Report number
PTS-ER-2011:18

Date
31 October 2011

Deploying IPv6 – Internet Protocol version 6

Practical guidance

Deploying IPv6 – Internet Protocol version 6
Practical guidance

Report number
PTS-ER-2011:18

File reference
11-157

ISSN
1650-9862

Authors
Erika Hersaeus and Roland Svahn

Swedish Post and Telecom Agency
Box 5398
SE-102 49 Stockholm, Sweden

+46 (0)8 678 55 00
pts@pts.se
www.pts.se

Foreword

Most operations in our society are becoming increasingly dependent on communicating electronically. Equipment connected to the Internet requires a unique address and must use common rules ('protocols') to enable it to communicate with other equipment. The addresses used in the dominant standard up until now (IPv4 – Internet Protocol Version 4) are running out.

Access to more addresses is required to facilitate the continued growth of the Internet, with more applications and users. This is a need that the new IPv6 standard could satisfy. Deploying IPv6 alongside IPv4 will also enable organisations to retain and improve their capacity to be reached by everyone in the future. It is expected that making services provided by the public sector available via IPv6 will accelerate the deployment of IPv6.

A number of reports have already been produced describing why IPv6 is needed. This report is aimed at the next stage and offers a more practical orientation; its purpose is to provide support for IT staff when they are working on installing and commissioning IPv6 within their organisations.

Stockholm, 31 October 2011

Göran Marby
Director-General

Contents

Warning – do not remove this line

Sammanfattning

Dagens adresser på internet håller på att ta slut. En lösning finns, internetprotokollet IPv6. IPv6 innebär nya möjligheter och funktioner samt påminner om den tidigare standarden (IPv4). I denna beskrivning redogörs för hur man kan införa IPv6.

En utgångspunkt är att införa IPv6 vid sidan om IPv4. Ytterligare är att starta i tid, ta beslut om införande och tillsätta ett projekt. Dessutom att börja i liten skala och arbeta utifrån och in.

Inför IPv6 i fyra faser
IPv6 kräver ett systematiskt och kontrollerat införande för god tillgänglighet och säkerhet. Inför i fyra faser:

- Inventera; Gå igenom it-miljön och utred åtgärder för ett införande med bibehållen säkerhet och tillgänglighet. Anpassa upphandlingsunderlag med krav på IPv6 och se över behov av utbildning.
- Planera; Bestäm typ av adresser, ta fram en adressplan, beställ IPv6-internetanslutning. Upphandla ny utrustning och tjänster samt se över processer, rutiner och säkerhetskrav.
- Genomföra; Aktivera IPv6 först i internetanslutningen, konfigurera och driftsätt brandväggen och annan nätverksutrustning. Aktivera sedan IPv6 i publika e-tjänster som DNS, externa webbplatser och för e-post. Därefter möjliggör åtkomst till externa IPv6-tjänster på det interna nätverket. Kontrollera och övervaka införandet.
- Förvalta; Övervaka, följ upp, anpassa och hantera störningar.

Konsekvenser på tillgänglighet, säkerhet och ekonomi
Inför och förvalta IPv6 med samma kvalitet som för IPv4. Beakta att säkerhetsarbete är en löpande process. Ett ytterligare protokoll innebär en ökad komplexitet.

Kostnaden för införandet beror på flera faktorer. Exempel är behovet av ny hård- och mjukvara, antalet e-tjänster, nätverkets storlek och komplexitet, krav på säkerhet och tillgänglighet, utbildning och konsultstöd.

Förslag på fortsatt arbete
Offentlig sektor bör införa IPv6 för att kunna kommunicera med alla på internet. Det medför ökad efterfrågan på produkter och tjänster med IPv6 vilket påskyndar utvecklingen. PTS föreslår att statliga ramavtal beaktar IPv6.

Regeringen har i sin digitala agenda angett att myndigheter bör ha infört IPv6 senast 2013. För att möjliggöra detta föreslår PTS att myndigheten får i uppdrag att främja och följa upp införandet av IPv6 hos statliga myndigheter.

Abstract

Today's Internet addresses are running out. The Internet protocol 'IPv6' represents one solution. IPv6 entails new opportunities and functions, but resembles the previous standard (IPv4). The following describes how IPv6 can be deployed.

One starting point is to deploy IPv6 alongside IPv4. Others are to start on time, make decisions concerning the deployment and set up a project. Another is to start on a small scale, starting at the periphery and working towards the core.

Deploy IPv6 in four phases
IPv6 requires a systematic and controlled deployment for good accessibility and security. Four-phase deployment:

- Take stock: review the IT environment and investigate measures for a deployment that will maintain security and accessibility. Adapt procurement documentation with requirements for IPv6 and review the need for training.
- Plan: determine the type of addresses, produce an address plan, order IPv6 Internet connection. Procure new equipment and services and review processes, routines and security requirements.
- Activate: first activate IPv6 in the Internet connection, configure and commission firewalls and other network equipment. Then activate IPv6 in public e-services such as DNS, external websites and for email. After that, enable users on the internal network to access external IPv6 services on the Internet. Check and monitor the deployment.
- Manage: monitor, follow up, adapt and deal with disruptions.

Consequences in respect of accessibility, security and finances
Deploy and manage IPv6 with the same level of quality as IPv4. Take into consideration that security work is an ongoing process. An additional protocol entails increased complexity.

The cost of deployment depends on several factors. For example, the need for new hardware and software, the number of e-services, the size and complexity of the network, requirements for security and accessibility, training and the support of consultants.

Proposals for further work
The public sector should deploy IPv6 to make it possible to communicate with everyone on the Internet. This means an increased demand for products and services with IPv6, which will accelerate progress. PTS proposes that IPv6 should be considered in government framework contracts.

The Government has stated that public authorities should deploy IPv6 no later than 2013. To make this possible, PTS should be assigned to promote and follow up the deployment of IPv6 at government authorities.

1 Introduction

1.1 Government mandate

The Government has instructed the Swedish Post and Telecom Agency (PTS) to produce a description of how the new addressing standard IPv6 (Internet Protocol Version 6) can be deployed at an authority level (see Appendix 1). This description should take into account PTS's own experiences of IPv6 as well as the work of other stakeholders concerned.

The description is to serve as support when deploying IPv6. It will describe potential complications when deploying IPv6 within an organisation's public e-services and propose how such complications should be dealt with.

The description should explain the consequences of IPv6 deployment on accessibility, security and finances. An impact analysis should be conducted of IPv6 as a single protocol. A proposal should be submitted concerning how to administer and develop the eGovernment Delegation's guidelines for the deployment of IPv6.

1.2 Purpose and target group

The purpose of the description is for it to serve as support for stakeholders within the public sector when IPv6 is being deployed alongside IPv4. It includes a concrete description and guidance for practical implementation.

The primary target group for the description is staff whose work involves IT issues in an organisation, principally those responsible for public e-services. The description is consequently at a practical and technical level. The meaning of 'public e-services' in this description is explained in Section 1.5.

1.3 Scope and delimitations

This description describes the deployment of IPv6 in public e-services as well as within the necessary security-related functions with a view to maintaining a high level of accessibility and security.

It is stated in the assignment that PTS should conduct an impact analysis of IPv6 as a single protocol. As these protocols will coexist for the foreseeable future, a limited report is provided of IPv6 as a single protocol.

The description includes examples of common products and services. PTS does not ascribe any value in relation to the choice between these products and services.

The description does not replace training or courses in the subject. It describes a general methodology for implementation and proposes solutions.

1.4 Methods

This description is based on supporting documents from a consultancy report undertaken by Interlan Gefle AB. In addition, the report is based on the competence within PTS and the experience available at the authority following its deployment of IPv6.

This work has been conducted as a project. Erika Hersaeus, Joakim Aspengren, Anders Eliasson, Jonatan McEvenue, Anders Rafting, Roland Svahn and Petter Öhrn have participated in the project.

PTS consulted a number of stakeholders during the course of this work. These include the eGovernment Delegation, the Swedish Tax Agency, the Legal, Financial and Administrative Services Agency, .SE, CERT-SE and the Swedish Civil Contingencies Agency (MSB). A draft description has been subject to a broad consultation procedure involving a large number of stakeholders. Comments provided in the course of this consultation and the formal consultation have been incorporated into the description.

1.5 Terms and definitions

A number of terms and definitions are used in this description. This section provides an explanation of a few key terms, such as ‘public e-services’, ‘security’ and ‘accessibility’. Appendix 11 explains most of these terms.

‘Public e-services’ are delimited and defined in this description as those e-services that an organisation communicates externally with its users/customers. These include:

- Internet connections
- Firewalls with security functions
- DNS (servers that deal with address and domain name lookups, referred to as ‘internal resolvers’ and ‘external authoritative’)
- Websites
- Email communication (sending and receiving emails by email servers that support IPv6)
- Internal access to resources on the Internet that only support IPv6/Internet surfing from the internal network out on the Internet

Information security is often defined as the capacity to maintain the desired level of secrecy (confidentiality), accuracy and accessibility in relation to information and information assets. In this description, the term ‘information security’ is split into two parts: ‘accessibility’ and ‘security’.

‘Accessibility’ in this description means a service that is reachable, operationally secure, robust and in working order.

‘Security’ in this description means information security in the sense that systems and services can withstand intrusion, infringement, manipulation, etc.

1.6 Reading instructions

This description provides an overall approach to the deployment of IPv6. An introductory chapter sets out preconditions for the description. After that, Chapter 2 contains a general report on the deployment of IPv6. The subsequent chapters report on the four different phases of deployment. These are:

- taking stock in Chapter 3
- planning in Chapter 4
- activating in Chapter 5
- managing in Chapter 6

The concluding chapter contains proposals for future work relating to IPv6.

Several appendices supplement and provide more in-depth information to the main text. The appendices describe the reasons for deploying IPv6, tangible advice for deployment and also examples of solutions for products and services. The appendices also include the Government mandate and explanations of terms used, etc.

2 Deployment of IPv6

This chapter provides a description of the deployment of IPv6, which is the new addressing standard on the Internet. Appendix 2 reports on the reasons for the deployment of IPv6.

2.1 Deploy IPv6 alongside IPv4

Deploying IPv6 alongside IPv4 is referred to as 'dual stack'. The deployment of dual stack will facilitate, for example, communication with anyone on the Internet no matter if IPv4 or IPv6 is used.

The two standards are not compatible with each other. This means that deploying IPv6 as a single protocol will mean that you will be unable to communicate with those parts of the Internet that use IPv4. It is for this reason that dual stack is recommended.

2.2 Timely launch of the deployment

There are several advantages to launching the deployment of IPv6 in good time. Deployment costs can then be planned. A time-pressured deployment can also be avoided, which may affect accessibility and security. If too much time is taken to launch the deployment of IPv6, you may be forced into taking immediate action and there is a risk that solutions will be used that are not as suitable.

All components of the deployment work take time. The preparatory work takes time, and allowance should be made for the time this may take; taking stock of the internal IT environment and of the new hardware and software that supports IPv6 and that meets the organisation's requirements for security and accessibility. Moreover, procurement, including the production of security and functional requirements for equipment/software, and also the set up time from order to supply of IPv6 support, takes time and there is a risk of deployment, etc. being delayed.

In addition to this, staff will require further training to learn how to manage the new protocol (see Section 3.4).

2.3 Make a decision about deployment and set up a deployment project

It has transpired that the most difficult issue relating to IPv6 has been making the decision to deploy it within an organisation. It appears that organisations that have deployed or are well on their way to deploying IPv6 have had one or more real enthusiasts who have pursued the issue within their organisations. Making a start on the work to deploy IPv6 has often only called for 5-10 per cent of one manpower year.

Make a decision and set up a project to facilitate and improve the efficiency of IPv6 deployment within the organisation. Goal profiles and time schedules may vary depending on the decisions, needs and requirements of the organisation.

2.4 Start on a small scale, beginning at the periphery and working towards the core

There is some general advice that is important for maintaining a high level of accessibility and security. The basic advice is to start on a small scale. In the first instance, functions and services that an organisation communicates to users externally should be accessible over both IPv6 and IPv4 ('dual stack'). Other advice is to deploy IPv6 'starting at the periphery and working towards the core'. This means deployment in the following order:

1. Internet connection(s)
2. Firewalls including security functions
3. DNSs (referred to as 'internal resolvers' and 'external authoritative DNS')
4. Websites
5. Email communication
6. Internal surfing from the internal network out onto the Internet
7. Internal access to resources on the Internet that support IPv6

Deploying IPv6 for all of these functions and services at the same time is extensive and complex. There is therefore a risk that the transition will be too big to manage.

Define and prioritise the IPv6 deployment work based on the needs and resources of the organisation. Take advantage of the fact that IPv4 and IPv6 can coexist, and deploy IPv6 gradually.

2.5 Work in four phases – take stock, plan, activate and manage

The deployment of IPv6 requires a systematic and planned approach to maintain a high level of security and accessibility. Deployment should be structured in four phases. These are:

- taking stock

- planning
- activating
- managing

Some of the activities in the taking stock and planning phases may be carried out in parallel.

Activities and advice within each phase will be described in the following chapters. This approach is presented in chronological order.

3 Take stock

This chapter describes a number of activities that need to be implemented during the preparatory work to enable IPv6 to be deployed within an organisation.

3.1 Take stock of the IT environment

Before IPv6 can be deployed in networks and services, it is important to take stock of the organisation's IT environment. The aim is to identify the need for measures to enable services to support both IPv4 and IPv6, i.e. dual stack.

Document existing equipment as regards any requirements for changes so that both protocols are supported. This inventory will depend on the size of the environment and the quality of existing documentation.

Take stock of and document

- the server platforms affected with respect to software and hardware that support IPv6
- network equipment, network structure and addressing at a more overall level that supports IPv6
- client platforms (operating systems and software) that support IPv6
- services and functions for which there is internal responsibility and similarly functions for which a third party is responsible

Based on accessibility, security and finances, take stock of, for instance, the following functions:

- Internet connections
- Firewall solutions including security functions
- DNS solutions
- Web solutions
- Email solution
- Email filtering solutions
- Access switches
- L3 switches
- Access points for setting up wireless networks
- DHCPv6 servers
- VPN solutions
- Proxy solutions for activating IPv6 on client computers
- Administration tools
- Monitoring tools

Responsibility for services such as DNS, email and proxies may be under the organisation's own auspices or outsourced, depending on the needs of the organisation. See Section 3.2.4 for more information about services where responsibility lies externally.

3.2 Investigate proposed measures to deploy IPv6, retaining the level of security and accessibility

After taking stock of the IT environment, investigative work is required aimed at identifying appropriate measures. This relates to measures both to ensure that equipment can support both IPv6 and IPv4 and to ensure that security and accessibility is maintained.

3.2.1 Maintain security at the level of IPv4

It is important that there is no impairment of security when deploying IPv6. The security functions implemented using IPv4 must provide the same level of protection after IPv6 is deployed; something that is not always self evident. A common example is that devices can be addressed using IPv6, but its security functions cannot analyse and also block harmful traffic over IPv6.

3.2.2 Take stock of suitable products

Take stock of suitable products in the market that support IPv6. Consider, for example, security, accessibility and finances (commercial software/hardware, open source codes).

Get information about IPv6 and the security support in the hardware/software concerned from the supplier of the product in order to ascertain its IPv6 maturity. When contacting the manufacturer, ask for a list of functions that support or do not support IPv6.

Check that products supporting IPv6 also provide an equivalent administrative interface as when managing IPv4. In some cases, the existing interfaces of products cannot be updated with respect to IPv6. The user is reduced to managing IPv6 functionality via configuration files or a command interpreter, something that could impede day-to-day work.

3.2.3 Conduct a risk and vulnerability assessment for the deployment

Conduct a risk and vulnerability assessment to assess risks and threat profiles. Supporting documents for the assessment are the results of the inventory of software/hardware that support IPv6 and also security aspects.

Take measures to minimise risks and produce contingency plans on the basis of the risk and vulnerability assessment.

Organisations that have introduced an information security management system (ISMS) or that are systematically working with information security in some other way will consequently have methods and procedures for implementing a risk assessment. It may be appropriate to use these methods and procedures in conjunction with the deployment of IPv6.

3.2.4 Investigate whether responsibility for services is under own auspices or outsourced

A review should be conducted as part of the work of taking stock or planning, encompassing who is responsible for public e-services such as for instance the web, DNS (the domain name system) and email communication. One alternative is for this to be done internally; another is to outsource the task. Legal and security requirements should also be considered when making this choice. The result will affect what needs to be considered in future work, e.g. specifying requirements and procuring services.

A correctly structured DNS infrastructure represents a precondition for functioning IPv6 communication, regardless of whether the responsibility for DNS lies internally or externally.

See Appendices 3 and 4 for more tangible advice.

3.2.5 Produce an action plan for transition

Produce an action plan of what needs to be done to ensure that functions and services support dual stack while maintaining a high level of accessibility and security.

3.3 Adapt framework contracts and procurement documentation with requirements for IPv6

It is appropriate to specify requirements for IPv6 support when conducting regular reviews of procurement documentation relating to electronic communications services. In addition to this, security and accessibility requirements should also be considered. In this way, the deployment of IPv6 will not entail any direct additional costs in this respect.

If this has not been done, the documentation must be adapted prior to the deployment of IPv6.

Appendix 3 provides more tangible advice to consider when specifying requirements.

3.3.1 Use the Legal, Financial and Administrative Services Agency's framework contracts for IT and telecommunications

The Legal, Financial and Administrative Services Agency has several framework contracts within the area of IT that can be used by public authorities, municipal authorities and county councils. Their purpose is to coordinate purchases to achieve savings. The framework contracts can be found at http://www.avropa.se. They have been grouped into several fields, such as

- Data communications, networks and telephony
- IT operations services
- IT consultancy services (e.g. contract consultants)
- PCs and services
- Software and services
- Servers, storage and services closely linked to products
- IT training
- e-Government support services

These contracts have been formulated in different ways and have different levels of detail, which means that each organisation must consider its own needs and proceed on the basis of these needs. It is currently possible for purchasers to introduce requirements for IPv6 in their own orders.

The contracts make it possible to obtain both services and products. Examples of services include

- IT training relating to IPv6
- Contract consultants to produce an implementation plan for IPv6

3.3.2 Specify requirements according to recommendations

This section provides examples of organisations and fora that have produced advice when specifying requirements. This may be helpful when specifying requirements. However, you must make your own assessment based on your situation.

RIPE is the Internet Technical Community in the European and the Middle Eastern region. RIPE has produced a document with recommendations about IPv6 in ICT equipment (RIPE 501). It is intended that this document should serve as support when producing new ICT equipment that supports IPv6. It lists requirements to consider for various kinds of equipment related to the Internet. This document can be found at http://www.ripe.net/ripe/docs/ripe-501 (in English). Further improvements are likely to be made to this document.

NIST (National Institute of Standards and Technology) in the United States has produced a specification of recommendations to use as a basis when specifying requirements for new equipment (Buyer's guide, http://www.antd.nist.gov/usgv6/).

3.4 Take stock of training needs

It is appropriate to review the IPv6 training requirements for IT staff in the course of the work involved in taking stock and planning (i.e. before deploying IPv6). Courses that explain the differences between IPv4 and IPv6 are of particular value. It is also important for such a course to describe all aspects of IPv6 deployment, i.e. also cover security and accessibility aspects, etc.

A few days' training is generally sufficient if members of staff are already competent with IPv4.

4 Plan

This chapter provides tangible advice on how to plan for IPv6 deployment. Plan the deployment of IPv6 based on the action plan produced when taking stock (see Section 3.2.5). This will facilitate implementation and may also reveal any incorrect assessments.

Activities within taking stock and planning may be performed in parallel. The planning phase includes several important components for a carefully prepared deployment.

4.1 Plan addresses

RIPE NCC's responsibility includes managing and administering IP addresses in the European and the Middle Eastern region. RIPE has produced a policy for how IPv6 addresses may be assigned (RIPE-523) to its LIRs (Local Internet Registries).

