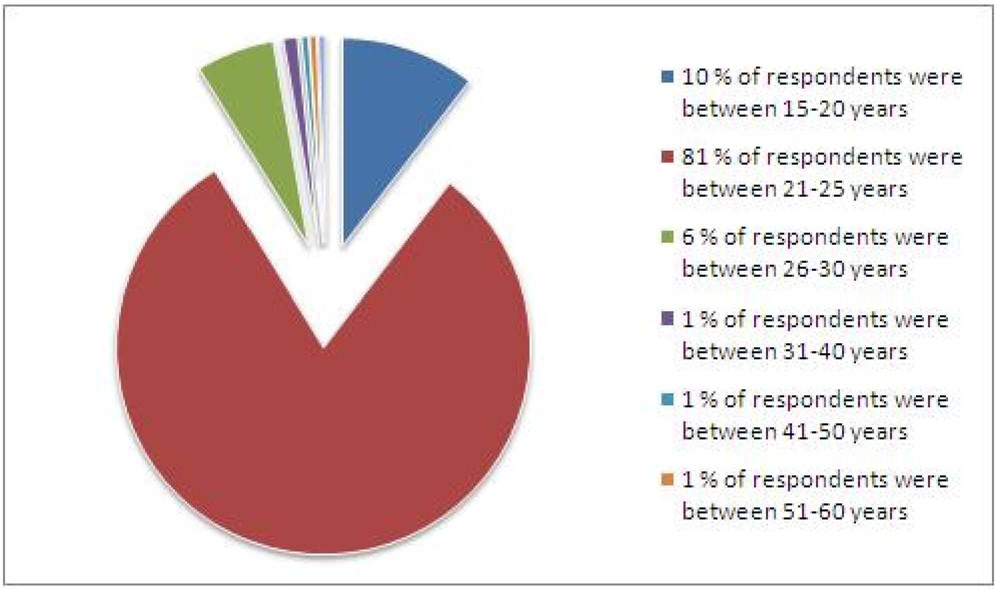


Figure 11-1 Age distribution of Respondents

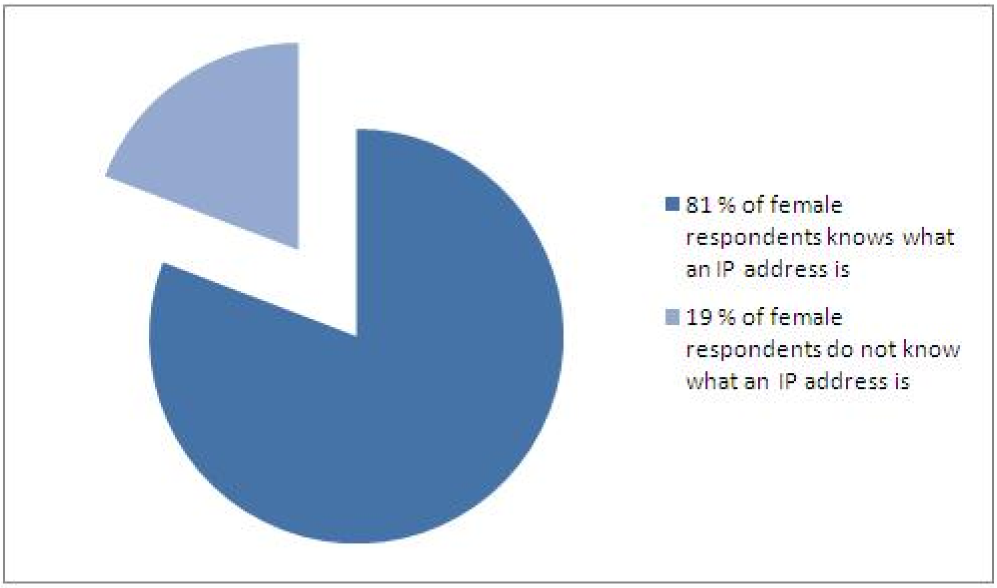


Figure 11-2 Female respondent's knowledge about IP-addresses

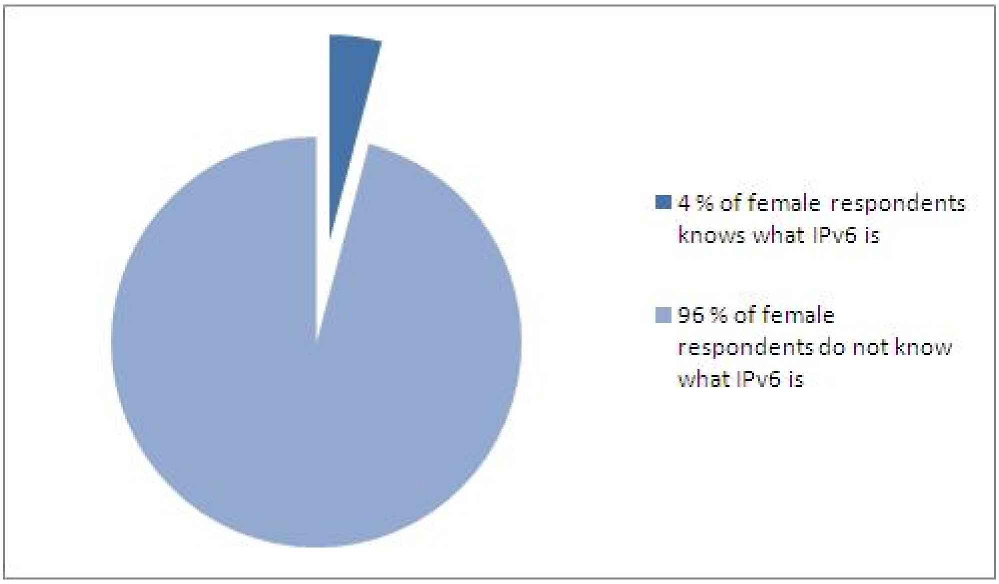


Figure 11-3 Female respondents’ knowledge about IPv6

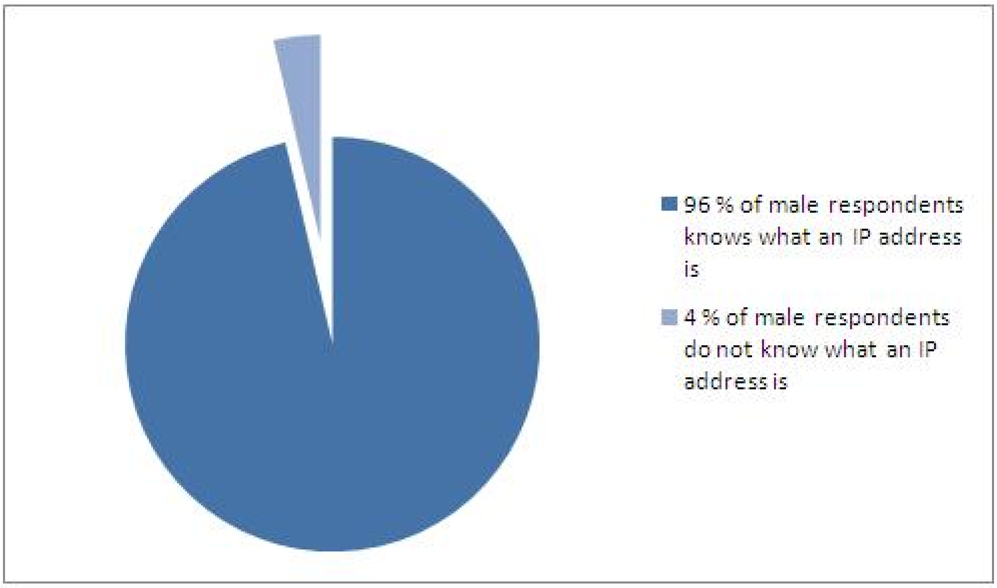


Figure 11-4 Male respondents’ knowledge about IP-addresses

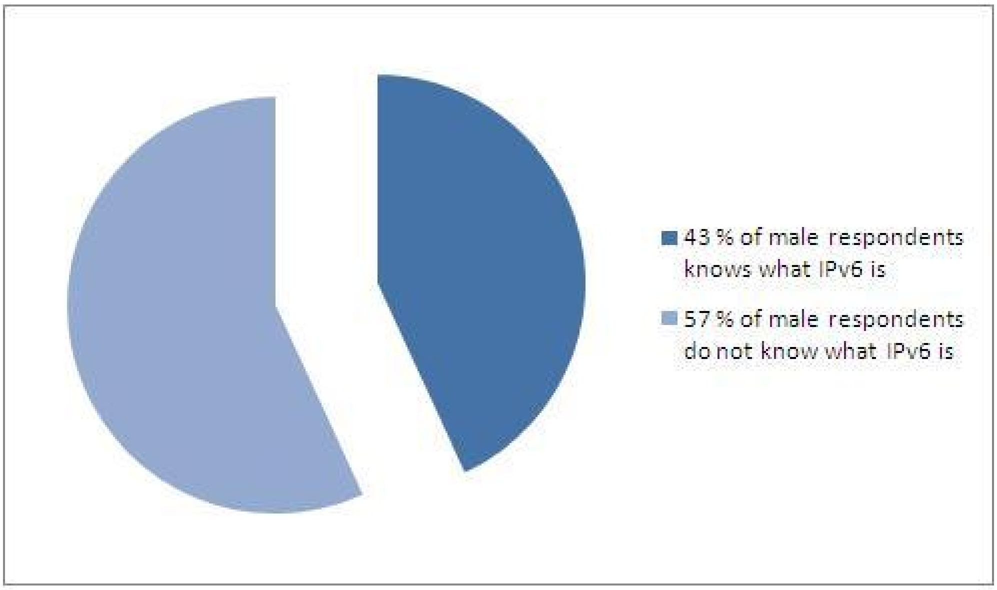
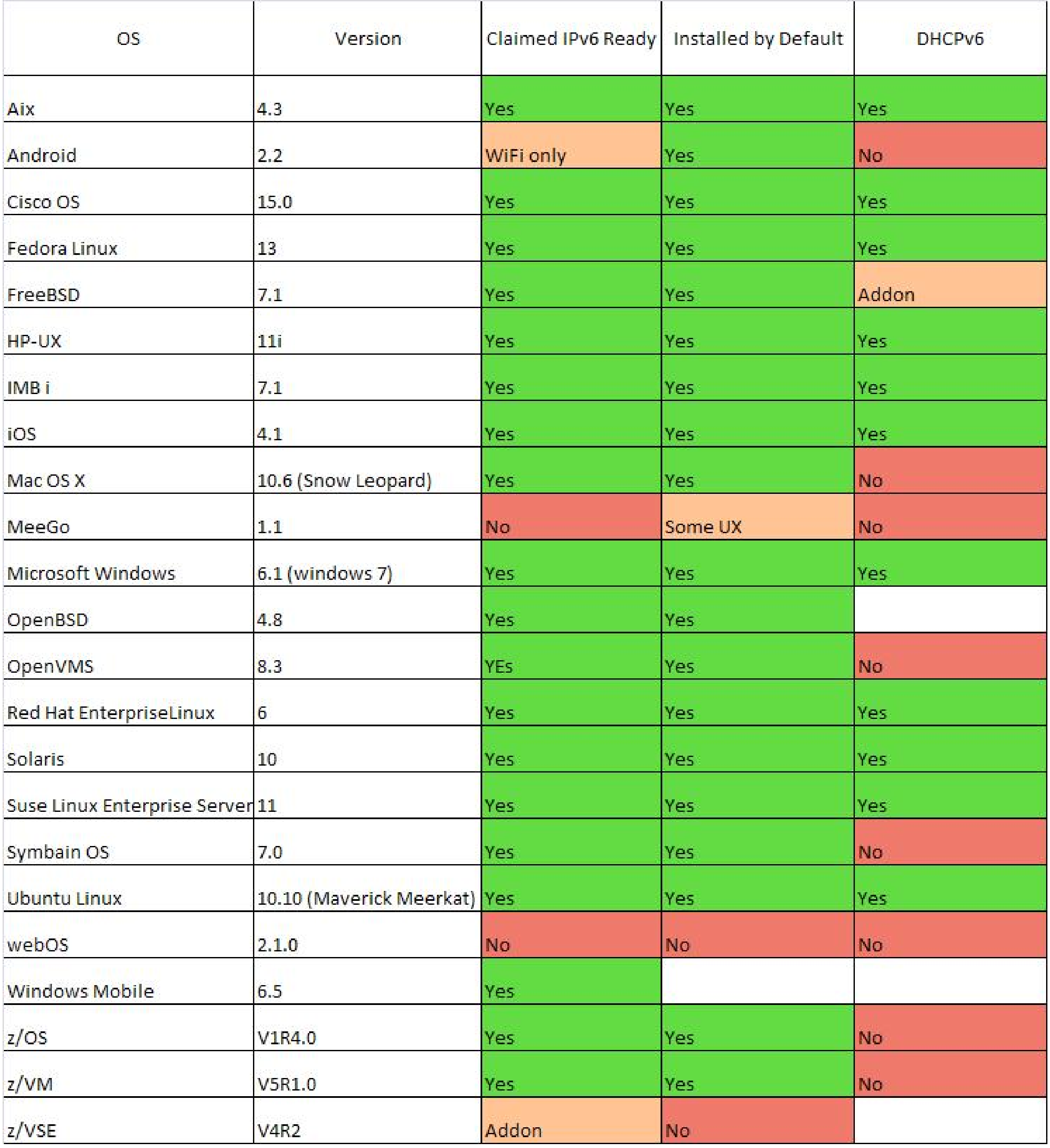