4.1.1 Decide on the type of IPv6 address

There are two different types of IP address: Provider Independent (PI) addresses and Provider Aggregatable (PA) addresses. Allow sufficient time for investigating which type of IP address should be used.

With PI addresses the organisation can keep its IPv6 addresses (i.e. its network structure) in the event that there is a change of Internet Service Provider.

In order to be granted PI IPv6 addresses, the applicant organisation needs to be multihomed (have Internet connections to at least two different suppliers). It is important to remember that the border router for the Internet Service Provider will need to support Border Gateway Protocol (BGP) and IPv6 if PI addresses are to be used. It may be demanding for a small organisation to start multihoming and to apply BGP. Broad use of PI addresses has disadvantages for the global Internet and the routing tables.

IP addresses cost nothing. However, there is an annual charge to cover RIPE NCC's administrative expenses, which amounts to a couple of thousand Swedish kronor per year.

4.1.2 Applying for PI addresses

The organisation needs to do the following in order to apply for and be granted PI addresses:

- complete the relevant application form (IPv6 PI Assignment Request Form, RIPE 467), see RIPE NCC's website http://www.ripe.net/ripe/docs/ripe-467, and for instructions http://www.ripe.net/ripe/docs/ripe-483
- conclude an agreement with LIR, among other things regarding the provision of current contact details for the organisation at any time and how IPv6 addresses may be used (Contractual Requirement for Provider Independent Resources Holders in the RIPE NCC Service Region). A signed original must be sent to LIR or RIPE NCC

More information about the agreement may be found at the following link: http://www.ripe.net/lir-services/resource-management/direct-assignments/independent-assignment-request-and-maintenance-agreement. See also Section 5.2.1.

The address block will be assigned to the organisation when a correct application and signed agreement have been sent to RIPE NCC or via its LIR.

4.1.3 Applying for PA addresses

When using PA addresses, the organisation will have to renumber its networks in the event that there is a change of Internet Service Provider. Contact your LIR to apply for PA addresses. No agreement needs to be concluded with a foreign organisation. Nor is any knowledge required about how to deal with global routing or maintain RIPE's database.

4.2 Produce an address plan

An Internet Service Provider or an LIR normally allocates a 48-bit prefix to organisations that apply for IPv6 addresses. This (/48) means more IPv6 addresses than are generally available for IPv4 addresses. More specifically it means 65,536 x 64-bit subnets (or LAN segments). A 64-bit subnet is the minimum recommended subnet mask in an IPv6 network and provides $1.8*10^{19}$ addresses. A subnet mask defines by number of bits which parts of the IP address are networks and which are host portions.

A well thought-out network structure and address plan represent a precondition for functioning IPv6 communication.

There are several ways in which to create an address and network structure. The deployment of IPv6 provides good preconditions and opportunities for reviewing your address plan. Another way is to base this on your existing address plan for IPv4 addresses.

Plan and document a network structure and address plan for IPv6. Also decide how to assign dynamic addresses: SLAAC or DHCPv6. Support for assigning addresses via DHCPv6 varies between client operating systems. There are pros and cons for both DHCPv6 and SLAAC. The final selection should be based on each organisation and made on a case to case basis. DHCPv6 affords better control over the addresses that computers are assigned. This is because you are allowed to define an address space within which addresses are assigned. Addresses are assigned randomly with SLAAC. This means that you have no control over the source address and it will generate more addresses.

The time required to produce an address plan depends on the size and complexity of the infrastructure. It will take a relatively short time for small organisations with few segments. It is more complex and will take longer for larger organisations with several hundred connections.

It is important for the address plan to be well-documented and kept up-to-date.

See Appendix 5 for more information on how to produce an address plan. Furthermore, the SURFnet organisation has produced a manual that may help (Preparing an IPv6 Addressing Plan –Manual, http://www.surfnet.nl/en/nieuws/Pages/IPv6numberplan.aspx).

4.3 Order IPv6 Internet connections from an Internet Service Provider

You are now in a position to investigate whether your Internet Service Provider can provide an IPv6 Internet connection (i.e. a native connection, not tunneled). If they can, you should then ask how long the supply will take. Ask your Internet Service Provider for IPv6 references; do they have experience of the technology, do they have other IPv6 customers, etc. One important issue when specifying requirements relating to Internet Service Providers is whether they can supply transit for multihoming using BGP, not just capacity.

Different kinds of IPv6 address are required depending on whether the organisation intends to be multihomed (see Section 4.2.3). Decide which kind of IPv6 address the organisation should apply for.

It is important to specify and get the same SLA requirements for the IPv6 connection as for IPv4.

Consider consulting another provider for the provision of an IPv6 Internet connection if the service cannot be supplied with the same SLA requirements or if the supply will take too long.

One recommendation is not to use a supplier that sets up a tunnel to the customer's CPE as a solution for the live operation of an IPv6 Internet connection. However, this may function in a laboratory context.

The Legal, Financial and Administrative Services Agency's framework contracts may provide support when ordering Internet connections over IPv6; see Section 3.3.1.

Appendix 3 provides more tangible advice to consider when setting requirements.

4.4 Procure new equipment and services

Before proceeding with a procurement of new equipment (hardware/software) and services (Internet connections, DNS, the web, email servers, etc.), adapt documentation to take account of IPv6 support and security aspects. Remember that this normally takes time.

Procure the equipment and services required to deploy IPv6 within the organisation.

See Sections 3.2.4 and 3.3 regarding the work to take stock in respect of these issues. Appendix 3 provides more tangible advice to consider when setting requirements.

4.5 Review processes, procedures and security requirements so that they cover IPv6

Before deploying IPv6 in the organisation, it is important to review the existing processes and procedures so that they cover IPv6 traffic and networks.

Traffic over IPv6 should be operated and managed with the same level of quality and care as for IPv4. One example is that risk and vulnerability analyses can be reviewed so that they take account of IPv6 traffic/threats. There should also be procedures for penetration tests.

Organisations that have introduced an information security management system (ISMS) or that are systematically working with information security in some other way will have methods and procedures that may be used in conjunction with the deployment of IPv6.

4.5.1 Produce a continuity plan

It is important for the organisation to produce a continuity plan for the eventuality of an interruption or disruption arising. The purpose of a continuity plan is to be prepared for and capable of dealing with undesired events, such as, for instance, interruptions and disruptions that may occur in public e-services, IT and administrative systems etc., in a quick and systematic way.

This plan should also ensure that the operation can be run on a limited scale but under controlled conditions in the event of any disruption to IT support.

Continuity planning also means taking measures to prevent or minimise the effect of an undesired event.

A continuity plan for IPv6 may broadly resemble the plan for IPv4.

5 Activate

Activation can start after the taking stock and planning work. Activation comprises deploying IPv6 through gradual and controlled activation and commissioning. Supervision is required after each commissioning to maintain good function, security and accessibility, etc.

5.1 Activate IPv6 Internet connections

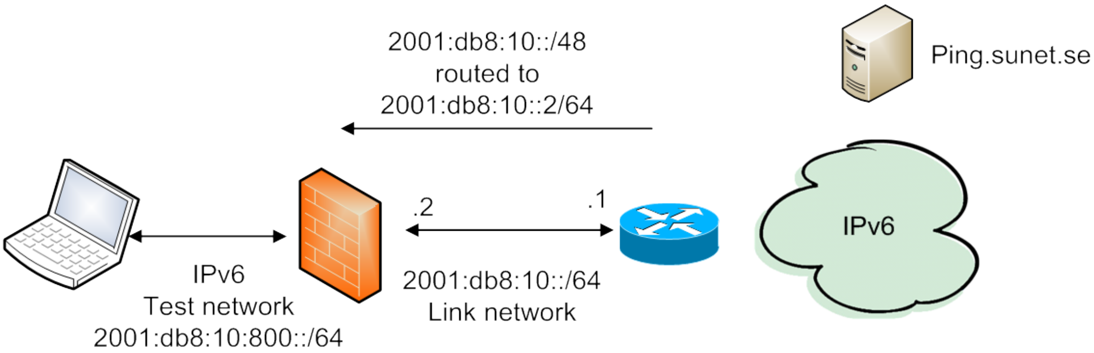
The first stage of activation is for the Internet Service Provider to supply an IPv6 Internet connection.

5.1.1 Verify that traffic is functioning

When an Internet Service Provider has activated IPv6 up to the firewall, it is important to check that the address space assigned is functioning. Configure any of your own routers that are directly connected to the Internet Service Provider (border routers or default gateway routers). Check that IPv6 has been correctly routed from the operator. This is done by connecting a computer on the inside and conducting tests through the firewall. Do this from an isolated network so that you do not advertise IPv6 at a location where this is not wanted or if you are unsure about what you are doing.

One test command for verification is `ping -6 ping.sunet.se`. If this does not work, test using `tracert -6 ping.sunet.se` (traceroute in Linux and Unix).

The following diagram shows a possible activation of IPv6 in relation to an Internet Service Provider:

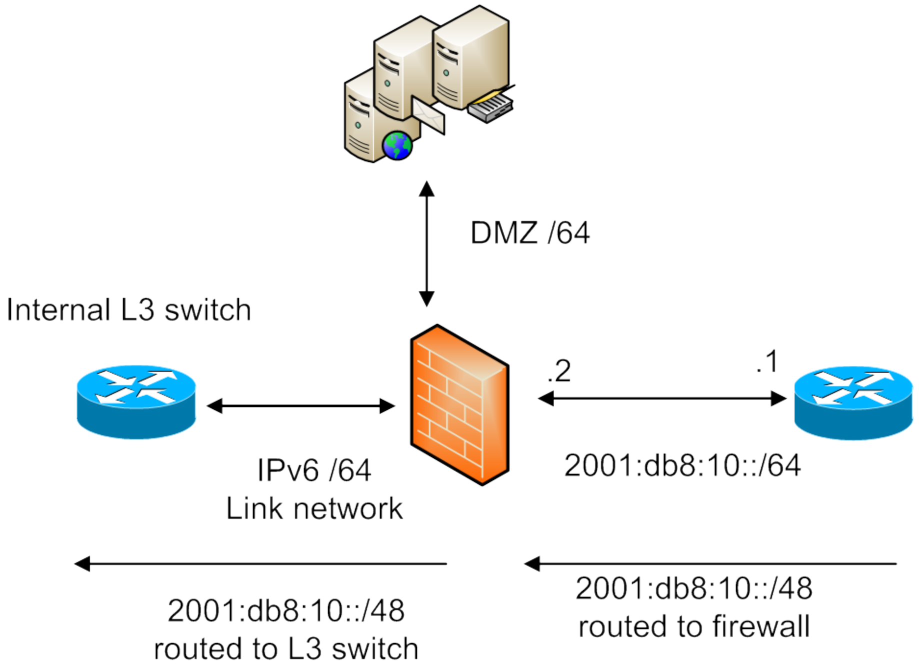


Problems and interruptions, including delays and connections that are not functioning, are common if no function checks have been conducted.

5.2 Distribute assigned addresses based on the address plan

The deployment of IPv6 can continue when the Internet connection has been activated and checked. The /48 assigned to you should now be distributed to the segment where IPv6 is to be activated.

One way is to route the entire prefix /48 in the L3 switch and set up a 'null route' (blackhole route) for this prefix. A null route should be set up to prevent routing loops in the network. The following diagram shows how the /48 is routed one step further into the internal central switch ('the L3 switch'). Remember that if the entire /48 is routed in and the null is routed, the prefix(es) in the firewall must be routed back to the firewall.



Null routes can be set up as follows:

```
ip route 2001:b48:10::/48 null 0
```

5.2.1 Considerations when using PI addresses

When PI addresses are deployed, a route6 object needs to be generated in RIPE NCC's database. There should be a route6 object available if you search in the address space in the database; see example for PTS below:

```
route6:       2001:67c:dc::/48
descr:        PTS
origin:       AS50273
mnt-by:       RESILANS-MNT
source:       RIPE
```

If there is no route6 object, it is unlikely that the addresses will be routed everywhere on the Internet.

5.3 Configure the firewall for IPv6

IPv6 can be activated in the firewall after the Internet Service Provider has activated IPv6 for your Internet connection and this has been checked.

The configuration and activation of firewalls include numbering the interface in the firewall according to the address plan produced, establishing the rules that will apply, etc. See Appendix 5 for more specific advice on how this can be done.

5.3.1 Considerations relating to ICMPv6 in the firewall

Ping and ICMP are considered to be unsuitable protocols in IPv4 communications and they are consequently often filtered out in the firewall. ICMPv6 is thus fundamental for IPv6 traffic. Find out which types of ICMPv6 your network needs to allow. Do not filter out unknown ICMPc6 types. If these need to be filtered, filter out no more than ICMPv6 Echo Requests and only from the Internet (not from the internal network) and ICMPv6 Echo Responses.

Neighbor Discovery Protocol (RFC 4861 http://tools.ietf.org/html/rfc4861, NDP) is fundamental to IPv6 and uses ICMPv6. NDP corresponds to, among other things, Address Resolution Protocol (ARP) in IPv4. You should consequently be careful when filtering because an error will stop IPv6 from working.

See RFC 4890 (http://www.ietf.org/rfc/rfc4890.txt) for more recommendations about filtering ICMPv6.

5.4 Configure and commission routers, switches and other network equipment

Activate IPv6 gradually in the switches and routers needed in order to achieve the first deployment targets.

Turn off Router Advertisement (RA) so that servers cannot autoconfigure their IPv6 address using SLAAC. This is done to prevent any unplanned servers becoming IPv6 activated (IPv6 Enabled). This provides more control over which servers are to become IPv6 Enabled and makes troubleshooting easier.

5.5 Activate IPv6 for server platforms

Deploy IPv6 in one server at a time. Before activating IPv6 in any more functions and services, it is important to test that the service is functioning as it should, that it has a high level of accessibility, and security and does not have a negative effect on other services. Do this by, for instance, setting up monitoring and logging for the service.

5.5.1 Activating IPv6 in DNS

Most DNS servers support IPv6. See Appendix 6 for more tangible advice on how to activate IPv6 in DNS.

See Appendix 3 for more advice on specifying requirements for IPv6 support for DNS.

5.5.2 Activating IPv6 for public websites

IPv6 is currently supported by most web servers, including their operating systems, CMS (Content Management Systems) and web engines (e.g. Apache).

Activate IPv6 in the operating system if the internal organisation is responsible for the public website. Configure server software to listen to IPv6 addresses and review any configurations of hosts and CMS. If CMSs are used, they will usually automatically function with IPv6 as they are built as a supplement to web servers.

In order to be able to activate IPv6 on the web server, the entire chain from the Internet Service Provider, firewall up to the web server needs to function well over IPv6. It is advisable not to set up any AAAA RR in the real name on the web server. Set up a temporary name for the Internet service in DNS or a host file instead, where AAAA RR is entered to verify the function before the web server with IPv6 is put into full live operation.

If an external supplier is responsible for the web service, it is important to specify requirements for IPv6 support when procuring the service. Furthermore, it is important that peripheral functions for the web service support IPv6 traffic, such as for instance keeping statistics, so that the organisation's traffic and traffic patterns can be measured (number of visits, etc., over IPv4 and IPv6 respectively).

It is important to use load balancers/proxies to ensure the capacity of the web server. In this case the load balancer must support IPv6, while IPv6 support in the web server is no longer required.

5.5.3 Activating IPv6 for emails

There are several solutions for how to conduct email communications over IPv6 (MTA, email relays, email servers). See Appendix 6 for more information about this.

There are several different items of hardware and software for filtering spam and viruses in email communications. Check the IPv6 status, and how IPv6 is activated with the manufacturer.

5.6 Enable access to external IPv6 services for client computers on the internal network

Access to external IPv6 services for client computers on the internal network can be achieved in many different ways. It can be done either by activating native IPv6 or by activating IPv6 in a proxy server. The method chosen depends on the existing environment, the proxy used (support is not available for all) and the internal infrastructure.

Enabling via Native (Section 5.6.1) or a proxy (i.e. the first solution in Section 5.6.2) is preferable because it is simpler to activate and maintain than other proposals. The second solution proposed (5.6.2) is a quick method and should be regarded as a temporary solution.

5.6.1 Activating Native IPv6

All modern operating systems in client computers support IPv6. By activating IPv6 in the internal network, the computers in question can reach external computers/resources that support IPv6 or IPv4. IPv6 support for all conceivable services and functions can be achieved using a native solution that does not normally use a proxy server, e.g. IP telephony.

5.6.2 Alternative activation through a proxy

Examples of solutions to activate IPv6 in client platforms through a proxy are:

1. If the proxy server supports IPv6, it is easy to activate IPv6 for all computers that are using it.

2. Policy-based routing can be applied if the proxy does not support IPv6. In this case the router reroutes, for example, HTTP traffic for IPv4 to the proxy, whereas HTTP for IPv6 passes through. This should be regarded as a temporary solution. If an external supplier is responsible for the proxy service, you should specify requirements for IPv6 support from this supplier. If the supplier cannot offer this support, consider allowing another provider to provide the service.

3. A third proposed solution is to set up a proxy with IPv6 support in front of the unsupported proxy.

The last two solutions can be applied if, for example, the existing proxy has identity management, filters content and/or virus scanners.

Today, proxy and security services are also provided via cloud computing. When using such a solution, the organisation should specify requirements for IPv6 support for this. See Appendix 10 for proposals if an open source code is a solution over a proxy solution.

5.7 Check and monitor

When IPv6 has been activated, it is important to monitor and follow up that traffic and traffic patterns remain at the same level and have the same security requirements as for monitoring and the statistics held for IPv4. See Section 6.1 for more information about monitoring.

6 Manage

When IPv6 has been deployed, ongoing management is required to maintain good function and technical security (i.e. operational and information security in services and networks). Management involves monitoring, adjusting and adapting the technology.

6.1 Monitor, follow up and adapt to maintain security and accessibility

It is extremely important to monitor services when deploying a new and an additional protocol in the network. This enables the detection of abnormal conditions in terms of traffic volumes, performance, response times, etc. Monitoring using alarms enables the organisation to respond rapidly.

Monitoring tools for IPv6 can comprise both commercial tools and software with open source codes. Examples of monitoring tools can be found in Appendix 10.

6.1.1 Monitoring IPv6 traffic and differentiating alarms from IPv4 and IPv6

Some monitoring software cannot distinguish from the alarms whether the interruption relates to IPv4 or IPv6 communications. It is therefore important to differentiate whether the alarm from monitoring involves IPv4 or IPv6. The purpose of this is to be able to take measures to deal with interruptions and disruptions. There should be same quality of monitoring for IPv6 as for IPv4.

In order to be able to differentiate between alarms from IPv4 and IPv6, you can set up different names for different servers, e.g. for a web server. Monitoring can, in the manner shown below, trigger an alarm for all possible combinations for IPv4 and IPv6 traffic in the event that any of the protocols is not functioning:

- http://ipv4-only.myndighet.se (only IPv4, A RR)
- http://ipv6-only.myndighet.se (only IPv6, AAAA RR)
- http://dualstack.myndighet.se (both IPv4 and IPv6, A and AAAA RR)

6.1.2 Keeping operational statistics for traffic volume and accessibility

It is important to keep statistics relating to traffic volume and accessibility to various services. This is how you can find out whether IPv6 is functioning as it should. Information about traffic volume can also be good for making adaptations to ensure that equipment can cope with traffic volume. One example is whether a small IPv6 firewall needs to be upgraded.

If your firewall does not support the MIB (Management Information Base) function for IPv6 traffic, separate statistics for IPv4 and IPv6 can be gathered using one interface for IPv4 and one for IPv6 in relation to the Internet Service Provider.

6.1.3 Keeping logs

It is important to keep logs when deploying a new protocol in the network. Ensure that the log servers support IPv6. The organisation's system for receiving syslog, netflow etc. should support IPv6 traffic, although this cannot always be taken for granted.

Keeping a log documents what is happening in the network and facilitates follow-ups, etc.

6.2 Dealing with interruptions

Various forms of interruption may arise. This section provides some advice for how to deal with these in a systematic and satisfactory way. Appendix 4 provides advice about the action to be taken in the event that interruptions or disruptions arise in certain services.