Figure 11-5 Male respondents' knowledge about IPv6

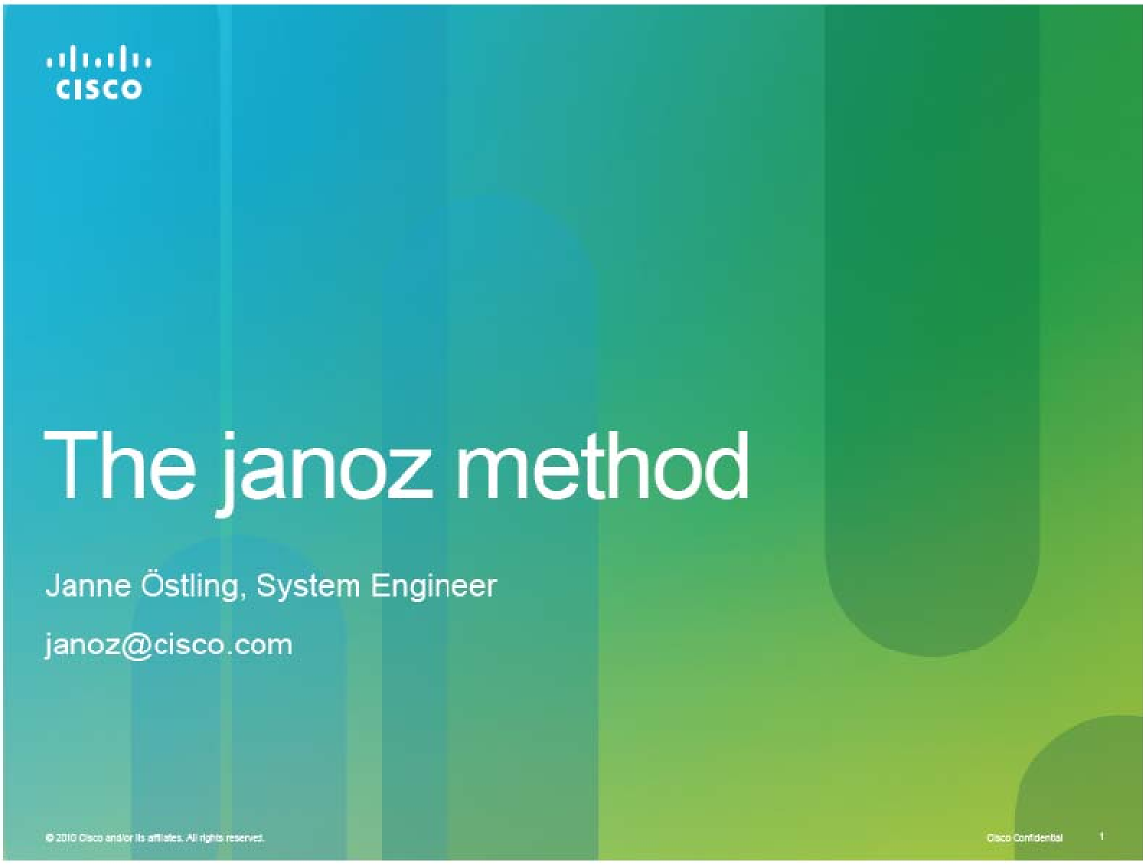
Appendix II – List of appliances with IPv6 support



OS	Version	Claimed IPv6 Ready	Installed by Default	DHCPv6
Aix	4.3	Yes	Yes	Yes
Android	2.2	WiFi only	Yes	No
Cisco OS	15.0	Yes	Yes	Yes
Fedora Linux	13	Yes	Yes	Yes
FreeBSD	7.1	Yes	Yes	Addon
HP-UX	11i	Yes	Yes	Yes
IMB i	7.1	Yes	Yes	Yes
iOS	4.1	Yes	Yes	Yes
Mac OS X	10.6 (Snow Leopard)	Yes	Yes	No
MeeGo	1.1	No	Some UX	No
Microsoft Windows	6.1 (windows 7)	Yes	Yes	Yes
OpenBSD	4.8	Yes	Yes	
OpenVMS	8.3	YEs	Yes	No
Red Hat EnterpriseLinux	6	Yes	Yes	Yes
Solaris	10	Yes	Yes	Yes
Suse Linux Enterprise Server	11	Yes	Yes	Yes
Symbain OS	7.0	Yes	Yes	No
Ubuntu Linux	10.10 (Maverick Meerkat)	Yes	Yes	Yes
webOS	2.1.0	No	No	No
Windows Mobile	6.5	Yes		
z/OS	V1R4.0	Yes	Yes	No
z/VM	V5R1.0	Yes	Yes	No
z/VSE	V4R2	Addon	No	

Figure 11-6 List of appliances with IPv6 support (Adapted from figure provided by www.wikipedia.com)

Appendix III-The Janoz Method (by Jan Östling, Cisco Systems) [11]

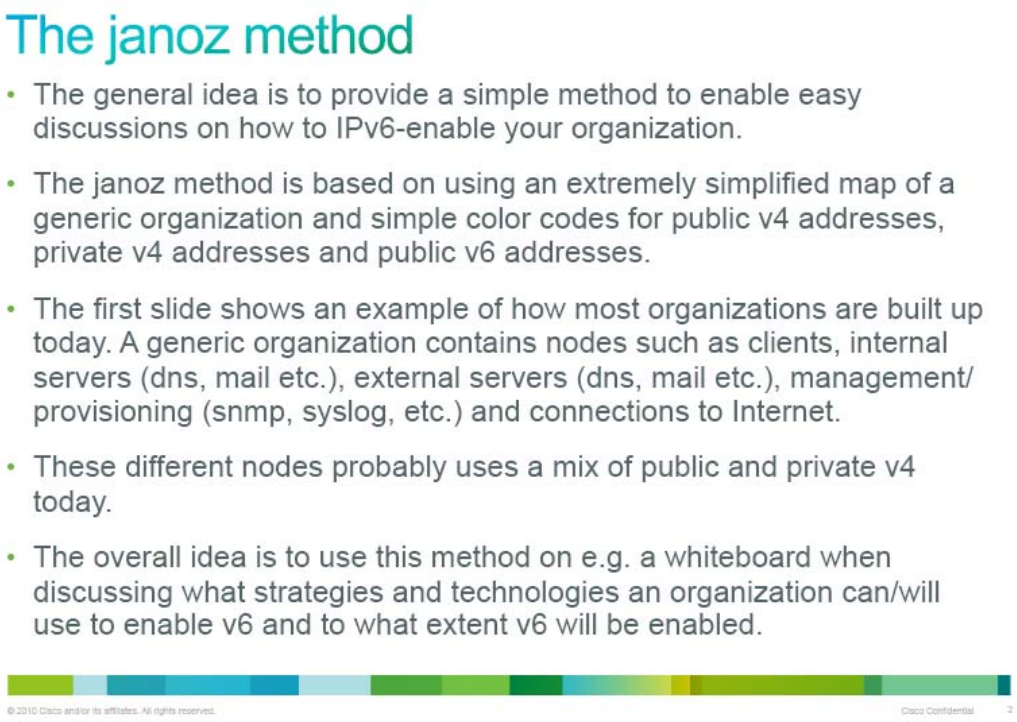


The janoz method

Janne Östling, System Engineer

janoz@cisco.com

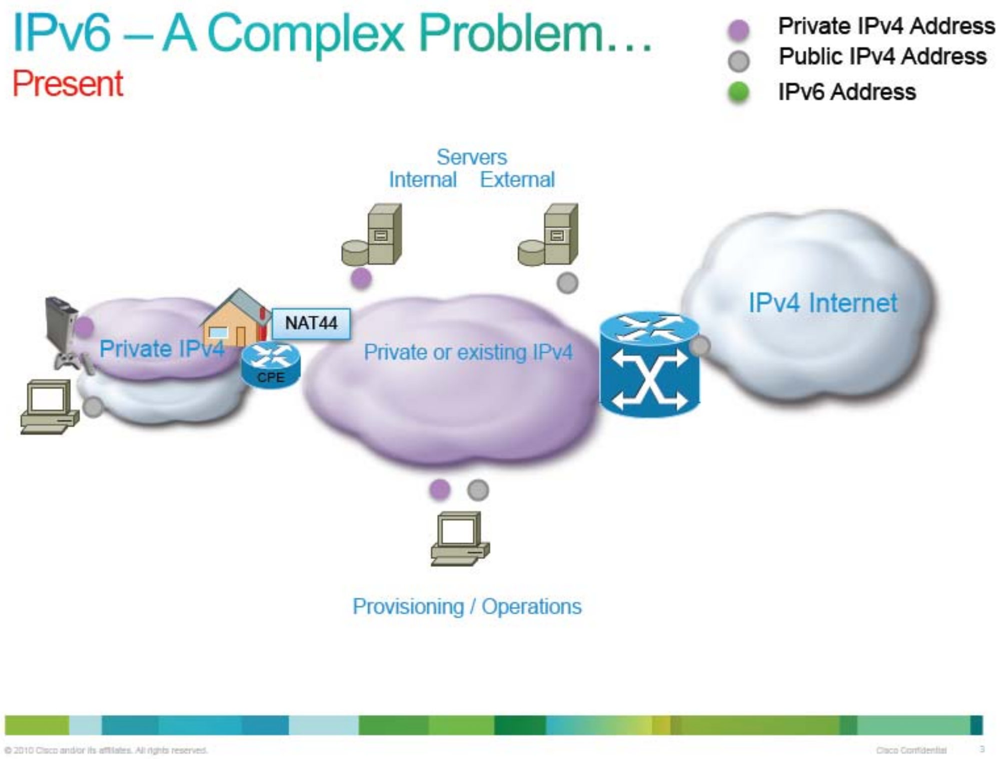
Cisco Confidential 1



The janoz method

- The general idea is to provide a simple method to enable easy discussions on how to IPv6-enable your organization.
- The janoz method is based on using an extremely simplified map of a generic organization and simple color codes for public v4 addresses, private v4 addresses and public v6 addresses.
- The first slide shows an example of how most organizations are built up today. A generic organization contains nodes such as clients, internal servers (dns, mail etc.), external servers (dns, mail etc.), management/ provisioning (snmp, syslog, etc.) and connections to Internet.
- These different nodes probably uses a mix of public and private v4 today.
- The overall idea is to use this method on e.g. a whiteboard when discussing what strategies and technologies an organization can/will use to enable v6 and to what extent v6 will be enabled.