6.2.1 Document incidents and follow up causes

Document any incidents systematically. Do this so that it is possible to follow up causes of interruptions and disruptions. This also makes it possible to report faults relating to bugs to suppliers.

IPv6 still does not have the same level of maturity as IPv4 as it has not been applied for as long and to the same extent. For this reason, it is particularly important to follow up any problems and obstacles. This gradually leads to better functionality.

6.2.2 Contact CERT-SE in the event of IT incidents

Contact MSB/CERT-SE for support and assistance with measures in the event of interruptions or disruptions where there is a suspicion that these have been caused by attacks or security problems associated with products. The contact details for MSB/CERT-SE are:

Email address: cert@cert.se
Telephone number: +46 (0)8-678 57 99

CERT-SE is Sweden's national CSIRT (Computer Security Incident Response Team), which has the mandate to support society in its work to deal with and prevent IT incidents. The operation is conducted at the Swedish Civil Contingencies Agency (MSB).

7 Proposals for future work

This chapter reports on a number of proposals for future work relating to IPv6.

7.1 The public sector should deploy IPv6

Statistics show that there are few stakeholders within the public sector that support IPv6 in their public e-services (see http://www.myndighetermedipv6.se and http://www.kommundermedipv6.se). Only five per cent of administrative authorities support IPv6 in their public websites, seven per cent in their email systems and approximately 30 per cent support it in any of their DNS servers. Just over one per cent of municipal authorities support IPv6 in their external websites.

Measures should be taken to ensure that the public sector deploys IPv6.

7.1.1 Public authorities should have deployed IPv6 by no later than 2013

The Government stated in its Digital Agenda that public authorities should have deployed IPv6 by no later than 2013.

Stakeholders within the public sector play an important role in the transition to IPv6 in the form of purchasers and procurers. If stakeholders within the public sector specify requirements for IPv6 support in equipment and services, this will result in an increased demand for this equipment and these services, which in turn will mean that manufacturers can produce them. This applies to everything from requirements for Internet connections, network equipment, special customer-related equipment and administrative and monitoring tools. However, the services and applications will then also require IPv6 support. The deployment of IPv6 will bring with it the gradual development of the Internet. For this reason, the public sector should make a decision regarding the deployment of IPv6.

7.1.2 Government framework contracts should consider the deployment of IPv6

The Legal, Financial and Administrative Services Agency procures and administers framework contracts within, among other areas, IT and telecommunications that can be used by public authorities, municipal authorities and county councils (see Section 3.3.1).

It is important for framework contracts to take into consideration the deployment of IPv6 in both products and services within all areas. These framework contracts will constitute support, offering good preconditions for the deployment of IPv6. The framework contracts will thereby contribute to improving the efficiency of public authority purchasing processes, including the potential to save resources in the form of time and better prices.

7.2 The eGovernment Delegation's guidelines have been incorporated into PTS's description

The eGovernment Delegation has produced guidelines for the deployment of IPv6 together with SKL and the Stockholm County Association of Local Authorities. The aim of this guidance is to support public administration.

PTS has discussed the administration and development of the guidelines in consultation with the eGovernment Delegation. These discussions have resulted in the guidelines having been incorporated into PTS's description. The eGovernment Delegation's guidelines have thus been replaced by this description.

7.3 PTS should be directed by the Government to continue to promote the deployment of IPv6

The Government should instruct PTS to continue to promote the deployment of IPv6 through various measures to enable the objectives of the Government's Digital Agenda. The purpose is to facilitate the deployment of IPv6 in the public sector.

Examples of work tasks within the framework of an assignment may be

- monitoring the development of IPv6 deployment within central government authorities (imposing a requirement for reporting to PTS)
- implementing information activities
- arranging for the exchange of experience between public authorities
- conducting an assessment of whether there is a need to review this description up until 2013, when public authorities should have deployed IPv6

This assignment may be regarded as a continuation of the assignment reported here and also requires special funds in the future.

Bibliography

E-delegationens vägledning för införande av IPv6 [The eGovernment Delegation's Guidelines for the Deployment of IPv6], http://www.edelegationen.se/sida/vagledning-for-inforande-av-ipv6

.SE - Att gå över till IPv6, En guide om att övergå till IPv6 i ett medelstort företag [.SE – Transition to IPv6. A guide to IPv6 transition for medium-sized businesses], Jani Juvan, IP Solutions. Appendix Torbjörn Eklöv, http://www.iis.se/docs/IPv6-guide_MedBilaga1.pdf

Robust elektronisk kommunikation - vägledning för användare vid anskaffning [Robust electronic communications – guidance for users when buying], PTS-ER-2011:16

The Legal, Financial and Administrative Services Agency's framework contracts, http://www.avropa.se

National Institute of Standards and Technology (NIST), USGv6 Program, http://www.antd.nist.gov/usgv6/

Office of Management, OMB Memorandum M-05-22

OMB, Memorandum for chief information officers of executive departments and agencies, September 2010, Transition to IPv6

Preparing an IPv6 Addressing Plan, SURFnet, http://www.surfnet.nl/en/nieuws/Pages/IPv6numberplan.aspx

RIPE NCC, http://www.ripe.net/

ARIN, http://www.arin.net

Cisco First Hop Security, http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-first_hop_security_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Appendix 1 – Government mandate

PTS's mandate for IPv6

Government decision (N2010/7521/ITP)

The Government instructs the Swedish Post and Telecom Agency (PTS) to describe how IPv6 can be deployed at an authority level considering accessibility, security and finances. The purpose of this description is that it should serve as support for public authorities, municipal authorities and other organisations within the public sector when deploying IPv6. As part of this work, PTS will utilise the experiences gained by the Agency when it implemented IPv6 in parts of its IT environment in the spring of 2010. As part of its assignment PTS is also to conduct an impact analysis concerning the deployment of IPv6 as both a single protocol but also in coexistence with IPv4.

PTS should consider the work performed by the eGovernment Delegation, the Internet Infrastructure Foundation (IIS) and other similar work both within and outside Sweden. PTS should consult the eGovernment Delegation, other relevant public authorities and relevant stakeholders within the private sector. Within its work on the assignment, PTS should also gather experience from other public authorities and organisations that have implemented or are about to implement IPv6. The description should apply to both internal and external communications. PTS should also describe aspects relating to the security, robustness and functionality of communications and services when deploying IPv6 as well as any complications that may arise and how these can be remedied. The eGovernment Delegation produced guidelines for the public authorities' deployment of IPv6 during the autumn of 2010. PTS should make proposals concerning how these guidelines should be administered and developed in consultation with the eGovernment Delegation.

An interim report on the assignment should be submitted to the Government Offices of Sweden (the Ministry of Enterprise, Energy and Communications) no later than by 31 December 2010 and a final report together with a financial report no later than by 31 October 2011.

The costs of the assignment may amount to no more than SEK 750,000. The costs will be carried by appropriation 2:4 Information Technology: Telecommunications, etc., appropriation item 2. To the Government's appropriation within area of expenditure 22 Communications. SEK 200,000 of these costs shall be carried by the appropriation for 2010 and the remaining SEK 550,000 carried by the appropriation for 2011 subject to the precondition that the Riksdag (Swedish Parliament) grants this appropriation in accordance with the Government's Budget Bill for 2011. Any unused funds shall be repaid to postal giro (PlusGiro) account no. 957688-5, stating the decision's file reference number, no later than by 31 October 2011.

Background

The Internet Protocol (often abbreviated to 'IP') is the communication protocol used to transfer information over the Internet. Internet Protocol version 4 (IPv4) is the first version of IP and is currently the version on which the Internet is largely based. The Internet Corporation for Assigned Names and Numbers (ICANN) is the organisation that has the coordination responsibility for domain names and IP addresses. The latter are managed by the Internet Assigned Numbers Authority (IANA) function. IANA coordinates the management of IP addresses from the regional Internet registries which in its turn provides these to the Internet Service Providers.

ICANN states that the addresses for IPv4 will come to an end during the first six months of 2011. When this happens, there will be an increased need to implement the next version of the Internet Protocol (IPv6) so that it can coexist with IPv4 for a period of time. There will thus not be a complete transition to IPv6 in the short term, although this will be the case in the longer term. However, the use and dissemination of IPv6 will mean that it must be possible to reach the existing e-services that are produced using IPv6.

The eGovernment Delegation has been assigned to produce a strategy for, among others, the public sector's transition to IPv6 (Government Directive 2009:19). Within the framework of its assignment, the Delegation has produced guidelines for IPv6 deployment by public authorities. However, these comprehensive guidelines need to be supplemented with a concrete description and technical guidance for the practical implementation at the public authorities.

Reasons for the Government's decision

As IPv6 will increasingly be the only way for new users to communicate on the Internet, it is important to speed up the work to enable this technology to be implemented in Sweden. This is important for accessibility to Swedish public authorities' e-services. The public sector and in particular government administrative bodies should set good examples during this development. The

Government therefore considers that PTS should be instructed to prepare this description, focussing on technical solutions and models for implementing IPv6 in coexistence with IPv4.

On behalf of the Government

Anna-Karin Hatt

Anna Gillholm

Copies to

Prime Minister's Office/SAM
Ministry of Finance/BA/SF
Ministry of Enterprise, Energy and Communications/KLS
eGovernment Delegation
Internet Infrastructure Foundation

Appendix 2 – Background and reasons for deploying IPv6

This appendix reports on the background to and several reasons for deploying IPv6.

1 Background

1.1 Current addresses on the Internet are running out

Each computer, smartphone, tablet and other device on the Internet needs to be assigned a unique IP address to enable them to communicate with each other. The Internet addressing standard is IPv4 (Internet Protocol version 4). An IPv4 address is made up of 32 bits and enables 4,294,967,296 unique addresses (approximately 4.3 billion addresses).

These IPv4 addresses are running out. It is estimated that at some time in 2012 there will be no more addresses at a regional level to assign to organisations that want more addresses.

1.2 A standardised solution to the scarcity of addresses – IPv6

There is a new addressing standard – Internet Protocol version 6 (referred to as 'IPv6') – that will resolve the scarcity of addresses. IPv6 addresses are made up of 128 bits. This results in 2^{128} addresses or 3.4 x 10^{38} addresses (340,282,366,920,938,463,463,374,607,431,768,211,456). This means much more address space, which is likely to be adequate for the foreseeable future.

2 Reasons for deployment

There are several reasons for deploying IPv6.

2.1 IPv6 makes it possible to communicate with everyone on the Internet

At the current time, just under a third of the world's inhabitants are connected to the Internet. Most inhabitants in regions where access to the Internet is being rolled out over the next few years will probably use IPv6 communication. At the same time, there will be users that will continue to communicate using the old standard (IPv4) for some time.

Both standards – IPv6 and IPv4 – are two different communication protocols with different address formats that are not compatible with each other. They can run through the same cable, but cannot communicate with each other. It will be some time before all communication takes place over IPv6. For this reason it is extremely important that all organisations can support both protocols at the same time ('dual stack'). This will make it possible to communicate with everyone on the Internet.

2.2 IPv6 enables the future development of the Internet

By deploying IPv6, public administration and industry will continue to have access to the number of IP addresses required. This makes new innovations and business opportunities possible.

New IP-based areas of application will develop that require a large number of IP addresses. One example is the 'Internet of things' which will need a large number of IP addresses. The vision is to enable all of the gadgets that we surround ourselves with – everything from toasters and lamps to car keys and processors inside cars – to communicate with each other.

2.3 Starting in good time will facilitate the deployment of IPv6

IPv6 adaptations need to start in good time, among other things to gain access to the expertise required to help everyone who waited to the very last. Early deployment also means that there will be more time for learning and gaining experience before IPv6 is put into full live operation, as users will demand that it functions from the very first day.

No additional costs will arise if a requirement for IPv6 support is set out in the course of an ordinary procurement for an organisation. On the other hand, there will be additional costs if you are forced to implement an additional procurement to satisfy the requirement for IPv6.

2.4 IPv6 has advantages relating to security and end-to-end communication

IPv6 has a number of advantages when compared to IPv4. In the future we can count on an increased need for an unbroken encrypted end-to-end connection. By using IPv6 to eliminate the scarcity of addresses, address translation using NAT (Network Address Translation) will no longer be needed – at least in those cases where scarcity of addresses is the reason why it is being used. This means that sensitive communication can take place in a secure way and that personal privacy is protected. It should be noted that traceability becomes easier when everyone has an IP address, which has both its advantages and disadvantages – it is easier to combat undesired attacks at the same time as it makes requests for anonymity difficult.

Other advantages are of a more technical nature. For example, more effective routing through improved processing of information in the headers and the removal of check sums, which yields higher performance.

Appendix 3 – Advice concerning requirements

This appendix provides advice on requirements for IPv6 in various functions and services. Services and products need to support both IPv4 and IPv6, i.e. dual stack.

Sections 3.2.4 and 3.3 of the main text also deal with information relating to requirements when procuring products and services.

1 Comprehensive advice for high accessibility, operational reliability and information security

A point of departure is that there should be no major functional differences between a product or service that supports dual stack and one that only supports IPv4. The performance of both IPv4 and IPv6 should be similar.

Specify the same level of SLA requirement (i.e. accessibility requirements for up-time and down-time, response time, reinstatement time) for a service or function that has dual stack activated as for those over IPv4.

When dual stack has been activated in a service, computers and servers that are IPv6 Enabled will choose IPv6 first. If the service is down over IPv6, the service will choose IPv4, but in that case there may be long delays. It may even be the case that it does not choose to transfer over to IPv4 at all. This is sometimes referred to as 'IPv6 Brokenness'.

Requirements should be specified on the basis of the organisation's requirements for function, accessibility and security. As a rule, the more security functions (requirements) specified, the more expensive it is. Ensure that you are aware of the implication of the recommended requirements before specifying requirements.

2 Specifying requirements for Internet connections

Requirements to specify for Internet Service Providers are:

- Native IPv6 connections with PA or PI addresses (i.e. a non-tunneled IPv6 connection). If PI addresses are used, it is currently required that both Internet Service Providers and organisations manage BGP for IPv6 PI addresses.

- The Internet Service Provider's DNS resolver must support queries and lookups over IPv6.

- If the Internet Service Provider's email relays (Mail Transfer Agents) are used for outgoing email, this must be configured using IPv6.

3 Specifying requirements for firewalls

Firewalls must support IPv6. Their inbuilt security functions should also support IPv6. Some firewalls have UTM (Unified Threat Management) functions. This means that they may provide, for example, SPAM and antivirus protection, IPS (Intrusion Protection/Prevention System), IDS (Intrusion Detection System), VPN, filtering of content and domains, prevention of data leakage. It is recommended that firewalls have such shell protection.

4 Specifying requirements for DNS services under external management

DNS services comprise two functions: external authoritative and resolver. A resolver is often received from your Internet Service Provider when an Internet connection is acquired. DNS should not be both authoritative and a resolver at the same time.

When an external stakeholder is responsible for your DNS service, it is important to specify requirements for IPv6 for both resolvers and authoritative DNS. All modern DNS software supports IPv6.

If the organisation is responsible for a DNS service under personal management, ensure that the DNS software supports IPv6.

In order to create redundancy and a high level of accessibility to your DNS services, it is best practice to have at least two geographically separate authoritative DNSs, preferably with different AS numbers, that support IPv6.

5 Specifying requirements for your domain names and domain name services

Specify a requirement so that the domain name provider (DNS operator, registrar), which is responsible for your DNS service and at which your domains are registered, can manage IPv6 glue records. Some registrars deal with these, but not always through their ordinary web interface (GUI); e.g. by an email to their support department instead.

DNS operators should be chosen on the basis of the needs and requirements of the organisation based on IPv6 and also other requirements for security, reliability and redundancy for domain name lookups, e.g. using DNSSEC.

6 Specifying requirements for reverse DNS lookups

Specify a requirement that the reverse lookup service (ip6.arpa) of your Internet Service Provider and/or DNS operator supports IPv6.

Reverse DNS lookups over IPv6 are required in the same way as for communication over IPv4, e.g. just for reverse lookups in DNS (IP numbers for domain names) and for email communication.

7 Specifying requirements for web services

When responsibility for the web server has been outsourced, require the web service provider to have IPv6 support for your Internet service(s). Most operating systems and web servers currently support IPv6.

8 When procuring proxy services, require them to support IPv6

A proxy with IPv6 support can speed up and simplify deployment for major parts of the organisation. This may mean that your website can provide content over IPv6 or enable your employees to surf over IPv6 to external content on the Internet. It is then no longer as necessary for IPv6 to be activated in a web server.

9 Specifying requirements for email services and email filtering

If the responsibility for email servers and email filtering solutions has been outsourced, specify a requirement that both outgoing and incoming emails at the organisation support IPv6 and that spam and viruses are filtered for both incoming and outgoing emails.

When responsibility for an email solution is internal, remember that MTA and email filters must support IPv6.

10 Specifying requirements for switches

The requirement specification document RIPE-501 (http://www.ripe.net/ripe/docs/ripe-501) can be used as a supporting document to define and adapt requirements on the basis of the needs of the organisation when procuring switches. The aim of the requirements listed in this document is to ensure that there is security for the network in the form of information security. It should be possible to activate MLDv2 snooping to achieve a minimum level of security in the network.

Switches need to support multicast groups and Ethertype 0x86DD to enable IPv6 communication to function. Ethertype 0x86DD means that equipment at the link layer level can manage IPv6 packets.

11 Specifying requirements for access points for wireless networks

When specifying requirements for wireless network equipment, require the equipment to support IPv6, multicast groups and Ethertype 0x86DD, etc.

12 Specifying requirements for DHCPv6 servers

Specify a requirement that the DHCP server supports IPv6. A DHCP server can often be updated to a DHCPv6 server. Otherwise, acquire a DHCPv6 server.

DHCPv6 is available for both commercial and open source code solutions. There are also IPAM systems that support IPv6.

13 Specifying requirements for VPN solutions

Specify a requirement that a VPN solution over IPv6 for roaming clients (teleworkers, etc.) manages IPv6.

14 Specifying requirements for administration tools for dealing with the internal network

It is important that the tools used to administer the internal network support IPv6. Specify a requirement that the administration tools supports IPv6.

15 Specifying requirements for monitoring and logging systems

In addition to the organisation's other requirements for monitoring and logging systems, both of these should support IPv6.

16 Specifying requirements for client software with network support

Ensure that there is IPv6 support in client operating systems, applications (web browsers, chat, telephone conference systems), etc.

17 Specifying requirements for security software in client platforms

Specify a requirement for IPv6 security software in client platforms, i.e., for example, anti-virus and firewalls.

Appendix 4 - Advice for maintaining a high level of security and accessibility

This appendix provides more tangible advice for maintaining a high level of accessibility and security when deploying IPv6. This advice is set out in chronological order according to how the deployment should be implemented.

This appendix describes examples of advice and complications in common systems and software. PTS does not ascribe any value to such systems and software, but describes the existing IPv6 maturity/information in common systems on the market.

1 DNS

1.1 A precondition for functioning communication over IPv6 is to set up DNS correctly

It is important to ensure that DNS (i.e. addressing, common name lookups and reverse lookups) has been set up correctly to enable it to function properly and simply over IPv6. An orderly DNS structure for clients, servers and other equipment represents a precondition for properly functioning use of IPv6.

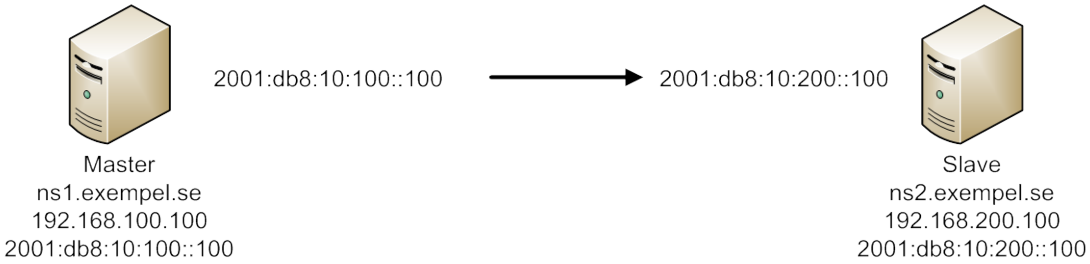
The length of the IPv6 addresses means that DNS will have an increasingly important role in the infrastructure.

Later versions of DNS software have support to respond to queries containing IPv6 information.

1.2 Considerations when activating IPv6 in DNS

When activating IPv6 on authoritative DNSs, the master will prefer IPv6 over IPv4. When a domain has changed, the master DNS sends a NOTIFY message to the slave server(s) about a change having been made. The slave will then not accept the NOTIFY message as it has the master’s IPv4 as master.

In the following diagram, the master is sending a NOTIFY message to ns2.example.se from its IPv6 address. ns2.example.se will not accept it. It will wait for SOA refresh RR before asking ns1 whether any change has been made. This may entail long delays before a change goes through.



In the following example for pts.se, a change may take up to four hours before it has been implemented on all slave servers.

```
dig +multiline soa pts.se
pts.se.             3600 IN    SOA majestix.pts.se.
hostmaster.pts.se. (
                    2011061302 ; serial
                    14400      ; refresh (4 hours)
                    3600       ; retry (1 hour)
                    604800     ; expire (1 week)
                    3600       ; minimum (1 hour)
                                        )
```

One solution to enable the slaves to activate changes in the master more quickly is for NOTIFY messages to be accepted from both IPv6 and IPv4 addresses. The following represents an example in ISC BIND. The settings are global for all domains in ns2.

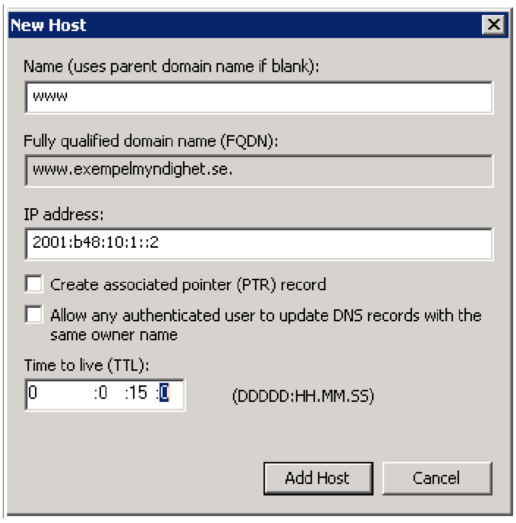
```
named.conf i ns2.exempel.se:
options {
         allow-notify { 192.168.100.100;
2001:db8:10:100::100 };
}
```

1.3 IPv6 and DNS TTLs

If a problem arises with IPv6, it is important not to set values that are too high on the TTLs (Time To Live) on your RR so that changes can be implemented/ take effect as quickly as possible, e.g. get out to the Internet. In this way you can minimise the effect of errors and rectify any problems. This represents more of a running in procedure than a long-term solution. When the IPv6 is operating well, the value of the TTLs can be increased again.

1.3.1 Windows DNS

In order to install the DNS's TTLs in a Windows DNS with a separate TTL for each RR, you normally have to do this via the menu Show -> Advanced. This is done in this way so that there are different values on TTL for IPv4 and IPv6. In this way you can quickly disable IPv6 for, for instance, a public e-service. The following diagram shows the settings in TTL for an IPv6 RR for a DNS.



New Host

Name (uses parent domain name if blank):
www

Fully qualified domain name (FQDN):
www.exempelmyndighet.se.

IP address:
2001:b48:10:1::2

□ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

Time to live (TTL):
0 :0 :15 :0 (DDDDD:HH.MM.SS)

1.3.2 ISC BIND

The TTLs for IPv4 and IPv6 respectively can be configured in ISC BIND as follows:

```
www   86400        IN    A                  192.168.1.10www
      1800         IN    AAAA         2001:db8:10:1::10
```

In this example, TTL for IPv4 has been set to twenty-four hours (86,400 seconds), while TTL for IPv6 has been set to 30 minutes (1,800 seconds).

1.4 Advice when using CNAME

It is advisable that if CNAME (Canonical Name Record or alias) is used, a large number of services can be activated for IPv6 without these having to be planned. If AAAA RR is activated on a server, all CNAMEs will be activated with IPv6 in relation to that name. Remember that CNAME can be linked to other domains so that it does not only have to be the second-level domain.

One suggestion is to set up a temporary subdomain name (e.g. http://www.ipv6.myndighet.se) with which you can test the service before the activation of IPv6 is put into live operation.

1.5 DNS, IPv4 and IPv6

A DNS that is only IPv4 Enabled can manage queries about IPv6 such as, for example, AAAA or ip6.arpa. A DNS that is only IPv6 Enabled can manage A and in-addr.arpa (i.e. make and respond to queries about IPv4). It is important to understand this so that IPv6-only DNSs are not set up to manage IPv6 RR, etc.

In order to illustrate how DNS can make and respond to queries over both IPv6 and IPv4 simultaneously, see the following two examples using the *dig* command that can be used to make many different kinds of query depending on flag. This asks over IPv4, but requests and receives an IPv6 (AAAA RR) as an answer.

```
dig +short aaaa www.pts.se @192.121.211.226
2001:67c:dc:1810::2
```

This asks over IPv6, but requests and receives an IPv4 (A RR) as an answer.

```
dig +short a www.pts.se @2001:67c:dc:43::227
192.121.211.215
```

2 Tunnels

This section provides advice on how to maintain accessibility and security in your network with respect to tunnels (6to4, Teredo and ISATAP in Windows and also VPN). The advice provided in this section should be considered before deploying IPv6.

2.1 Considerations for internal use of public IPv4 PA-/PI addresses and 6to4-tunnel in Windows

Some organisations use PA/PI IPv4 addresses in their internal networks. Problems will arise if the 6to4 tunnel has not been disabled when using PA/PI IPv4 addresses in the internal network (see following section).

If PA/PI is used in the internal network behind the firewall, the Windows computer/server will automatically generate a 6to4 address according to 2002:IPv4-address::IPv4-address and register this in the DNS if it is a member of an Active Directory. Other computers that are native IPv6 Enabled will then first attempt to reach computers over their unreachable 6to4 addresses, which may entail major delays.

2.2 Teredo and 6to4 in Windows can make the deployment of IPv6 difficult

Teredo and 6to4 tunnels are installed in Windows Vista/7 and Windows Server 2008. 6to4 currently has stability problems. One recommendation for reducing sources of errors for IPv6 is to disable both of these. There is also an RFC draft that recommends that 6to4 should be disabled globally on all hosts. Both Teredo and 6to4 also cause problems with native IPv6 in the internal network if you want to activate and use Microsoft's VPN feature Direct Access.[1]

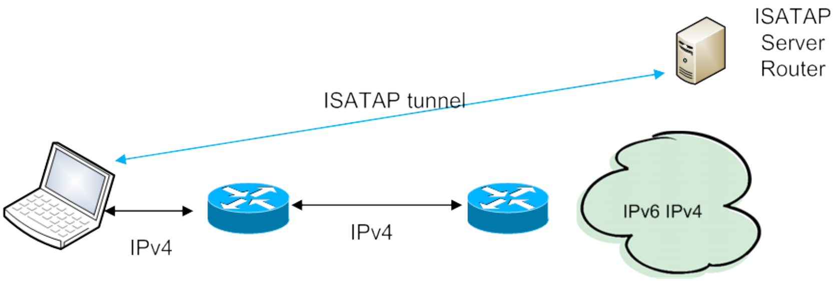
The following command will enable you to disable 6to4 and Teredo:

```
netsh interface teredo set state disabled
netsh interface 6to4 set state disabled
```

The tunnels can also be disabled using Group Policies in Active Directory.

2.3 Disable the ISATAP tunnel protocol

ISATAP is another activated tunnel in Windows. It is only used in the internal network and enables computers and servers to get IPv6 at locations where it is impossible or too expensive to activate IPv6 in the nearest router; see following diagram.



If ISTAP is not to be used, one recommendation is to disable it for reasons of accessibility. ISATAP can cause performance problems if a computer on the Internet tries to call up ISATAP. Disable ISATAP using:

```
netsh interface isatap set state disabled
```

ISATAP can also be disabled using Group Policies in Active Directory.

3 Other

3.1 Disable Router Advertisement

[1] See example on this link:
http://www.circleid.com/posts/microsoft_direct_access_is_it_heaven_or_hell_for_ipv6/

It is best to completely disable Router Advertisement (RA) in VLAN, where you do not want dynamic address assignment to apply (e.g. with SLAAC and/or DHCPv6). Such disabling may arise for a server LAN for which you may want to have static addresses.

The following example is for Cisco. The following command means you can disable RA, as only static addresses can be used on the VLAN in question.

```
interface vlan 100
    ipv6 nd suppress-ra
```

3.2 VPN tunnels

Establish rules for how VPN traffic may enter the organisation’s network. Do not allow tunnels that pass through and terminate inside the firewall without carrying out security screening for incoming traffic.

3.3 Filtering false routers can be circumvented

The purpose of Router Advertisement Guard (RFC 6105) is to filter Router Advertisements. Monitor and check that the filtering of false routers has not been circumvented so that measures can be taken when there is a solution to this problem.

3.4 Privacy aspects in IPv6

Privacy aspects for IPv6 have been dealt with and considered, for example, through Privacy Extensions for Stateless Address Autoconfiguration in IPv6 (RFC 4941).

The International Working Group on Data Protection in Telecommunications produced a document in 2002 identifying a number of threats/risks in relation to privacy that existed in IPv6 at the time. These are primarily dealt with by RFC 4941.

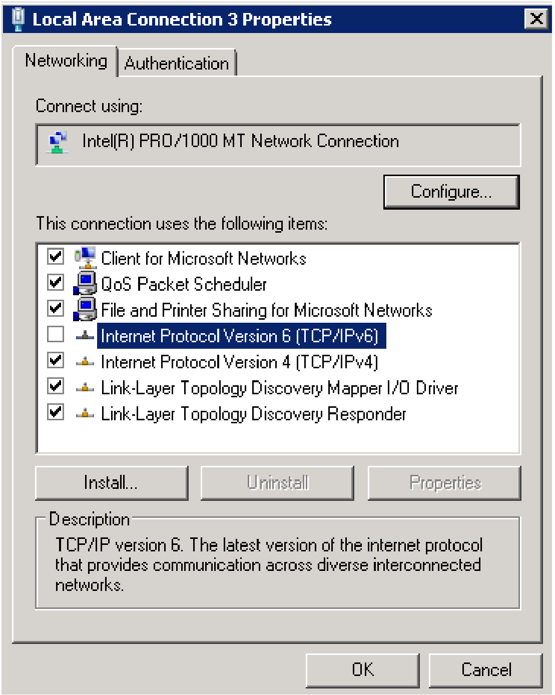
3.5 Block false routers and DHCPv6 servers

It is advisable to block false routers and DHCPv6 servers. This is done by activating DHCPv6 Snooping and Router Advertisement Guard if the access switches support this.

3.6 Disable IPv6 on the network card

If IPv6 needs to be disabled on a Windows computer (regardless of client computer or server), it is always advisable to disable IPv6 on the network card. Do not do this globally in the Windows computer, i.e. in a register, and then restart the computer. Disabling IPv6 on the network card avoids, for example, problems when IPv6 is to be reactivated in the computer.

Do the following to disable IPv6 in the network card:



Local Area Connection 3 Properties

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

3.7 Set up access lists for network devices

Remember to set up access lists for all network devices (e.g. routers). They should correspond to those that the organisation has for IPv4.

This can be done as follows:

```
ipv6 acess-list ssh
permit 2001:db8:10:200::/64 any
```

Appendix 5 – Advice on setting up an address plan

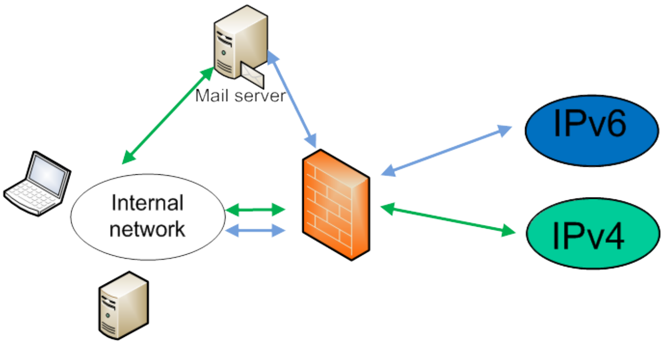
IPv6 addresses allow organisations to assign a large quantity of addresses (prefixes). This appendix therefore provides advice on how to set up an address plan for an IPv6 network (prefix) in an organised way.

See Sections 4.1 and 4.2 of the main text for comprehensive information about applying for and planning addresses.

1 Decide on how the address plan is to be set up

If the existing structure of the network is good, one method is to make a copy of this network and activate IPv6 according to the same structure on the VLAN and segment. This is a means of simplifying IPv6 deployment.

Another solution is to activate IPv4 on one interface (VLAN, segment) and IPv6 on another. Today, when many undertakings virtualise their environments, this is easy to do without incurring any additional high costs. See diagram for an example of two interfaces.



[Text for the diagram above: Change ‘Mailserver’ to ‘Mail server’, change ‘Internt nät’ to ‘Internal network’]

IPv6 deployment is otherwise a good opportunity to review your address structure and restructure the network if you are dissatisfied with your existing structure.

2 Assign your address block in a structured way

An Internet Service Provider, or an LIR, normally assigns a prefix of 48 bits to organisations that apply for IPv6 addresses. A /48 network means 65,536 networks (2^{16}). This means more IPv6 addresses than found overall for IPv4 addresses. More specifically, it means 65,536 x 64-bit subnets (VLAN or LAN segments). A 64-bit subnet is the minimum recommended subnet mask in an IPv6 network and provides 1.8 * 10^{19} addresses.

An example of assignment is where an organisation has been assigned 2001:db8:55::/48 (i.e. a /48). This means that 2001:db8:55:0000::/64 to 2001:db8:55:ffff::/64 will be assigned. The structure for your prefix (for the prefix and host components) will be as follows:

/48 assigned by Internet Service Provider	Available prefix (network)	Host component
2001:db8:55::/48	2001:db8:55:0::/64 – 2001:db8:55:ffff::/64	0000:0000:0000:0000 – ffff:ffff:ffff:ffff

Using a prefix size other than the standard /64
One advantage of IPv6 is that the same prefix size is used everywhere: /64. This differs from IPv4 where a large number of different subnet masks are used in order to economise on addresses. However, IPv6 and link networks between routers represent one exception. In this case there are several advantages to not using standard /64. One reason is that you do not have to use SLAAC, RA and other NDP-based protocols, which are unsuitable for link networks between routers. You can still take a /64, but use a /127 for the sake of simplicity and clarity.

Considerations for small networks
It is easier to number and structure internal networks for small organisations. The principle of these networks is also based on the form of the organisation's infrastructure. There are often fewer segments (VLANs), which makes it simpler to divide the VLANs.

If this involves, for example, an organisation that has centralised routing in a few L3 switches, the numbering of networks works on the basis of function and VLAN ID. The function and location is better suited if the routing for the organisation is highly decentralised (see the following section for explanation).

3 Set up an address plan based on your network structure

Two methods are shown below for setting up an address plan based on the network structure. They are:

- mapping the IPv6 network to the IPv4 network
- mapping VLAN IDs with IPv6

Mapping the IPv6 network to the IPv4 network
The following method can be used if address assignment for IPv6 is similar to that for IPv4. Do the following if the organisation has, for example, networks 10.123.0.0/16 assigned from 10.123.0.0/24 to 10.123.255.0/24:

10.123.0.0/24 => 2001:db8:55:0::/64
10.123.1.0/24 => 2001:db8:55:1::/64

10.123.254.0/24 => 2001:db8:55:254::/64 or alternatively 2001:db8:55:fe::/64
10.123.255.0/24 => 2001:db8:55:255::/64 or alternatively 2001:db8:55:ff::/64

Writing 55:255:: is the same, as 55:ff::.255 decimal corresponds to ff hexadecimal. The method of writing that you choose depends on how you would like to visualise the numbering.

Mapping VLAN ID with IPv6
Some consider it good to know the VLANs in which the IPv6 prefixes are located (geographical and physical; e.g. floor 5). This can be achieved in almost the same way as the IPv4 mapping above.

VLAN ID 154 => 2001:db8:55:154::/64 or 2001:db8:55:9a::/64

The advantage of the hexadecimal numbering above is that you get one more field to use and can then map more than just VLAN ID, e.g. to mark another function.

4 Number the network

The following shows three different methods of numbering a network.

Numbering based on function

We have chosen to number the IPv6 network according to function. Each function is given a unique address space; see the numbering in the following table. Although our IP telephones and most internal servers are not IPv6 Enabled from the outset, we have already included them in the plan. Our Internet Service Provider has assigned the organisation 2001:db8:55::/48. We have chosen to number the network as follows:

Prefix (hexadecimal)	**Function**
2001:db8:55:**1001**- 2001:db8:55:**1fff**::/64	Servers
2001:db8:55:**2001**- 2001:db8:55:**2fff**::/64	Desktop computers
2001:db8:55:**3001**- 2001:db8:55:**3fff**::/64	Wireless laptop computers
2001:db8:55:**4001**- 3001:db8:55:**4fff**::/64	IP telephony
Etc.	

Numbering based on function and VLAN

The VLAN standard enables up to 4096 VLANs per segment. This can be done in the following way if there is no need to use all 4096 possible VLANs and to make readability easier: we then use something that looks like decimal numbering, and VLAN ID 1-999 can be utilised.

Prefix (VLAN ID)	**Function**
2001:db8:55:**1001**- 2001:db8:55:**1999**::/64	Servers
Etc.	

Numbering based on VLAN

All 4096 VLANs can be used in the numbering if we do not use any introductory function number.

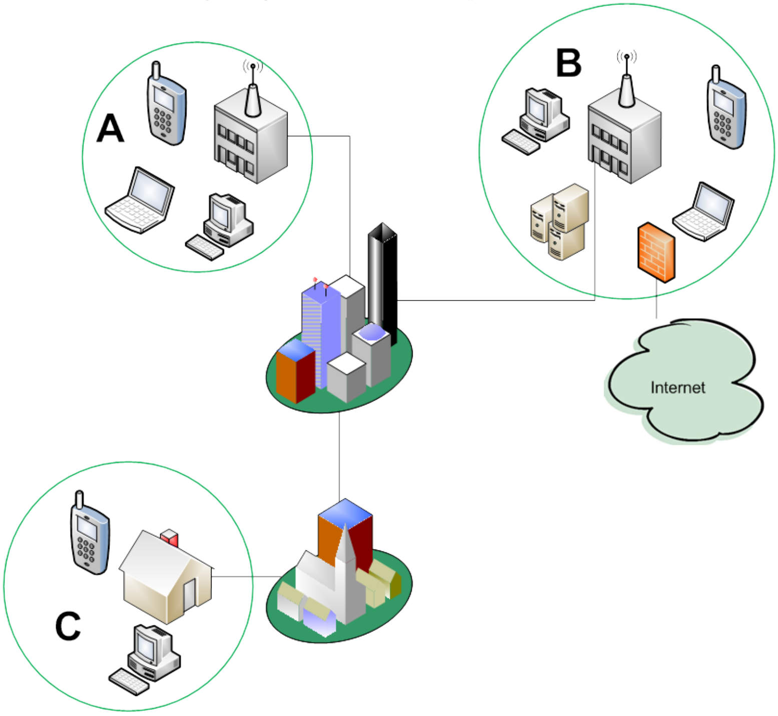
Prefix	VLAN
2001:db8:55:**0001**- 2001:db8:55:**4096**::/64	----

5 Examples of how to set up an address plan based on the network's structure

We are using a network that may belong to a county council, a large municipal authority or a public authority as an example. There are desktop computers and IP telephony units at all network locations. Laptops connect wirelessly at some locations and servers are located at one site. Desktop and laptop computers with wireless connections, IP telephony units and servers are split into different VLANs (segments).