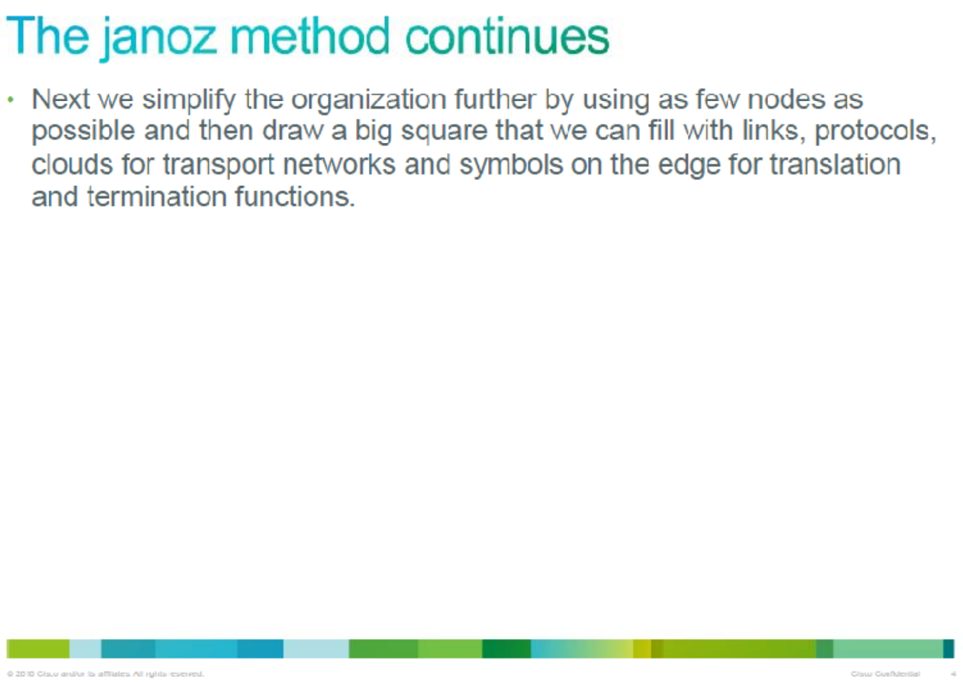
Cisco Confidential 2



IPv6 – A Complex Problem…

Present

- ● Private IPv4 Address
- ● Public IPv4 Address
- ● IPv6 Address



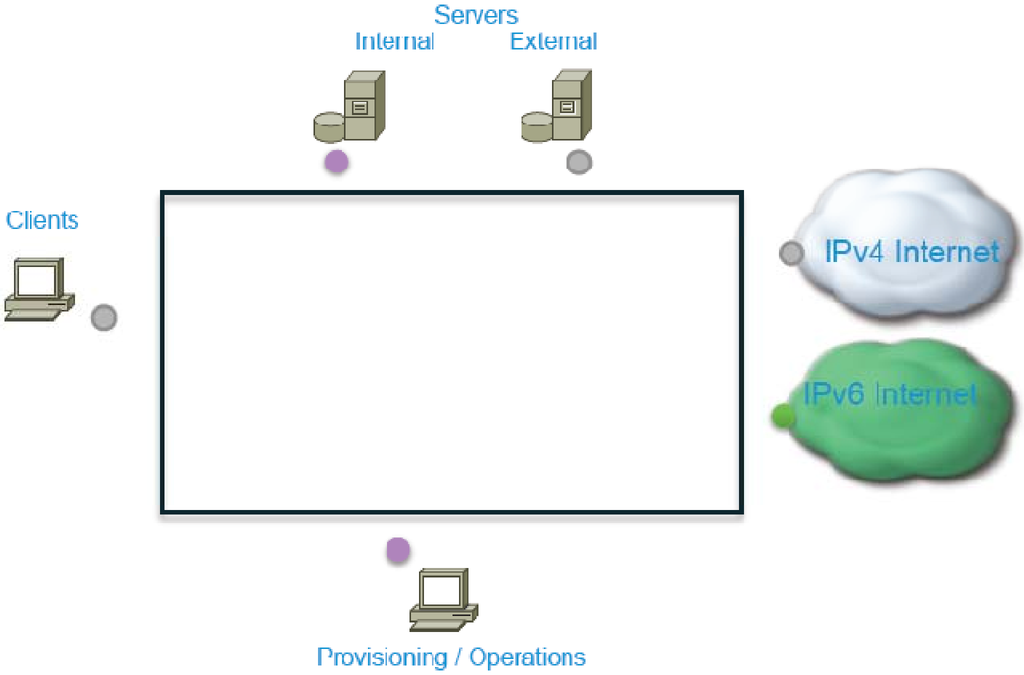
The janoz method continues

- Next we simplify the organization further by using as few nodes as possible and then draw a big square that we can fill with links, protocols, clouds for transport networks and symbols on the edge for translation and termination functions.

The janoz method

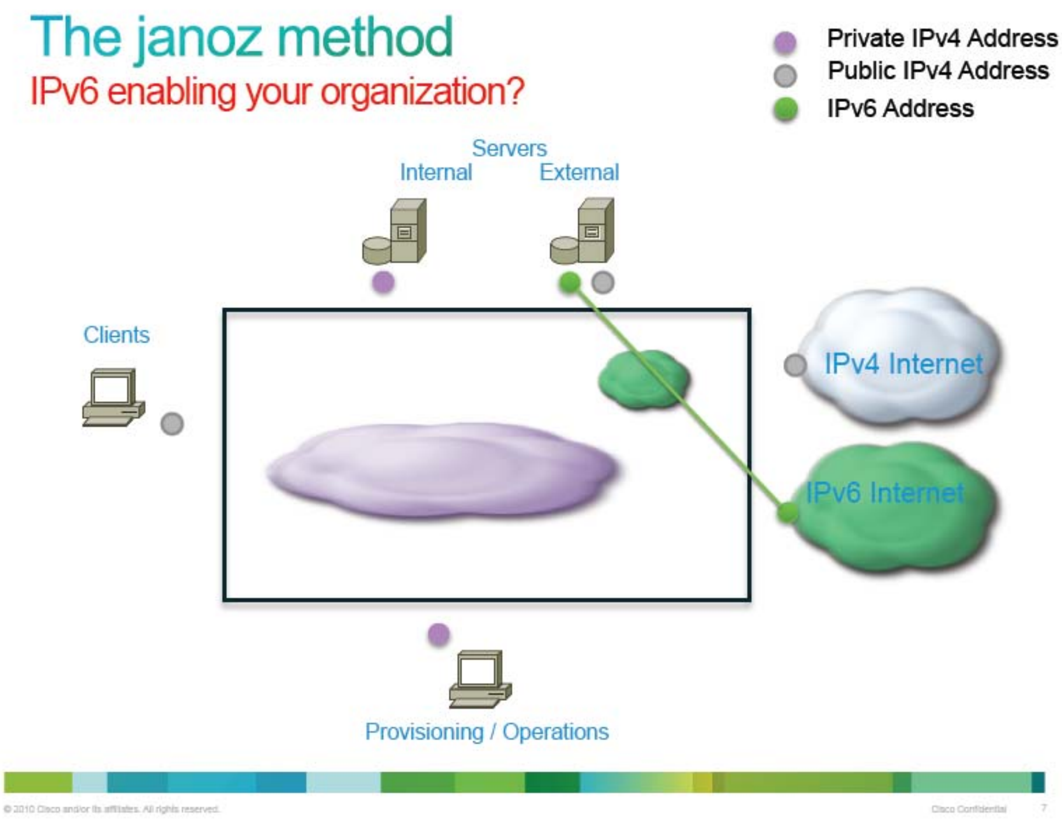
A generic network model

● Private IPv4 Address
● Public IPv4 Address
● IPv6 Address



The janoz method continues further

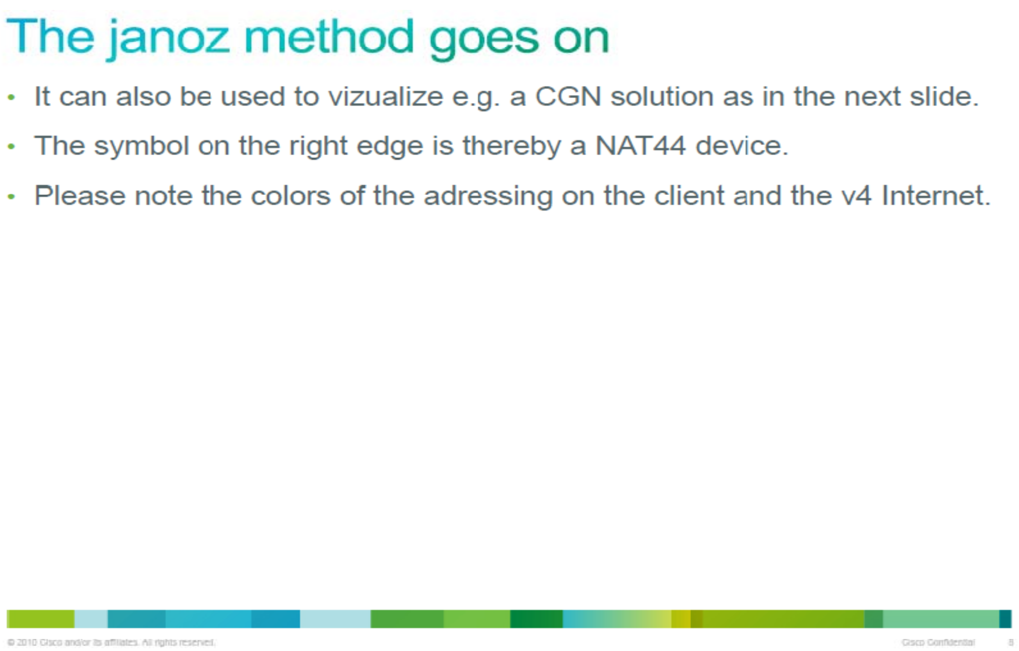
- Let’s start with what is usually the first step for an organization. V6-enabling the external servers.
- This can be visualized by drawing one v6 (green) line from the servers via a (perhaps pure dual stack) green cloud that symbolizes the transport mechanism from the servers to the v6 Internet.



The janoz method

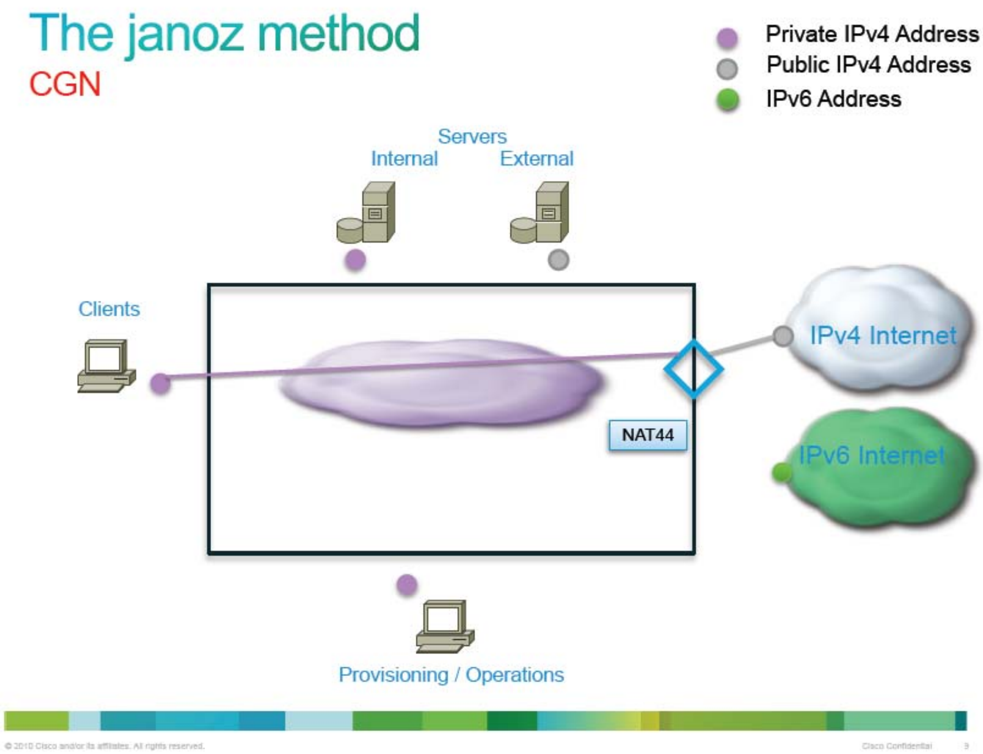
IPv6 enabling your organization?

● Private IPv4 Address
● Public IPv4 Address
● IPv6 Address



The janoz method goes on

- It can also be used to vizualize e.g. a CGN solution as in the next slide.
- The symbol on the right edge is thereby a NAT44 device.
- Please note the colors of the adressing on the client and the v4 Internet.



The janoz method

CGN

● Private IPv4 Address
● Public IPv4 Address
● IPv6 Address

Servers
Internal
External

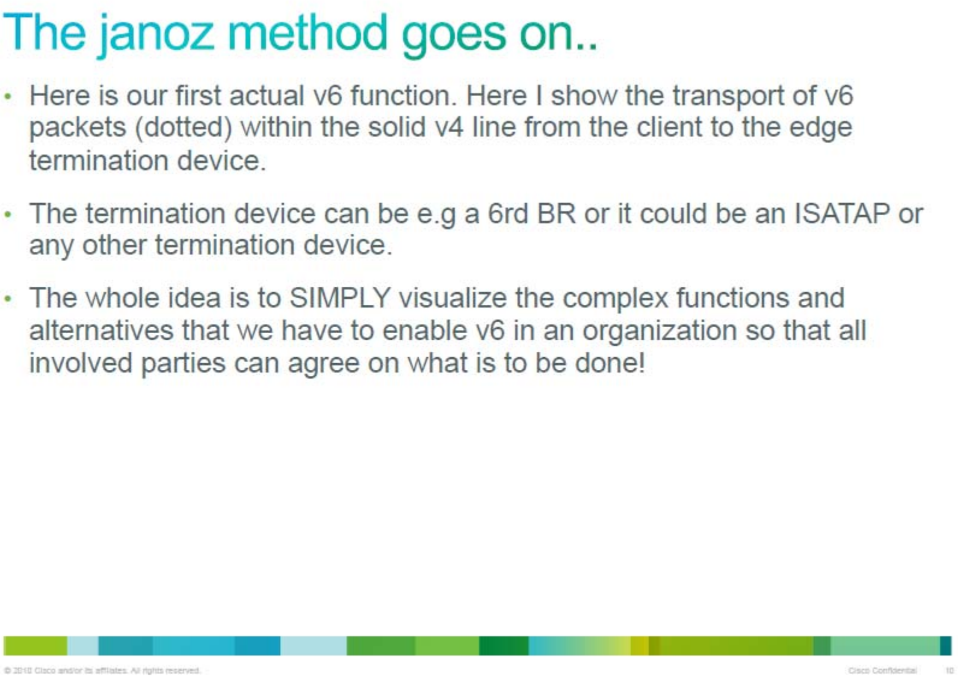
Clients

IPv4 Internet

IPv6 Internet

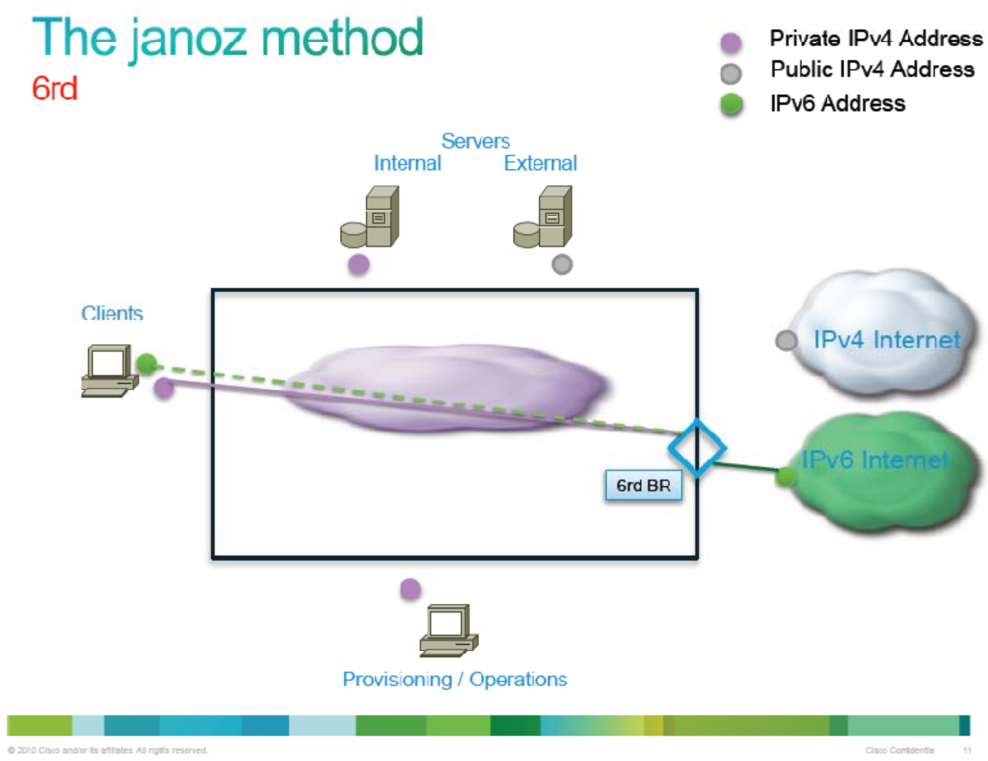
NAT44

Provisioning / Operations



The janoz method goes on..