Depending on the number of units connected, the desktop computers and IP telephony units are also divided into several VLANs per location. A VLAN ID is unique; no VLAN ID is found at several sites within an organisation.

See the following diagram as an example:



There are so many desktop computers and IP telephones at A and B that these are divided into different VLANs. There is a central L3 switch and the network is distributed out via L2 access switches. Location C comprises desktop computers and IP telephones.

Location B differs from locations A and C in that there is a central firewall. Public e-services are also located at a DMZ. The Internet connection enters at this location.

Numbering each VLAN and function

Number the network and decide how addresses are to be assigned (dynamic and static).

Location	Function	VLAN ID	IPv6 Prefix	Address assignment
B	DMZ	100	2001:db8:55:64::/64	Static
B	Server VLAN 1	237	2001:db8:55:ed::/64	Static
B	Server VLAN 2	238	2001:db8:55:ee::/64	Static
B	Stationary building 2	567	2001:db8:55:237::/64	DHCPv6
B	Stationary building 3	568	2001:db8:55:238::/64	DHCPv6
B	Wireless buildings 2 and 3	569	2001:db8:55:239::/64	DHCPv6
B	IP telephony building 2	570	2001:db8:55:23a::/64	DHCPv6
Etc.				

Assigning addresses within a VLAN

After a rough address plan has been drawn up in accordance with the previous section, it is time to number each /64. The assignment of addresses (static, dynamic) should be determined and planned for the internal network for various services. For example, there is a default gateway for each VLAN. Servers are assigned static addresses in this example. A decision should be made on the use of DHCPv6 assignment within a VLAN.

We always put the default gateway at the first address (1) so this is not shown in the following table. We have chosen to have no more than 255 hosts in a VLAN in order to resemble an IPv4 network.

Function	**Address assignment**	**Scope**
Servers	Static	2001:db8:55:**1**???::**1001**- 2001:db8:55:**1**???::**10ff**
Desktops	DHCPv6	2001:db8:55:**2**???::**1001**- 2001:db8:55:**2**???::**10ff**
Wireless laptops	DHCPv6	2001:db8:55:**3**???::**1001**- 2001:db8:55:**3**???::**10ff**
IP telephones	DHCPv6	2001:db8:55:**4**???::**1001**- 2001:db8:55:**4**???::**10ff**

Some security conscious people see disadvantages associated with DHCPv6 and static assignment as it is easier to scan networks and understand their structure. As this method affords good control of addressing, this is considered to outweigh the other alternatives.

The same final address may well be set for both IPv4 and IPv6 at those locations where static addresses are used. For example, a server that has 192.168.234.**77** is given the IPv6 address 2001:db8:55:1034::**77**.

Appendix 6 – Advice for activating IPv6

This appendix provides advice on how IPv6 can be activated in services and functions. Advice is provided in chronological order for how IPv6 should be deployed (i.e. starting at the periphery and working towards the core) and also first in public e-services and then in the internal network.

Advice is provided for a number of common environments.

IPv6 must be activated and tested in Internet connections before you can proceed with activation in equipment; see Section 5.1 of the main text.

4 Activate IPv6 in public e-services and security functions

This section describes how IPv6 is activated in firewalls, DNS, reverse lookups in DNS, the Internet, email servers and email filtering.

4.1 Activate IPv6 in firewalls

IPv6 can be activated in the firewall when the Internet connection over IPv6 has been provided and it has been verified that it is functioning up to the organisation’s firewall. Rules subsequently need to be set up in the firewall.

It is very important to configure the firewall correctly in order to maintain security in the network. In order to achieve this, it is conceptually important to always block incoming routed IPv6, as NAT does for IPv4.

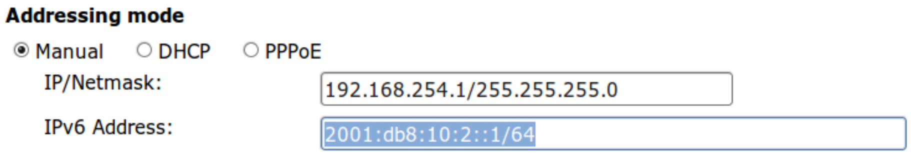
4.1.1 Number interfaces

Number interfaces in the firewall in accordance with the address plan produced (see Appendix 5). See below for an example of how this can be done.

Interface	Address	Possible static route
Internal	2001:db8:10:2::1/64	2001:db8:10::/48 via 2001:db8:10:2::10
WAN1	2001:db8:10:ffff::2	::/0 via 2001:db8:10:ffff::1

Etc.	--	--

The following examples show a typical administration interface for making firewall settings. The administration of the rules for IPv6 and IPv4 is fairly similar.

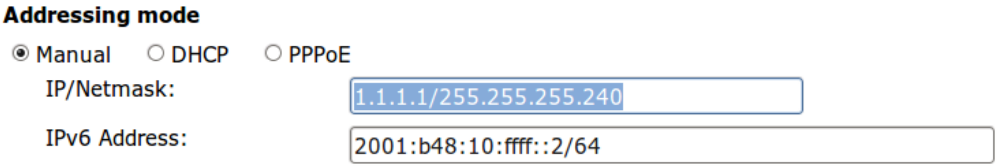


Addressing mode

● Manual ○ DHCP ○ PPPoE

IP/Netmask: 192.168.254.1/255.255.255.0

IPv6 Address: 2001:db8:10:2::1/64



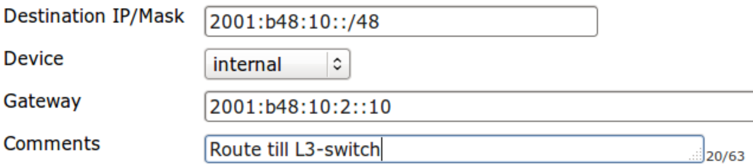
Addressing mode

● Manual ○ DHCP ○ PPPoE

IP/Netmask: 1.1.1.1/255.255.255.240

IPv6 Address: 2001:b48:10:ffff::2/64

Example for setting up a route to an internal L3 switch and a default route to the rest of the world:

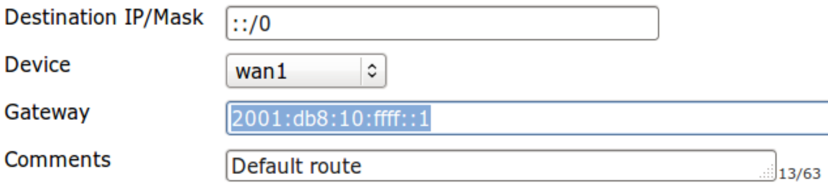


Destination IP/Mask: 2001:b48:10::/48

Device: internal

Gateway: 2001:b48:10:2::10

Comments: Route till L3-switch 20/63



Destination IP/Mask: ::/0

Device: wan1

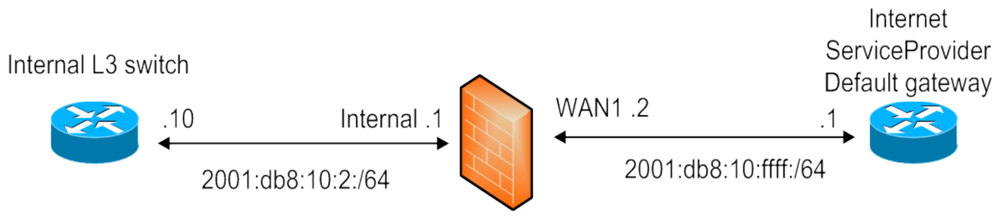
Gateway: 2001:db8:10:ffff::1

Comments: Default route 13/63

4.1.2 Set rules for IPv6

Set the most necessary firewall rules first. Wait until individual services are ready to be IPv6 Enabled.

The approach for activating IPv6 and setting up interfaces, routes, hosts, networks and rules resembles that for IPv4. IPv4 and IPv6 are managed within the same regulatory framework in some firewalls. However, most use separate address lists and systems of rules. The following diagram shows an example of a set up:



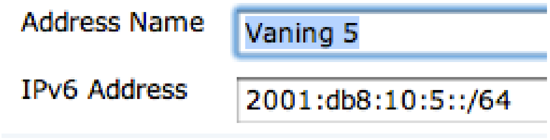
Review and document which hosts, networks, protocols and ports are to be a 'source' and a 'destination' in the firewall. It is better to do this before starting to set up rules. This saves time and requires fewer rules. See the following table for how documentation can be done:

Source	Protocol/Port	Destination
All	http	www.myndighet.se
All	Smtp	email.authority.se
Floor 5	IP telephony	IP teleservice
DNS servers	DNS	All
etc.	-	-

4.1.3 An example of a setting up rules in the firewall

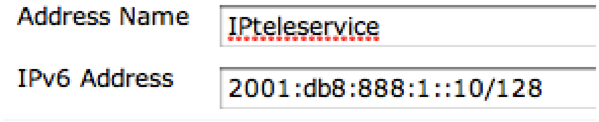
The following example shows how rules for networks, hosts and services for a certain segment (e.g. floor 5 of an organisation) can be set up in the firewall:

1. Set up the Floor 5 (*Våning 5*) network.



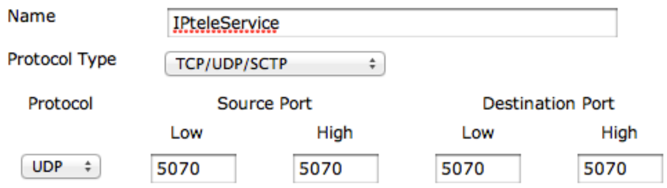
Address Name	Vaning 5
IPv6 Address	2001:db8:10:5::/64

2. Set up the IP teleservice host.



Address Name	IPteleservice
IPv6 Address	2001:db8:888:1::10/128

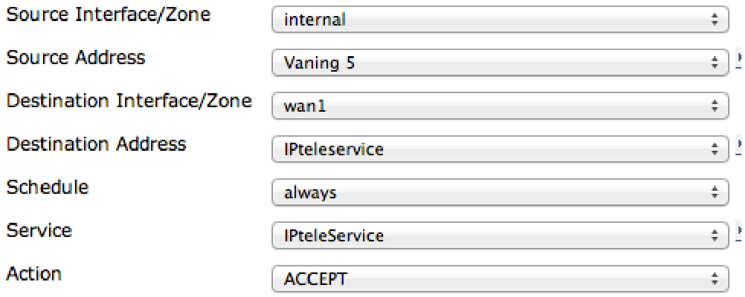
3. Create the service to connect over UDP port 5070.



Name	IPteleService
Protocol Type	TCP/UDP/SCTP

Protocol	Source Port		Destination Port	
	Low	High	Low	High
UDP	5070	5070	5070	5070

4. Finally set up the rule.



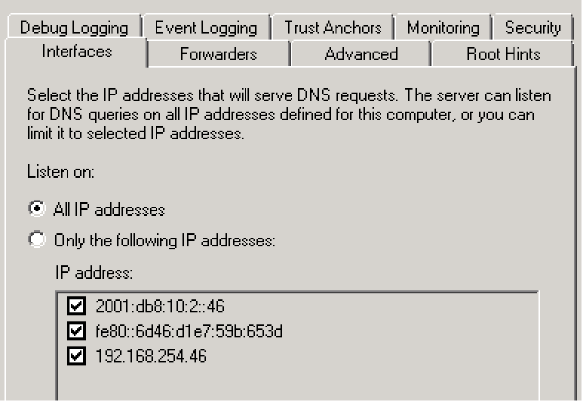
Source Interface/Zone	internal
Source Address	Vaning 5
Destination Interface/Zone	wan1
Destination Address	IPteleservice
Schedule	always
Service	IPteleService
Action	ACCEPT

4.2 Activate IPv6 in DNS servers

All common DNS servers currently support IPv6, and IPv6 is easy to activate. This section provides examples of how IPv6 can be activated in three common DNS servers: Windows 2008 DNS, ISC BIND and Unbound.

4.2.1 Activating IPv6 in Windows server 2008 DNS

Support for IPv6 is activated in Windows Server 2008 and later versions. If you activate IPv6 on the server, it will respond to and make queries over IPv6. IPv6 can be activated in Windows Server 2008 DNS using the following settings:



Select the IP addresses that will serve DNS requests. The server can listen for DNS queries on all IP addresses defined for this computer, or you can limit it to selected IP addresses.

Listen on:

● All IP addresses

○ Only the following IP addresses:

IP address:

☑ 2001:db8:10:2::46
☑ fe80::6d46:d1e7:59b:653d
☑ 192.168.254.46

4.2.2 Activating IPv6 in ISC BIND

ISC BIND is not IPv6 Enabled initially. IPv6 is activated in named.conf using the following option:

```
options {
        listen-on-v6 { any; };
};
```

Several settings can be made in named.conf for how IPv6 and dual stack should be managed.

4.2.3 Activating IPv6 in Unbound

IPv6 is activated in Unbound using
unbound.confdo-ip6: yes

4.3 Activate IPv6.arpa

Reverse DNS lookups are required in IPv6, as is the case for IPv4. Most providers delegate IP6.arpa to the organisation's authoritative DNSs when they supply an IPv6 Internet connection. IP6.arpa must be activated and function primarily for the organisation's MTAs for incoming and outgoing email. This is because many do not accept email unless the name on AAAA and PTR RR corresponds.

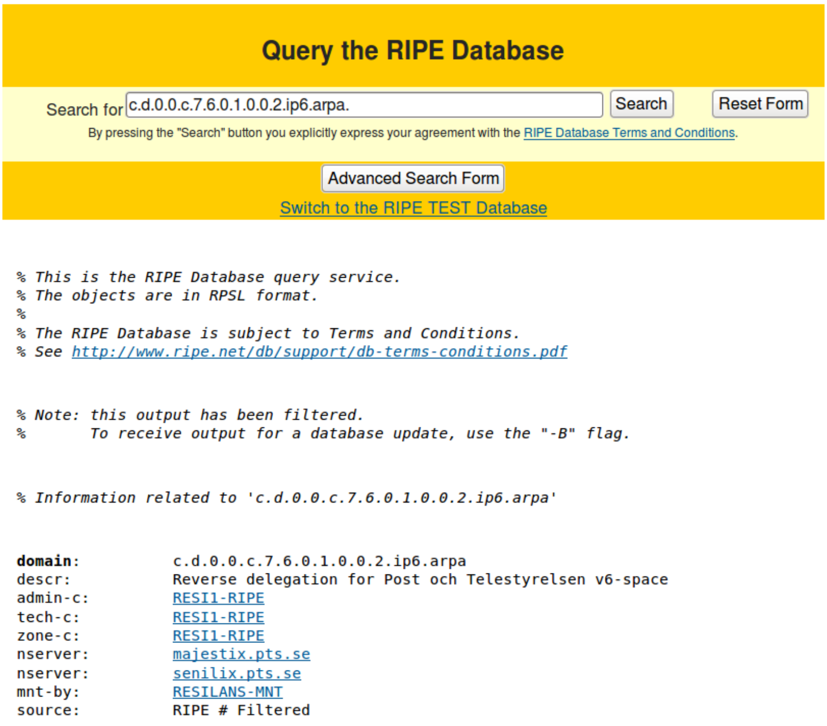
Ensure that your ip6.arpa is delegated to the organisation's DNSs and that reverse lookups have been activated and are functioning.

4.3.1 Examples with PTS DNS

PTS was assigned 2001:67c:dc::/48. PTS ip6.arpa becomes c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa. In the event of a WHOIS search in RIPE NCC's database (http://www.ripe.net), we see that c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa has been delegated to majestix.pts.se and senilix.pts.se.

ip6.arpa is created in the same way as IPv4's in-addr.arpa; i.e., this is done by starting with ip6.arpa. One then takes the whole address backwards. There is no shortcut using '::'.

See www.pts.se as an example; this uses 2001:67c:dc:43::215.
Its ip6.arpa then becomes:
5.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.4.0.0.c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa
All 32 hexadecimal figures must be included in ip6.arpa.



Query the RIPE Database

Search for c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa.

By pressing the "Search" button you explicitly express your agreement with the RIPE Database Terms and Conditions.

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf


% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.


% Information related to 'c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa'


domain:         c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa
descr:          Reverse delegation for Post och Telestyrelsen v6-space
admin-c:        RESI1-RIPE
tech-c:         RESI1-RIPE
zone-c:         RESI1-RIPE
nserver:        majestix.pts.se
nserver:        senilix.pts.se
mnt-by:         RESILANS-MNT
source:         RIPE # Filtered
```

4.4 Set up ip6.arpa in DNS and adopt a position on whether it should be public

It is important to set up ip6.arpa for authoritative DNSs and to set up the organisation's email servers within them. When computers and other hosts inside the firewall have public addresses that are seen on the Internet, a position should be adopted on how to manage ip6.arpa for workstations. One recommendation is not to have a public ip6.arpa except for proxies, email servers, DNSs and public e-services (web server).

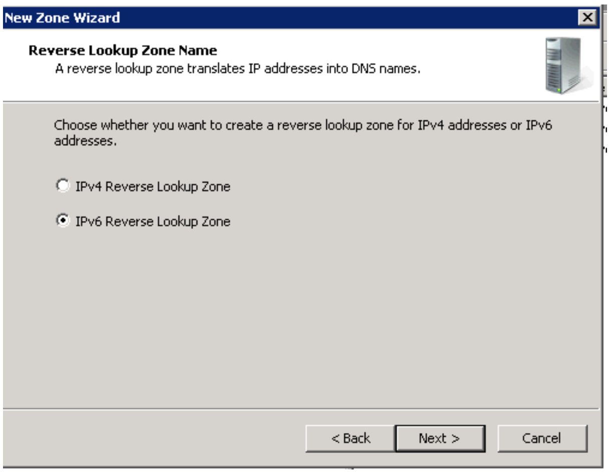
An ip6.arpa may be signed using DNSSEC just as for any other DNS zone.

This section provides a description of how to activate IP6.arpa in a number of common systems: Windows, ISC BIND and Webmin. Webmin is an open source code solution (http://www.webmin.net) that simplifies the administration of Linux, Solaris and Windows.

4.4.1 Activating ip6.arpa in Windows

This is not the full set of images, but basically shows how to set up ip6.arpa in Windows.

1. Choose to create an ip6.arpa, i.e. IPv6 Reverse Lookup Zone Name.



New Zone Wizard

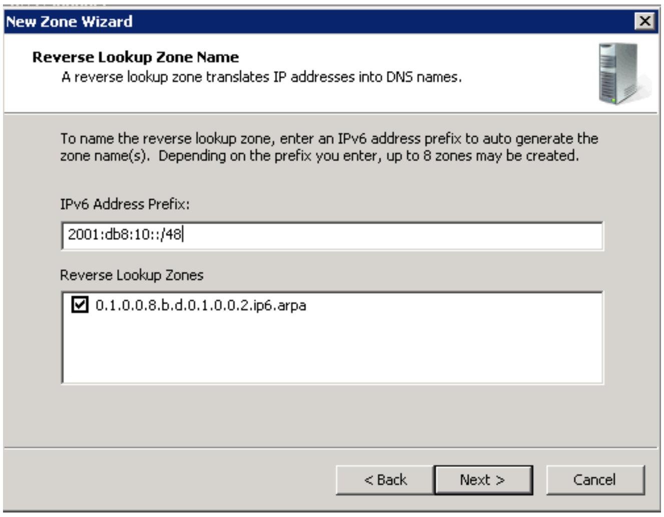
Reverse Lookup Zone Name
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

○ IPv4 Reverse Lookup Zone

● IPv6 Reverse Lookup Zone

2. Choose a prefix that it will manage. Windows helps you to create IP6.arpa, so you do not have to work this out manually.



New Zone Wizard

Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

To name the reverse lookup zone, enter an IPv6 address prefix to auto generate the zone name(s). Depending on the prefix you enter, up to 8 zones may be created.

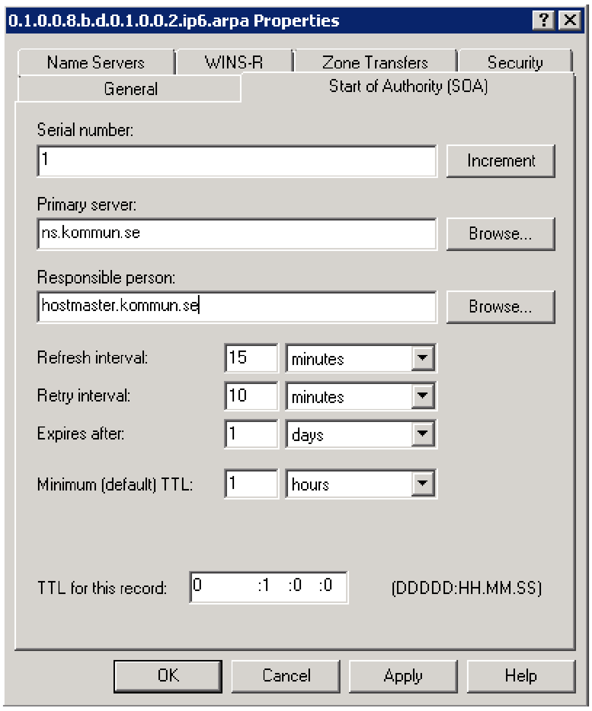
IPv6 Address Prefix:

2001:db8:10::/48

Reverse Lookup Zones

☑ 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa

3. When the zone is ready, it is important to provide the correct information for the name server's SOA (Start of Authority), the name of the primary name server (primary name server or master) and the email address of the person responsible for the name server.



0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa Properties

Start of Authority (SOA)

Serial number: 1

Primary server: ns.kommun.se

Responsible person: hostmaster.kommun.se

Refresh interval: 15 minutes

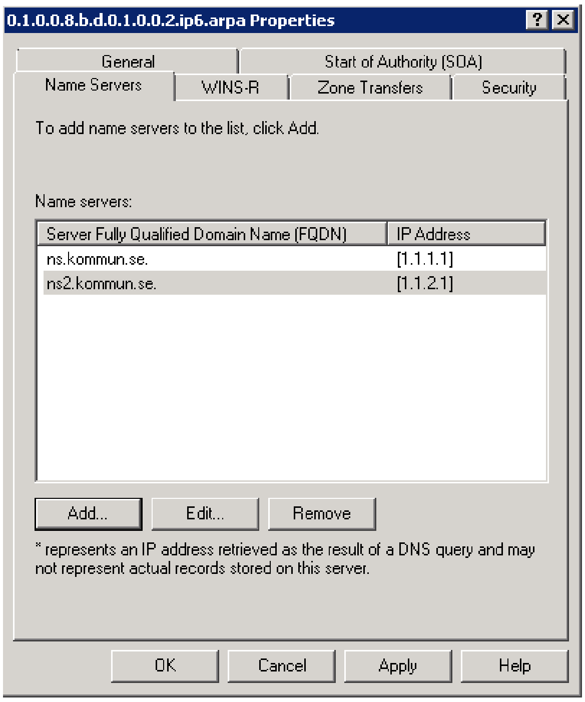
Retry interval: 10 minutes

Expires after: 1 days

Minimum (default) TTL: 1 hours

TTL for this record: 0 :1 :0 :0 (DDDDD:HH.MM.SS)

4. The correct name must be provided for the name server (NS RR). Windows proposes an internal name. Enter the DNS's external name. In Windows you can enter an NS without providing its IP address, which may cause problems if the network is renumbered.



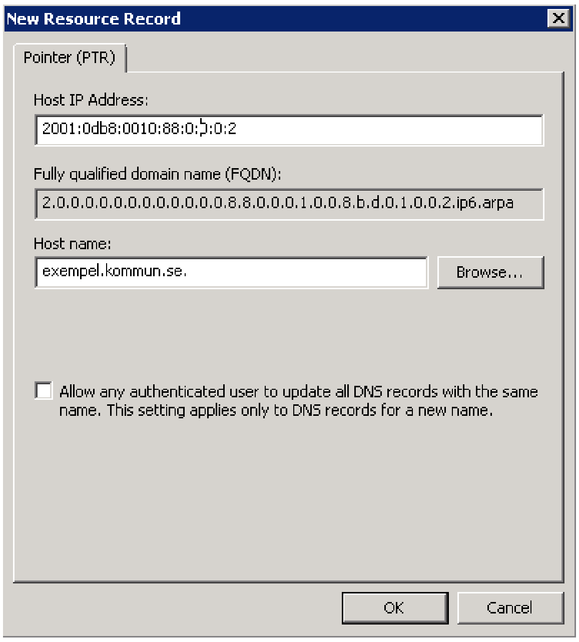
To add name servers to the list, click Add.

Name servers:

Server Fully Qualified Domain Name (FQDN)	IP Address
ns.kommun.se.	[1.1.1.1]
ns2.kommun.se.	[1.1.2.1]

* represents an IP address retrieved as the result of a DNS query and may not represent actual records stored on this server.

5. We then add our first PTR RR.
   You cannot state the address as 2001:db8:10::2, but must enter :: as 0:0:0.



New Resource Record

Pointer (PTR)

Host IP Address: 2001:0db8:0010:88:0:0:0:2

Fully qualified domain name (FQDN): 2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.8.0.0.0.0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa

Host name: exempel.kommun.se.

□ Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.

After this step, ip6.arpa is activated.

4.4.2 Activating ip6.arpa in ISC BIND

Activating ip6.arpa in ISC BIND can be done as follows:

1. Create ip6.arpa for 2001:db8:10::/48 by creating a new zone in named.conf as shown in the following example:

```
zone "0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa." {
        type master;
        file
"0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa”;

};
```

2. Then create the file 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

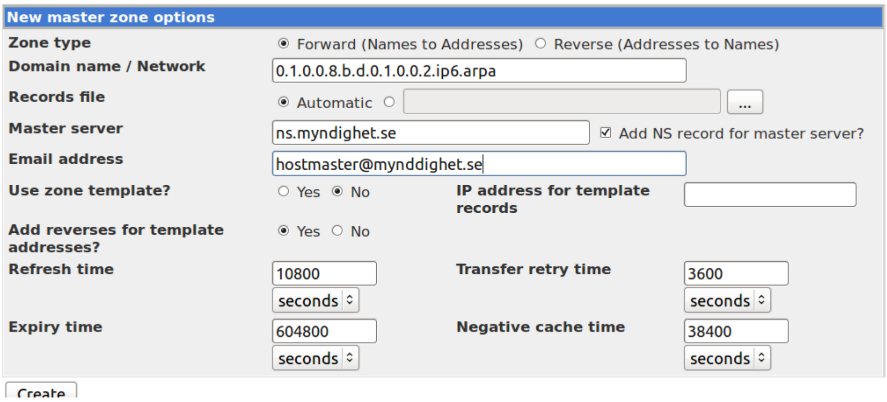
```
@ IN SOA ns.myndighet.se.
hostmaster.myndighet.se. (
                        2011060202
                        1800
                        7200
                        2678400
                        3600 )
                        NS
ns1.myndighet.se.
                        NS
ns2.myndighet.se.
```

3. To create a PTR RR for 2001:db8:10:10::2 , enter `2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0 IN PTR smtp.myndighet.se.` in file 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

4.4.3 Setting up IP6.arpa via Webmin

If Webmin is used to edit text files or make settings, this is done as follows:

1. Create an ip6.arpa for your /48. Please note that Webmin wishes the zone to be specified as a 'Forward Name to Addresses', not as a Reverse.

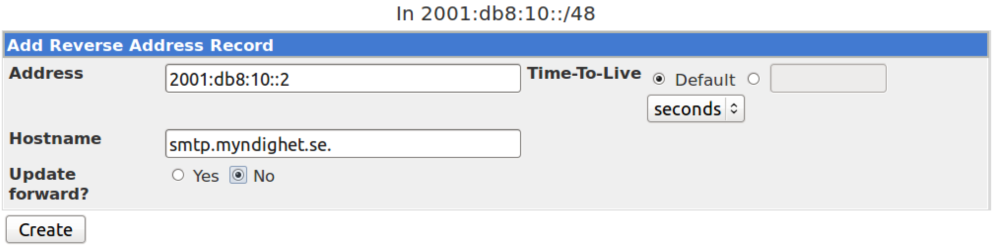


New master zone options

Zone type	● Forward (Names to Addresses) ○ Reverse (Addresses to Names)		
Domain name / Network	0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa		
Records file	● Automatic ○ ...		
Master server	ns.myndighet.se	☑ Add NS record for master server?	
Email address	hostmaster@mynddighet.se		
Use zone template?	○ Yes ● No	IP address for template records	
Add reverses for template addresses?	● Yes ○ No		
Refresh time	10800 seconds	Transfer retry time	3600 seconds
Expiry time	604800 seconds	Negative cache time	38400 seconds

The above example shows that Webmin has created a 2001:db8:10::/48 of 0.1.0.0.8.b.d.0.1.0.0.2.ip6.arpa.

2. To add an ip6.arpa PTR, provide the IPv6 address and host name. Remember to add a concluding full stop after the host name.



In 2001:db8:10::/48

Add Reverse Address Record

Address: 2001:db8:10::2

Time-To-Live: ● Default ○ seconds

Hostname: smtp.myndighet.se.

Update forward? ○ Yes ● No

After this step, we have now created an ip6.arpa in Webmin.

4.5 Important things to remember about IP6.arpa

Never use wildcards (*). This causes problems with log files. NXDOMAIN (Non existent domain) is better than a non-equivalent AAAA RR and PTR RR.

Another recommendation is not to publically use the dynamic ip6.arpa generated by Active Directory.

4.6 Dynamic and static addressing for computers and servers

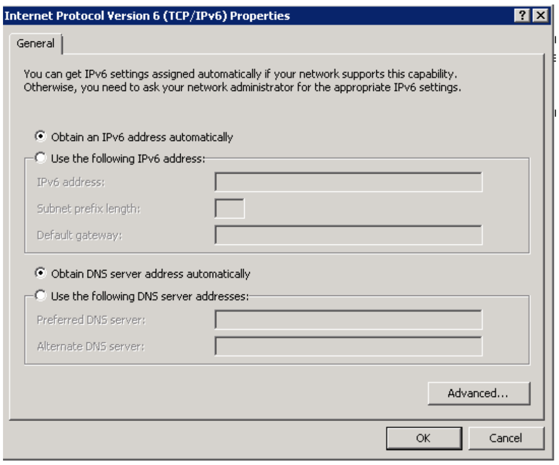
There are several ways of addressing in an internal network on segments (VLAN). This can be done using, for example, SLAAC (StateLess Address Autoconfiguration), stateful DHCPv6 and stateless DHCPv6. Stateful DHCPv6 affords greater control over addressing. Stateless DHCPv6 resembles SLAAC.

The intention was for SLAAC to manage addressing in IPv6. SLAAC arranges for computers to generate their own addresses and have a DNS assigned to them. This is often not sufficient, but you want to be able to assign other DHCPv6 options such as, for example, a SIP server or NTP server. DHCPv6 will then have to be used. One disadvantage of DHCPv6 is that it is not supported by Mac OS X (versions prior to MAC OS X Lion, 10.7). DHCPv6 often has to be activated manually in Linux.

The following describes how static addressing can be set up in a number of different environments.

See the following example for the settings in Windows. Please note that you do not have to state a DNS when providing a static IPv6 address. Queries concerning AAAA RR can then just as easily go over IPv4.

With automatic addressing, the router tells the computer via SLAAC and/or DHCPv6 whether or not it should be given a dynamic address.



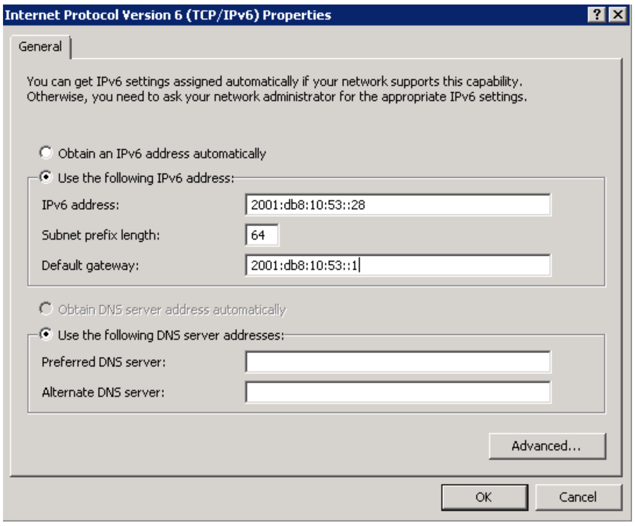
You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically
○ Use the following IPv6 address:
IPv6 address:
Subnet prefix length:
Default gateway:

● Obtain DNS server address automatically
○ Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

The following is an example of static addressing for a computer in a network where others have dynamic assignment.

One problem with Windows is that even if you activate static IPv6 addresses, the computer will still generate SLAAC and run DHCPv6 if this has been specified by the router's RA.



You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically
● Use the following IPv6 address:
IPv6 address: 2001:db8:10:53::28
Subnet prefix length: 64
Default gateway: 2001:db8:10:53::1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:

If a Windows computer is to have a static address in a network, where others will be using SLAAC and/or DHCPv6, Router Advertisement must be disabled so that it does not listen to it using:

```
netsh interface ipv6 set interface "Local Area Connection"
routerdiscovery=disable
```

If Linux is used on the server, a static address can be set either in a text file or in Webmin.

If a Debian distribution is used and you want to configure static IPv6 addressing in a text file, this is done in /etc/network/interfaces as follows:

```
iface eth0 inet6 static
        address 2001:db8:10:3::18
        netmask 64
        gateway 2001:db8:10:3::1
```

Redhat is another commonly used distribution. Set static addressing in this as follows:

/etc/sysconfig/network

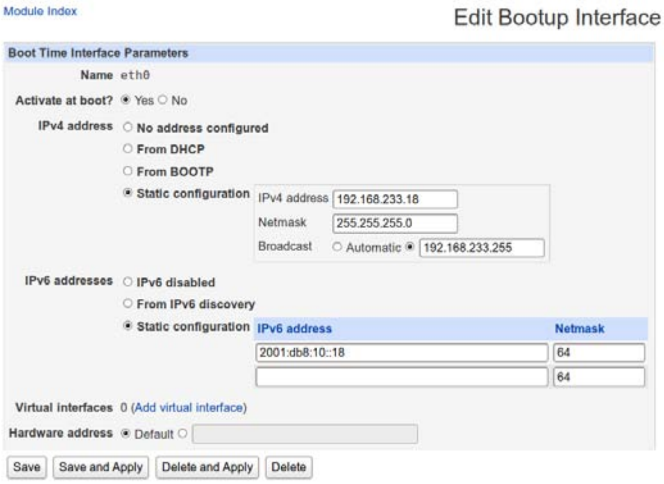
```
NETWORKING_IPV6=yes
IPV6_DEFAULTGW=2001:db8:10:3::1
```

/etc/sysconfig/network-scripts/ifcfg-eth0

```
IPV6INIT=yes
IPV6ADDR="2001:db8:10:3::18/64"
```

The way in which static IPv6 addressing is set in other distributions that are not based on Debian and Red Hat may vary. This is done in Webmin by activating IPv6 on eth0; see the following example:

1. Set up an IPv4 and IPv6 address on eth0:



Edit Bootup Interface

Boot Time Interface Parameters

Name eth0

Activate at boot? ● Yes ○ No

IPv4 address ○ No address configured
○ From DHCP
○ From BOOTP
● Static configuration

IPv4 address 192.168.233.18

Netmask 255.255.255.0

Broadcast ○ Automatic ● 192.168.233.255

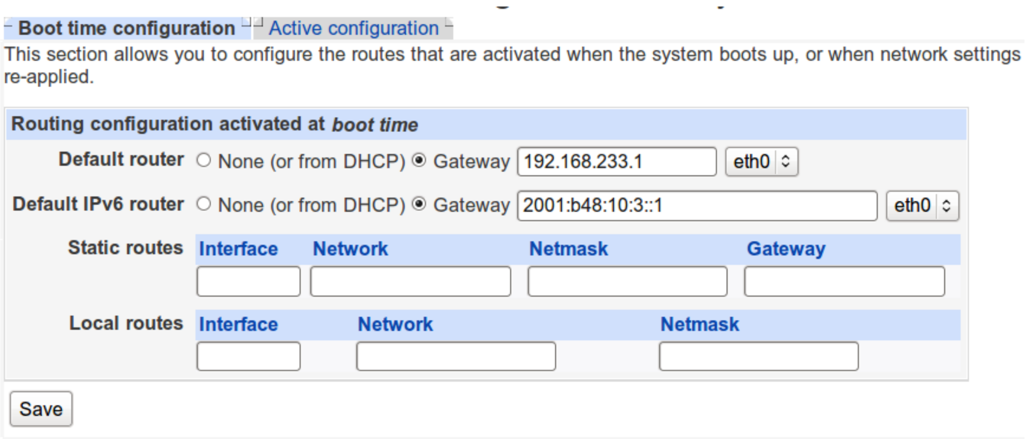
IPv6 addresses ○ IPv6 disabled
○ From IPv6 discovery
● Static configuration

IPv6 address	Netmask
2001:db8:10::18	64
	64

Virtual interfaces 0 (Add virtual interface)

Hardware address ● Default ○

2. Set up a default gateway for IPv4 and IPv6:



This section allows you to configure the routes that are activated when the system boots up, or when network settings re-applied.

Routing configuration activated at *boot time*

Default router ○ None (or from DHCP) ● Gateway 192.168.233.1 eth0

Default IPv6 router ○ None (or from DHCP) ● Gateway 2001:b48:10:3::1 eth0

Static routes

Interface	Network	Netmask	Gateway

Local routes

Interface	Network	Netmask

Static addressing has now been activated.

4.7 Activate IPv6 in web servers

This section provides advice on how to activate IPv6 in a number of common web servers and Content Management Systems. The most commonly used web servers together with the most commonly used CMSs support IPv6. Automatic support for IPv6 on the Internet is provided when the server's operating system is IPv6 Enabled.

Examples are provided for Microsoft Internet Information Server, SiteVision over Tomcat, Apache Web Server and Webmin.

IPv6 is activated automatically in Microsoft's Internet Information Server when it is activated in the operating system. Check the IPv6 status using the command netstat –an . The web server will then listen to IPv6 and port 80.