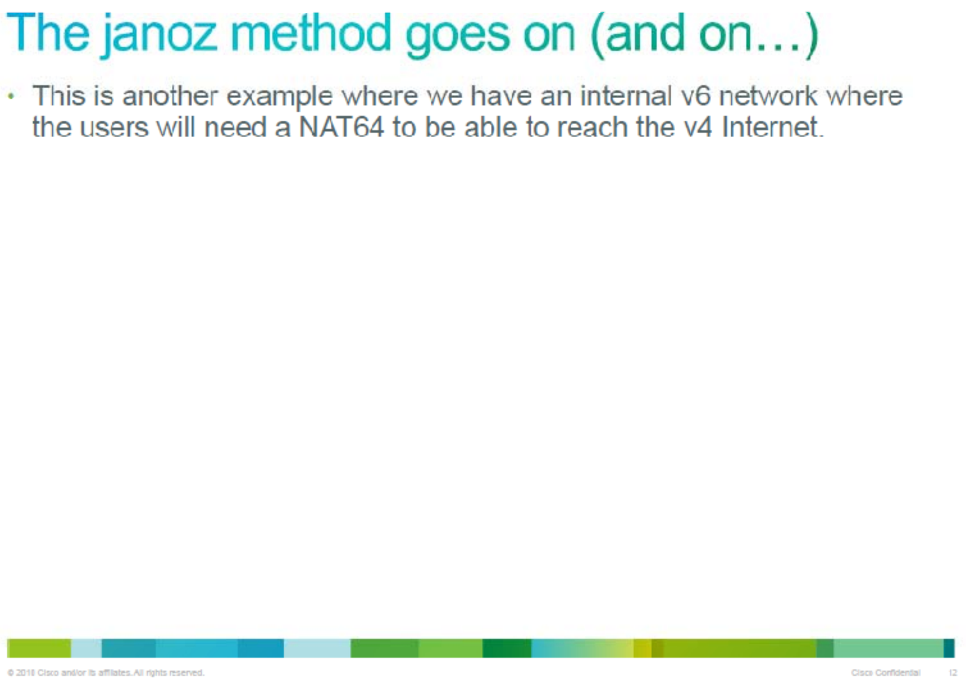
- Here is our first actual v6 function. Here I show the transport of v6 packets (dotted) within the solid v4 line from the client to the edge termination device.
- The termination device can be e.g a 6rd BR or it could be an ISATAP or any other termination device.
- The whole idea is to SIMPLY visualize the complex functions and alternatives that we have to enable v6 in an organization so that all involved parties can agree on what is to be done!



The janoz method

6rd

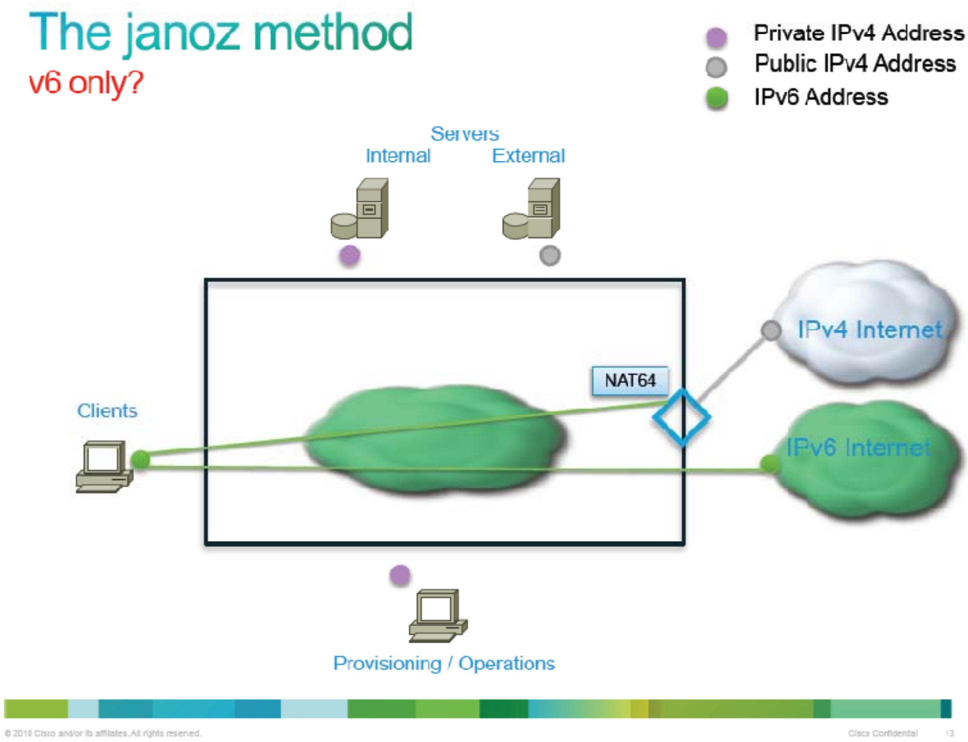
Cisco Confidential 11



The janoz method goes on (and on…)

- This is another example where we have an internal v6 network where the users will need a NAT64 to be able to reach the v4 Internet.