```
TCP    [::]:80              [::]:0              LISTENING       0
```

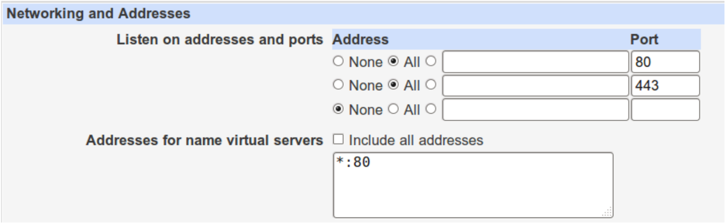
The CMS SiteVision system is sometimes used among other things with the Tomcat web server. This functions with IPv6. It should look like this in an .xml server:

```
<connector port="80">
```

If an Apache web server is used, the following should be specified in httpd.conf:

```
Listen 80
NameVirtualHost *:80
```

If Webmin is installed on the server, it should look like this:



Networking and Addresses

Listen on addresses and ports	Address	Port
	○ None ● All ○	80
	○ None ● All ○	443
	● None ○ All ○	

Addresses for name virtual servers ☐ Include all addresses

```
*:80
```

Check that IPv6 has been set up correctly using the command

```
netstat –an.
tcp6       0       0 :::80                    :::*                       LISTEN
```

4.8 Activate IPv6 on the email server

There are several manufacturers of email communication systems (email servers and Mail Transfer Agents (MTA)) that support IPv6 and IPv4. This section describes how IPv6 can be activated in the four most common email systems: Microsoft Exchange, Halon Security, Postfix server and Sendmail. Microsoft Exchange and Halon Security are commercial software. The others are solutions with open source codes.

It is important to consider security requirements when choosing an email system. The system should be able to filter emails in both incoming and outgoing traffic.

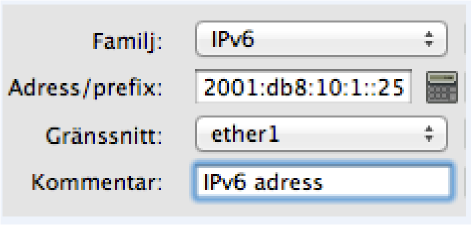
4.8.1 Microsoft Exchange

Microsoft Exchange comprises both an MTA and an email server. Windows Server 2003/2008 supports IPv6. See .SE's guide on the deployment of IPv6 in medium-sized undertakings (http://www.iis.se/docs/IPv6-guide_MedBilaga1.pdf) for more information about experiences relating to these email servers.

4.8.2 Halon Security

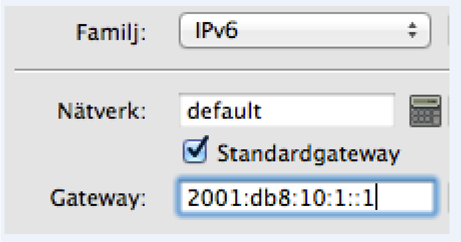
Activate IPv6 in Halon's solution as follows:

1. Set up an IPv6 address. This is done by going into the menu 'Network -> Addresses'.



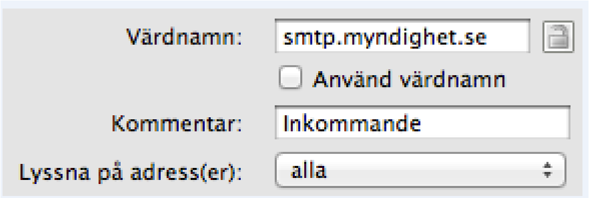
Familj: IPv6
Adress/prefix: 2001:db8:10:1::25
Gränssnitt: ether1
Kommentar: IPv6 adress

2. Set up a default route. This is done by going into the menu 'Network -> Routing'.



Familj: IPv6
Nätverk: default
☑ Standardgateway
Gateway: 2001:db8:10:1::1

3. Under the menu 'Email gateway -> Domains -> Incoming' (listeners), check that it states 'everyone' in the interface for 'Listen to address(es)'.



Värdnamn: smtp.myndighet.se

□ Använd värdnamn

Kommentar: Inkommande

Lyssna på adress(er): alla

4.8.3 Postfix server

If a Postfix server is used as an MTA, IPv6 is often not activated in it. Add the following line to main.conf in order to activate IPv6:

```
inet_protocols = all
```

4.8.4 Sendmail

IPv6 is not usually activated if Sendmail is used as an MTA. Activate IPv6 in sendmail.mc using:

```
DAEMON_OPTIONS('Name=MTA-v6, Family=inet6')
```

The exact IP addresses that Sendmail should listen to must be specified in some versions of Sendmail. The following settings are then required:

```
DAEMON_OPTIONS('Port=smtp,Addr=192.168.1.25, Name=MTA')
DAEMON_OPTIONS('Port=smtp,Addr=::1, Name=MTA-v6,
Family=inet6')
DAEMON_OPTIONS('Port=smtp,Addr=127.0.0.1, Name=MTA2')
DAEMON_OPTIONS('port=smtp,Addr=2001:db8:10::25, Name=MTA2-v6,
Family=inet6')
```

Check that the MTA is receiving emails using IPv6 using

```
netstat –an
```

```
tcp6     0     0 :::25              :::*              LISTEN
```

4.9 Email filtering solutions

There are several items of hardware and software for filtering spam and scanning viruses in emails. Check with the manufacturer regarding the product's IPv6 maturity and how IPv6 is activated.

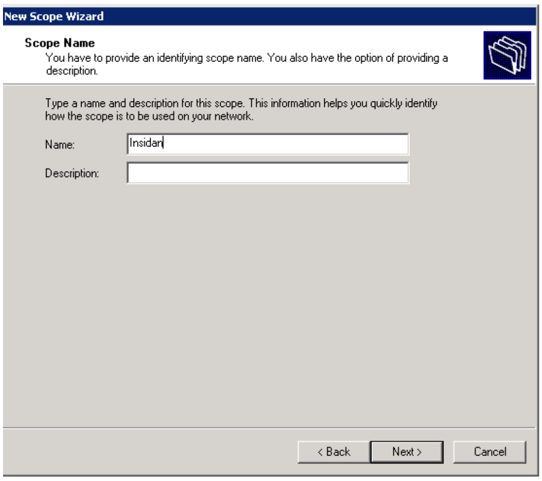
4.10 Activate DHCPv6

The following provides an example of how DHCPv6 can be activated in Windows 2008 and in ISC's DHCPv6 server (http://www.isc.org).

4.10.1 Activating DHCPv6 servers in Windows 2008

Windows Server 2008 and later versions have a DHCPv6 server built into their operating systems. It must be installed as a 'role', while it is often already installed and activated for IPv4. Activate DHCPv6 in Windows 2008 as follows:

1. Create a new DHCPv6 scope (address space). Give the DHCPv6 space an informative name.



New Scope Wizard

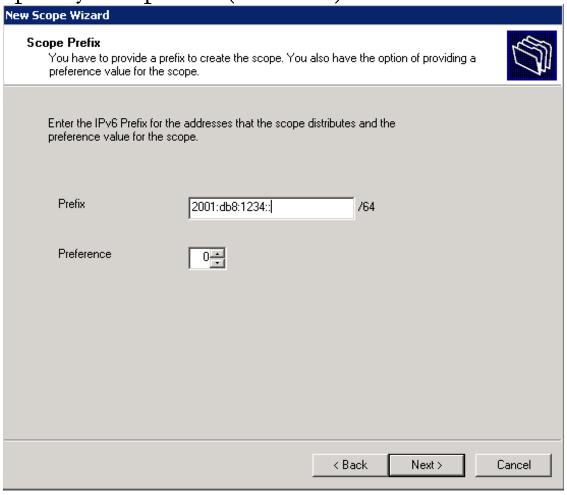
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: Insidan

Description:

2. Specify the prefix (network) to which the DHCP scope is to apply.



New Scope Wizard

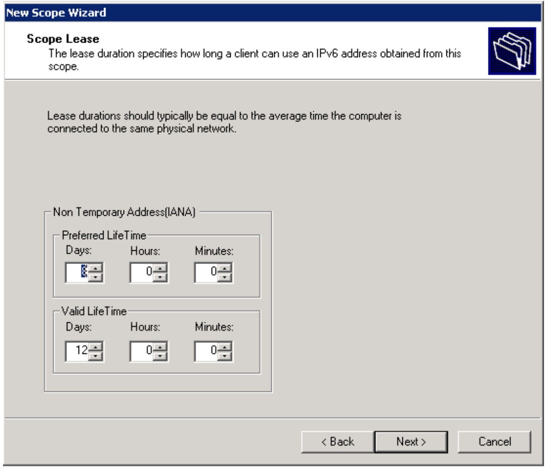
Scope Prefix
You have to provide a prefix to create the scope. You also have the option of providing a preference value for the scope.

Enter the IPv6 Prefix for the addresses that the scope distributes and the preference value for the scope.

Prefix 2001:db8:1234:: /64

Preference 0

3. Specify the lifespan of the addresses.



New Scope Wizard

Scope Lease

The lease duration specifies how long a client can use an IPv6 address obtained from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network.

Non Temporary Address(IANA)

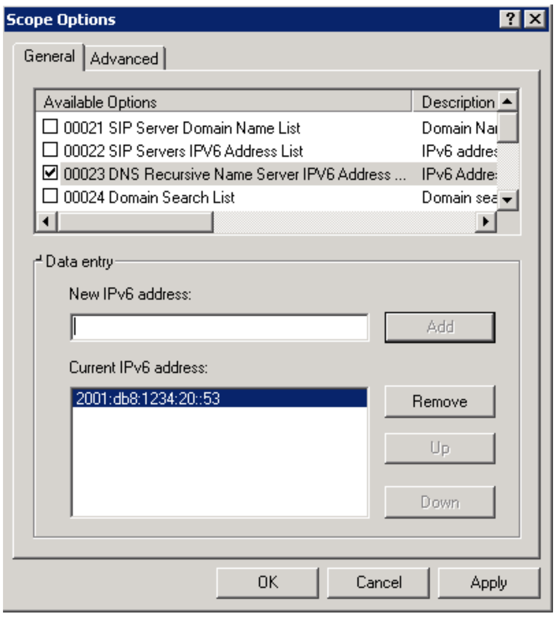
Preferred LifeTime

Days: 8 Hours: 0 Minutes: 0

Valid LifeTime

Days: 12 Hours: 0 Minutes: 0

4. Provide a DNS and activate DNS lookups over IPv6. When it is set up, a check is made of whether the DNS server functions from the DHCP server.



Scope Options

Available Options	Description
□ 00021 SIP Server Domain Name List	Domain Nai
□ 00022 SIP Servers IPV6 Address List	IPv6 addres
☑ 00023 DNS Recursive Name Server IPV6 Address ...	IPv6 Addre:
□ 00024 Domain Search List	Domain sea

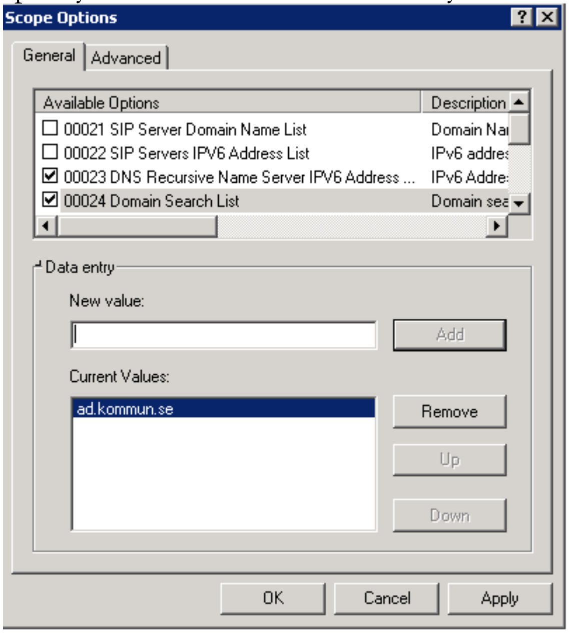
Data entry

New IPv6 address:

Current IPv6 address:

2001:db8:1234:20::53

5. Specify the search domain in which your Active Directory is located.



Available Options	Description
☐ 00021 SIP Server Domain Name List	Domain Nai
☐ 00022 SIP Servers IPV6 Address List	IPv6 addres
☑ 00023 DNS Recursive Name Server IPV6 Address ...	IPv6 Addre:
☑ 00024 Domain Search List	Domain sea

New value:

Current Values:

ad.kommun.se

4.10.2 Activating DHCPv6 in ISC's DHCP server

ISC's DHCP server version 4 and subsequent versions support DHCPv6. This forms part of and is activated in some newer Linux distributions. It must be compiled manually in some older distributions.

You must start two processes when using ISC's DHCP server for both IPv4 and IPv6: one for IPv4 and one for IPv6. The startup script and Webmin Module for ISC DHCPv6 are adapted for IPv4 so this has to be done manually using your own startup script and a separate configuration file. See SE's guide (www.iis.se/docs/Jörgen-Eriksson-Torbjörn-Eklöv.pdf) for more information about ISC and DHCPv6.

1. Configuration file, e.g. /etc/dhcpv6.conf

   ```
   max-lease-time 7200;
   default-lease-time 3600;
   authoritative;
   option dhcp6.name-servers 2001:db8:10:2::46;
   option dhcp6.domain-search "ad.myndigheten.se";

   subnet6 2001:db8:10:22::/64 {
           range6  2001:db8:10:22::        2001:b48:10:2::ffff;
   }
   ```

2. Startup command

   ```
   /usr/sbin/dhcpd -6 -cf /etc/dhcpv6c.conf
   ```

3. You can also provide temporary DHCPv6 addresses using ISC's DHCPv6 server. This is not a recommendation. This is done in dhcpv6.conf using:

   ```
   range6 2001:db8:10:22::/64 temporary;
   ```

5 Activating IPv6 in the internal network

This section describes how IPv6 can be activated in the internal network. This is done using examples of a number of systems that support IPv6.

The section covers IPv6 activation in a number of common functions in the internal network; L2 switch (connection switch), L3 switch (central switch) and use of DHCP to determine addressing for various internal segments and in a proxy.

The section assumes that the internal network has an L3 switch, a number of computers that are to run DHCPv6 and a server (which should have a fixed IPv6 address).

5.1 Activating IPv6 in a connection switch (L2 switch)

In most cases, IPv6 will function without taking any action in the connection switch. If it supports MLD snooping, activate it. MLD snooping is the same as IGMP snooping in IPv4.

MLD snooping is activated in a Cisco switch using:

```
ipv6 mld snooping
```

5.2 Activating IPv6 in a central switch (L3 switch)

Activating IPv6 in an L3 switch resembles activation using IPv4.
See the following example:

```
ip address 192.168.10.1 255.255.255.0
```

or

```
ipv6 address 2001:db8:10::1/64
```

```
ip route 0.0.0.0 0.0.0.0 192.168.324.1
```

or

```
ipv6 route ::/0 2001:db8:10:55::1
```

5.3 Activating DHCPv6 on a VLAN

The following example shows how to activate DHCPv6 on an interface (VLAN), turn off SLAAC and activate routing globally in the switch. This example uses a Cisco switch. Other manufacturers' switches have a similar setup but use different syntax.

Addressing hosts and assigning DNS and search suffixes for these is done using DHCPv6 through managed and other flags.

Use of ipv6 nd prefix default no-advertise turns off all advertisements for SLAAC.

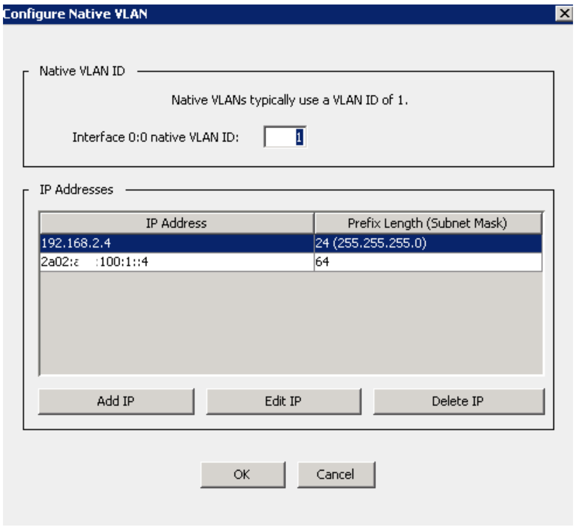
```
!Activate IPv6 routing
IPv6 unicast routing
```