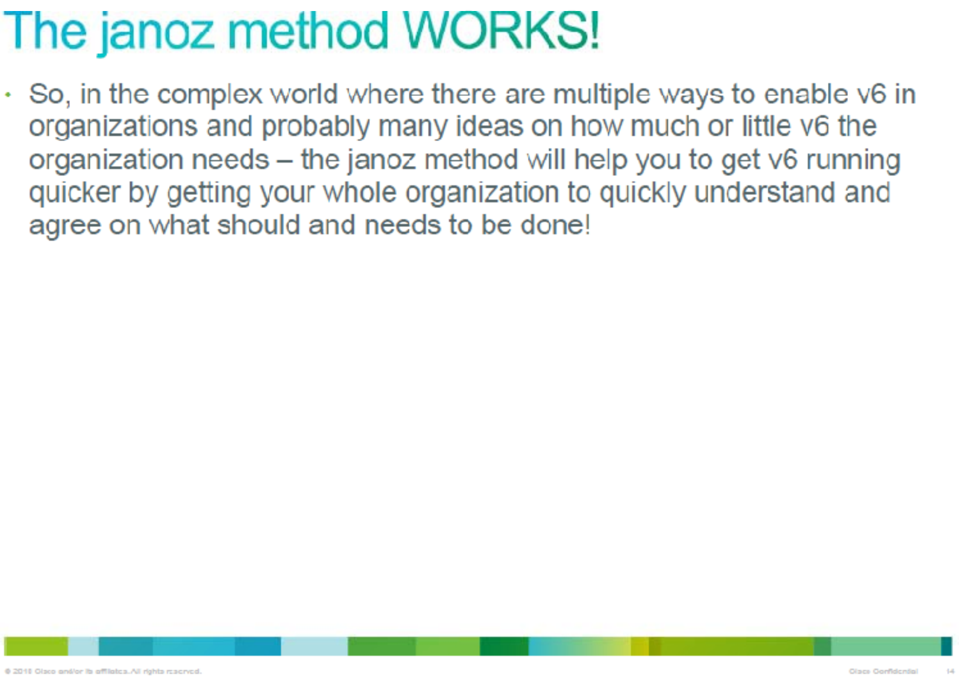
Cisco Confidential 12



The janoz method

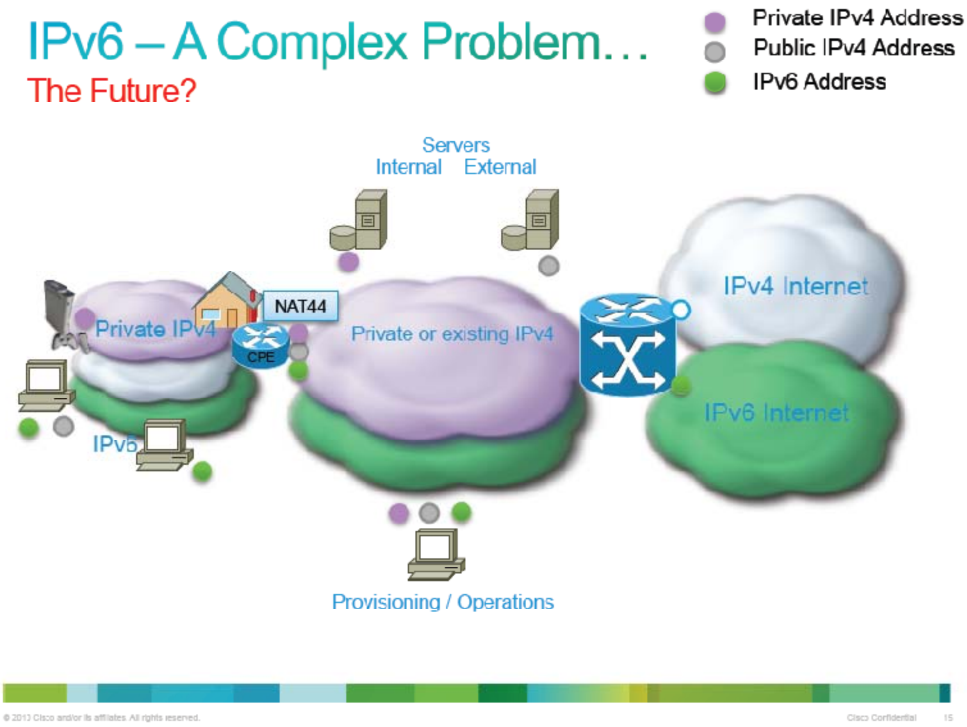
v6 only?

● Private IPv4 Address
● Public IPv4 Address
● IPv6 Address



The janoz method WORKS!

- So, in the complex world where there are multiple ways to enable v6 in organizations and probably many ideas on how much or little v6 the organization needs – the janoz method will help you to get v6 running quicker by getting your whole organization to quickly understand and agree on what should and needs to be done!

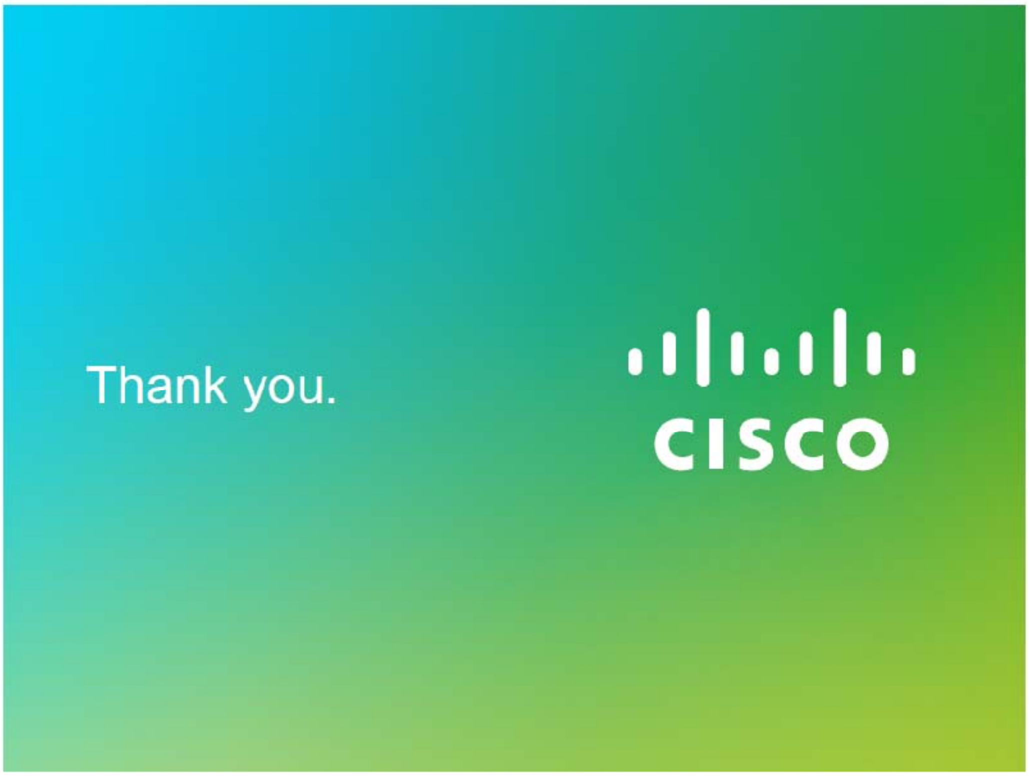


IPv6 – A Complex Problem…

The Future?

- ● Private IPv4 Address
- ● Public IPv4 Address
- ● IPv6 Address

Cisco Confidential 15



Thank you.

TRITA-ICT-EX-2011:72

www.kth.se