```
interface VLAN 6
 !Set a fixed address on VLAN 6
 IPv6 address 2001:db8:10:6::10/64
 ! O and M flags set => DHCPv6 shall be used for the address and other
options
 IPv6 nd managed-config-flag
 IPv6 nd other-config-flag
 ! State which DHCPv6 server is to be used
 IPv6 DHCP relay destination 2001:db8:10:50::20
 !Inactivate SLAAC on all prefixes on these interfaces
 IPv6 nd prefix default no-advertise
```

5.4 Activating IPv6 in a proxy

Not many proxy servers support IPv6. Bluecoat (http://www.bluecoat.com/) is one example of a proxy (hardware) that supports IPv6. The following images show how IPv6 is activated in Bluecoat.

1. Set up an address for the proxy server.

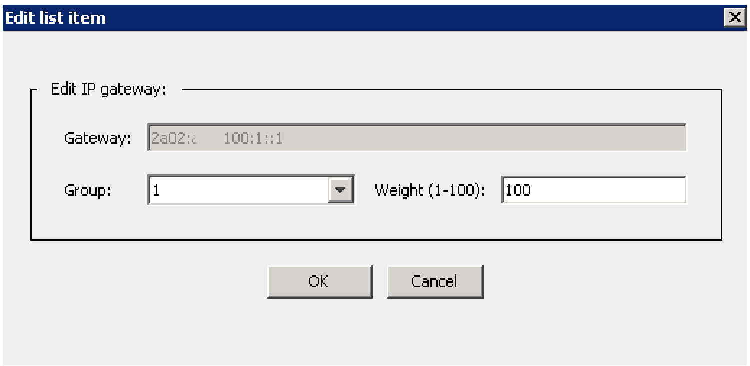


Native VLANs typically use a VLAN ID of 1.

Interface 0:0 native VLAN ID: 1

IP Address	Prefix Length (Subnet Mask)
192.168.2.4	24 (255.255.255.0)
2a02:a :100:1::4	64

2. Set up a default route.



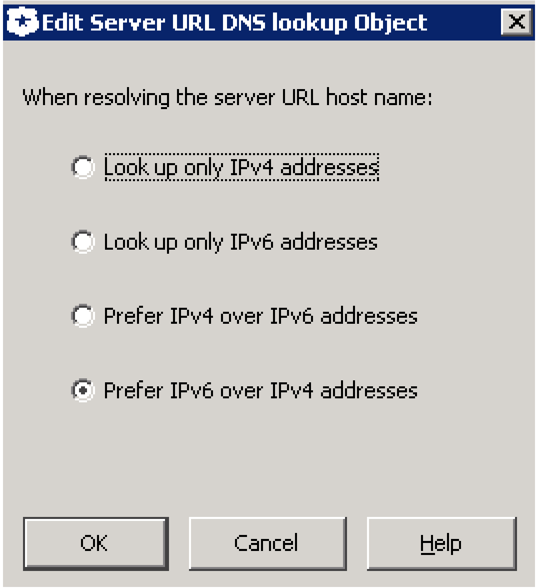
Edit IP gateway:

Gateway: 2a02: 100:1::1

Group: 1

Weight (1-100): 100

3. In Bluecoat you can set whether communication is to take place over IPv4 or IPv6. In the settings, choose that the system is to communicate over IPv6 in the first instance and over IPv4 in the second instance. It is easy to adjust the settings if there are any problems.



When resolving the server URL host name:

○ Look up only IPv4 addresses

○ Look up only IPv6 addresses

○ Prefer IPv4 over IPv6 addresses

● Prefer IPv6 over IPv4 addresses

IPv6 is now activated in the proxy server.

Appendix 7 - Financial consequences

This appendix discusses the estimated cost and time of deploying IPv6 in public e-services.

Appendix 8 provides examples of PTS's costs for deploying IPv6.

The cost depends on the IT environment and the level at which consultants are used

The cost of deploying IPv6 depends on the organisation's existing internal IT environment and its need to acquire new hardware and commercial software. If relatively new hardware is being used, software that supports IPv6 can be downloaded and configured on the existing equipment.

The cost also depends on the extent to which consultancy support is used for implementation.

The cost depends on the size and complexity of the network, the number of services and also security and accessibility requirements

The cost of deployment depends on the size and complexity of the internal network, the number of services (the operations 'out on the web'/number of domain names) and also security and accessibility requirements. This cost will increase if there are high accessibility requirements, e.g. regarding up and down-time (i.e. SLA requirements) and e.g. requirements regarding accessibility and on-duty service after normal office hours. The cost will be higher if updates and work for putting it into full live operation (e.g. upgrading firewalls) can be carried out after office hours. Firewall clusters and support for IP Address Management (IPAM) cost tens of thousands of Swedish kronor.

The estimated time for an external party (in cloud computing) to take stock of the internal IT environment together with the services for which they are responsible amounts to a few working days for own staff or external consultants.

The estimated time for a consultant with experience of IPv6 deployment to deploy IPv6 in public e-services (such as DNS and the web) for a small organisation amounts to some ten to twenty hours.

The cost of training staff

One cost is for staff training. If staff have knowledge of IPv4, an IPv6 course will not have to take many days. One to two days would suffice to get started with IPv6. A course describing the differences between IPv4 and IPv6 would be of particular value. After a period of time, this could be supplemented with more advanced courses**.** The estimated time and cost of training staff is initially one to two days. The cost starts at approximately SEK 5,000 per day.

Costs may be affected

Costs may be affected in several ways: primarily by preparing for the transition.

The cost depends on how well organised and documented the networks already are when IPv6 is deployed. These costs will reduce if you ensure that requirements are imposed for equipment and services to support IPv6 in conjunction with an ongoing acquisition.

Appendix 8 - Swedish experience of IPv6 deployment

Experience gained from IPv6 deployment is reported in this appendix.

1 Swedish stakeholders' experiences

PTS has gained experience as a result of discussions during consultations and also comments submitted in the course of formal consultation in respect of a previous edition of this description. However, statistics from various open sources indicate that very few stakeholders within the public sector have deployed IPv6 for their public e-services.

1.1 There is generally a lack of experience from deployment

With regard to the stakeholders that PTS has met within the framework of the consultation, the eGovernment Delegation, CERT-SE, and .SE support IPv6 alongside IPv4. They have shared their experiences, which are briefly described below.

.SE has had a board decision to deploy IPv6 for its public e-services for the past couple of years. .SE's experience is that IPv6 should be deployed according to the principle of beginning at the periphery and working towards the core. Work should be split into two phases: the activation of public e-services and activation in services on the internal network. The configuration of firewalls and routers are resource-intensive. Consultants have provided assistance.

The eGovernment Delegation's website and DNS have supported IPv6 alongside IPv4 since 2010. Consultants have assisted with this deployment.

CERT-SE within MSB has supported IPv6 alongside IPv4 since the beginning of 2009. Services provided by CERT-SE via IPv6 include external email communication, DNS and its website. CERT-SE has IPv6 transit from three different providers, and also exchanges IPv6 traffic ('peers') with a number of other service providers at STHIX (www.sthix.net).

The Swedish Tax Agency has produced an action plan for IPv6 deployment for its public e-services. Employees at the Swedish Tax Agency explain that it is important to deploy IPv6 alongside IPv4 so that everyone can reach the Agency's e-services regardless of where they are connecting in the world. First, public e-services should support IPv6; second, system-to-system communication between public authorities should support IPv6; third there should be full deployment of IPv6.

1.2 Discussions about the reasons for deployment

During consultations with stakeholders, discussions resulted in and focussed on the reasons for deploying IPv6. Furthermore, this issue does not seem to have been included on the agenda for the management groups. It transpires that IPv6 is a low-priority issue.

IPv6 involves a technical issue (an infrastructure issue). It raises issues relating to the cost of deployment and the resources that deployment requires. It is also not deemed to be a business area (if one is a commercial operation) and entails costs.

1.3 PTS should organise a exchange of knowledge and experiences for stakeholders within the public sector

Several stakeholders stated both during the consultation and the views submitted during the formal consultation that it would be valuable if PTS hosted an exchange of knowledge and experience between public authorities, municipal authorities and county councils. This will enable experiences from practical deployment to be shared and disseminated.

2 PTS's experience

PTS started its work with the deployment of IPv6 alongside IPv4 for its public e-services in 2009. PTS's external website and all e-services at etjanster.pts.se, email and DNS currently support IPv6.

New hardware and software that require IPv6 support was procured in a coordinated way in conjunction with the move to new premises. The Agency used the Legal, Financial and Administrative Services Agency's framework contract for this procurement.

PTS does not want to lower its level of accessibility in relation to the firewall's cluster function, which only supported IPv4 in the existing hardware at that time. A separate firewall was purchased through which all IPv6 traffic was routed. It was difficult to acquire a firewall and email filter that both supported IPv6 and provided a sufficient level of security. IPv6 support for DNS, email and its external website was deployed after PTS through an agreement had secured the same SLA for IPv4 and IPv6. The Agency operates these services under its own auspices.

PTS's existing system for receiving and filtering incoming emails against spam and viruses did not support IPv6. At first, PTS was able to use a temporary solution. This meant that instead of replacing the entire system, a supplementary system was deployed that enabled the same functions to be performed over IPv6. Only incoming email via IPv6 is sent to the new system. The new system is based on Linux and an open source code.

PTS's experience is that the configuration of routers and firewalls was particularly time-consuming. The same applied to the configuration of the BGP router (the border router in relation to Internet Service Providers) for external connections, as the authority is multihomed. Their experiences show that activating IPv6 on a web server takes up the least amount of time.

PTS used approximately 120 consultancy hours for the deployment. Their advice is to ensure that expert consultants are engaged for the complicated work involving the configuration of hardware and software. Furthermore, PTS's own members of staff worked on the deployment; in total approximately 250 man-hours.

The table below shows the estimated cost and time spent on deployment.

Component	Estimated cost	Estimated time spent*
Training of staff in the IT Section	SEK 5,000 per day and person	2 people x 3 days
IPv6 Internet connection incl. BGP	No additional costs for IPv6 in existing Internet connection + SEK 1,000 per month for BGP over IPv6 Cost of consultants, approx. SEK 28,000	Consultancy time for configuration and activation, 2-3 days
Firewall	1. Temporary supplementary IPv6 firewall, SEK 10,000. 2. Move of IPv6 traffic from	1. Time for setting up system of rules, approx. 8 hours 2. Consultancy time,

	temporary IPv6 firewall to existing clustered environment	approx. 60 hours
L2 and L3 switches	Existing environment, SEK 0 Cost of consultants, approx. SEK 72,000	Consultancy time, approx. 60 hours
Operating system (web servers, email servers, etc.)	Upgrading Windows OS, approx. SEK 5,000, transfer of CMS	Configuration and activation, 2-3 days
DNS	Existing environment, SEK 0	Configuration, 1 day
Email with SPAM and antivirus protection	Open source code, SEK 0	Installation and configuration, 4-5 days
Consultancy hours		

*The time taken includes learning time when IPv6 was first deployed by PTS staff

Appendix 9 - National and international work relating to IPv6

This appendix highlights some examples of activities and initiatives that have been and are being implemented, both nationally and internationally.

1 National perspective

In Sweden there are a number of organisations whose work involves IPv6. The following provides examples of organisations and websites where further information can be found.

1.1 .SE

.SE (Internet Infrastructure Foundation), which is primarily responsible for the operation of the national Swedish top-level domain ('.se'), has also been assigned to promote and develop the Internet in Sweden. This foundation has produced several guides relating to IPv6, e.g. concerning IPv6 maturity both within the private and public sectors in Sweden, CPE equipment that supports IPv6 and also a guide to the deployment of IPv6 in a medium-sized undertaking.

.SE has arranged seminars and training relating to IPv6. More information about IPv6 can be found on .SE's website, http://www.iis.se/internet-for-alla/ipv6. Some of the seminars are available on http://www.youtube.com/user/internetfoundation.

.SE has produced web training for IPv6.

1.2 eGovernment Delegation

The eGovernment Delegation together with the Swedish Association of Local Authorities and Regions (SALAR) and the Stockholm County Association of Local Authorities (KSL) has produced guidelines for the deployment of IPv6. These were published in the autumn of 2010. The guidelines are available at the following link http://www.edelegationen.se/sida/vagledning-for-inforande-av-ipv6.

1.3 ISOC-SE

The Internet Society in Sweden (ISOC-SE, http://www.isoc.se) is a non-profit association forming part of ISOC (Section 2.3 of this appendix). The purpose of ISOC-SE is to provide information about the Internet and the Internet

Society, support the development of the Internet in Sweden and work to achieve effective use and organisation of the Internet. The SOC-SE would like to, as an association, organise both corporate and private members to work with Internet issues in Sweden.

Use of the Internet and the importance of the Internet to Swedish society are ISOC-SE's fields of work. The society is specifically interested in everything that affects the electronic communications infrastructure in Sweden and the use of this infrastructure. In this connection, ISOC-SE wants to be able to cooperate with Swedish public authorities regarding the rules, control and organisation of our infrastructure.

1.4 Municipal and public authorities that support IPv6

The following websites http://www.kommunermedipv6.se and http://www.myndighetermedipv6.se have summaries of the municipal and public authorities respectively that have activated IPv6 in various public e-services.

2 International perspective

This section provides information about a number of international stakeholders that are working to deploy IPv6.

2.1 APNIC

APNIC is the regional Internet registry in the Asia and Pacific region (http://www.apnic.net/). APNIC provides information and advice on getting started with IPv6 at the following website http://www.apnic.net/community/ipv6-program.

2.2 ARIN

The North American Internet registry is called ARIN (American Registry for the Internet Numbers, https://www.arin.net/). ARIN is responsible, among other things, for the administration of IP addresses in its region. ARIN provides information about IPv6 on several of its websites, including https://www.arin.net/knowledge/ipv6_info_center.html and http://teamarin.net/spread-the-word/.

ARIN has also set up an official IPv6 Wiki where the registry encourages its community to contribute their experiences of the deployment of IPv6, see http://www.getipv6.info/index.php/Main_Page.

2.3 ISOC

The Internet Society (ISOC) is a worldwide organisation. ISOC has around 100 member organisations and around 44,000 private members in 80 countries.

ISOC organised the World IPv6 Day initiative on 8 June 2011. Several major organisations and undertakings activated IPv6 on this date during the course of a day. The purpose was to test IPv6 on a large scale and investigate whether any problems arose. Information and lessons from the day can be found, among other places, at http://www.worldipv6day.org/

2.4 IPv6 Forum

IPv6 Forum is an organisation that collects information about IPv6 (http://www.ipv6forum.com/). There are country-specific IPv6 forums, such as http://www.ipv6forum.se for Sweden.

IPv6 Forum has a certification operation that makes it possible to become a certified instructor, technician, Internet Service Provider, etc. within IPv6. The IPv6 Forum also certifies hardware that supports IPv6, http://www.ipv6ready.org

2.5 Irish IPv6 Task Force

The Irish IPv6 Task Force is a group in Ireland comprising representatives of the public and private sectors (http://www.ipv6.ie/). Its objective is to disseminate information and raise awareness of IPv6. This is done under the auspices of the Department of Communications, Energy and Natural Resources.

2.6 RIPE NCC

RIPE NCC (Réseaux IP Européens Network Coordination Center) is the regional Internet registry that, for example, is responsible for assigning IPv4 and IPv6 addresses in Europe and the Middle East (http://www.ripe.net). RIPE NCC has provided information for a long time about, for example, the importance of IPv6 deployment and the scarcity of addresses in IPv4. They also provide a number of e-services such as statistics relating to the global deployment of IPv6.

Examples of RIPE NCC's e-services include:

- An information portal called IPv6ActNow http://www.ipv6actnow.org/. This is intended for several different kinds of user; e.g. governments, Internet Service Providers and others
- Information about the number of networks on the Internet (AS numbers) that have activated IPv6: http://v6asns.ripe.net/
- Information about the proportion of Swedish Internet Service Providers that have activated IPv6: http://v6asns.ripe.net/v/6?s=_ALL;s=SE;s=_RIR_RIPE_NCC
- The RIPEness e-service provides statistics on the preparedness/maturity of Internet Service Providers in relation to IPv6 activation. Comparisons between countries as well as between individual service providers can be made using this e-service http://ripeness.ripe.net/ and http://ipv6ripeness.ripe.net/pies.html
- An e-service to award points to LIRs (local Internet registries, typically Internet Service Providers) with respect to IPv6
- RIPE NCC's summary of the findings from World IPv6 Day. https://labs.ripe.net/search?review_state:list=published&b_start:int=0&Subject:list=ipv6day
- A web page for RIPE's regional meetings, including presentations about, among other things, IPv6: http://www.ripe.net/ripe/meetings

2.7 Go6

Go6 is an institution that originated in Slovenia (http://go6.si). The intention of Go6 is to gather together experts who have experience of IPv6. Through Go6 they will disseminate their skills and provide training and advice about how to deploy IPv6.

2.8 The Slovenian Government

The Slovenian Government is working together with Go6 to produce a plan for activating IPv6. This plan is based on a feasibility study. It is available in Slovenian at http://go6.si/docs/Studija-IPv6-MVZT.pdf.
The Slovenian Government plans to finance training so that it is possible to started with IPv6 more quickly.

One of the largest Internet Service Providers in Slovenia (Telekom) has announced that it will activate Native IPv6 for private individuals during the autumn of 2011.

2.9 Office of Management and Budget

The Office of Management and Budget (OMB) in the United States has started a federal IPv6 Task Force. The work of OMB involves enabling all public authorities to activate native IPv6 on their websites, email systems, DNS and

Internet Service Providers. The objective is for this to be carried out no later than by the end of 2012. All computers in the internal networks will support IPv6 by the end of 2014. OMB emphasises the importance of dual stack – that both IPv4 and IPv6 are activated. OMB cooperates with NIST. They will have meetings with all of the public authorities during the autumn of 2011 to discuss the objectives. For information on the objectives for deploying IPv6, see: http://www.cio.gov/documents/IPv6MemoFINAL.pdf.

OMB had already produced a plan for the transition to IPv6 in 2005, Memorandum 2005
http://www.whitehouse.gov/site/default/files/omb/assests/omb/memorandm/fy2005/m05-22.pdf

Information about OMB can be found at http://www.whitehouse.gov/omb och http://www.whitehouse.gov/omb/organization_mission/).

2.10 NIST

The National Institute of Standards and Technology (NIST, http://www.nist.gov) forms part of the US Department of Commerce. Among other things, they have been assigned to promote the deployment of IPv6 and have published several documents relating to the importance of IPv6 deployment and how to set about activating IPv6. Examples include:

- A procurement guide for equipment that supports IPv6 for the public sector: http://www.antd.nist.gov/usgv6/
- Advice on how to activate IPv6 securely (SP 800-119): http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf.
- A website for the US Government's Profile and Testing Program for IPv6 (USGv6) can be found at http://www.antd.nist.gov/usgv6/index.html.

2.11 American IPv6 Task Forces

Several local IPv6 Task Forces have emerged within the United States. They are independent and loosely linked to the North American IPv6 Task Force and the global IPv6 Forum http://www.ipv6forum.com/. They organise meetings to discuss issues relating to IPv6. The most prominent IPv6 Task Forces are Texas (TXv6TF) and Colorado (RMv6TF).

2.12 SURFnet

SURFnet is a Dutch non-profit organisation. It forms part of a higher education and research collaboration for innovation development within ICT. SURFnet has been assigned to improve higher education and research. It has produced a manual about how to produce an IPv6 address plan http://www.surfnet.nl/en/nieuws/Pages/IPv6numberplan.aspx.

Appendix10 - Solutions using open source codes

This appendix provides examples of solutions using open source codes that support IPv6. This is done for the purpose of moderating information about commercial software and hardware and showing alternatives. The list is not comprehensive. A common feature is that they are free-of-charge.

Function	Program
Firewall	M0n0wall - http://m0n0.ch
Firewall	Pfenese - http://pfsense.com/
Firewall	Vyatta - http://www.vyatta.org/
Firewall	LEAF Project - http://leaf.sourceforge.net/
CMS	Wordpress – http://www.wordpress.org
CMS	Joomla – http://www.joomla.org
CMS	Drupal – http://drupal.org
CMS	Frog CMS - http://www.madebyfrog.com/
DNS	Unbound – http://www.unbound.net
DNS	BIND – http://www.isc.org
DNS	PowerDNS – http://www.powerdns.com/
DNSSEC	ZKT - http://www.hznet.de/dns/zkt/
DNSSEC	OpenDNSSEC – http://www.opendnssec.org/

Mail server	Dovecot - http://www.dovecot.org/
Mail server	Roundcube - http://roundcube.net/
Mail server Anti-spam/ Antivirus	MailScanner - http://www.mailscanner.info
Mail server/MTA	Sendmail - http://www.sendmail.org
Mail server/MTA	Postfix - http://www.postfix.org
Proxy	Squid - http://www.squid-cache.org/
Proxy	Apache - http://projects.apache.org/projects/http_server.html
Proxy	Nginx - http://nginx.org/
Proxy	Tinyproxy - https://banu.com/tinyproxy/
Router	Quagga - http://www.quagga.net/
Router	Vyatta - http://www.vyatta.org/
Router	Xorp - http://www.xorp.org/
Web server	Apache - http://projects.apache.org/projects/http_server.html
Web server	Nginx - http://nginx.org
Monitoring	Cacti - http://www.cacti.net/
Monitoring	Nagios - http://www.nagios.org/

Appendix 11 – Explanations of terms and abbreviations used

This appendix provides explanations for many of the terms and abbreviations used in this description.

Term	**Explanation**
6to4	An automatic IPv6 over IPv4 tunnel. This is activated from Start in Windows Vista and Windows 7.
A RR	A RR contains information about an IPv4 address.
AAAA RR	Quadruple A (AAAA RR) contains information about an IPv6 address.
AD	Active Directory (AD) is an LDAP-based directory service from Microsoft that contains information about the different resources in a network, e.g. computers, printers and users.
Anycast	Anycast is a technology used to create redundancy. Anycast enables you to publish a service, often DNS, in several different places but using the same IPv4/IPv6 address.
Appliance	Hardware or virtual machine. Available for many different functions/services.
ARP	Address Resolution Protocol is used for address translation between the network level (layer 3) and the link layer level (layer 2). This function is called Network Discovery Protocol (NDP) in IPv6.
AS number	A number that identifies who you are on the Internet. All major Internet Service Providers, as well as small organisations that are multihomed via BGP, have their own AS number.
Authoritative name server	A DNS server that is responsible for a domain's ('zone's') information.
BGP	The Border Gateway Protocol is an important protocol that enables the Internet to function. It maintains a table of IP networks or 'prefixes', which then designate network reachability among autonomous systems (AS).
CMS	Content Management System is an assistive aid to enable websites to be created easily without the need for any knowledge of HTML. Common systems include Wordpress, Drupal, Episerver and SiteVision.
CNAME	Canonical Name is used to establish an alias for a server.

DHCP Snooping	DHCP Snooping is a function to prevent false DHCP servers from being set up.
DHCPv6	DHCPv6 assigns IPv6 addresses in a controlled way within a segment. It corresponds to DHCP for IPv4.
DNS	The Domain Name System is a hierarchical distributed database for managing name resolving and addressing on the Internet. DNS comprises authoritative DNS servers and resolvers. DNS contains various kinds of item/information, which are referred to as Resource Records or RRs. Examples of items include: A – name of an IPv4 address, e.g. www.pts.se has 192.121.211.215 AAAA – name of an IPv6 address, e.g. ww.pts.se has 2001:67c:dc:43::215 MX – Mail Exchange, where email to a domain is to be sent
DNS64	Translates, for instance, IPv4 A RR into IPv6 AAAA RR to enable NAT64 to function.
DNSSEC	DNS Security Extensions is an extension of the domain name system, the aim of which is to increase the reliability and security of the system.
Dual stack	When a node supports IPv4 and IPv6 at the same time.
Dynamic ARP Inspection	Function to prevent 'ARP poisoning' where the attacker typically becomes a default gateway and in that way can eavesdrop on and control traffic.
Glue record	A glue record is, for instance, an A or AAAA RR that points at an IP address on a DNS server. This requires a name server that is responsible for its own zone.
GUA	Global Unicast Address is an IPv6 Unicast address that is routed and reachable over the Internet. Everyone who surfs and all services reached via the Internet must use GUA.
GUI	Graphical User Interface, a user interface.
ICMPv6	Internet Control Message Protocol version 6 (RFC 4443) corresponds to ICMP in IPv4. ICMPv6 is an integral part of IPv6 and provides error reporting, diagnostic functions (e.g. ping) and a framework for extensions to implement future changes.
IETF	The Internet Engineering Task Force is an organisation that produces 'Requests For Comments' (RFCs) concerning new proposals for protocols.

IGMP	The Internet Group Management Protocol is a protocol that attends to the management of multicast messages for clients and connected routers. Multicast management is an IPv6 network handled by Multicast Listener Discovery (MLD), which uses ICMPv6 messaging contrary to IGMP's IP encapsulation.
IGMP Snooping	IGMP snooping is a way in which a network switch can listen in on an IGMP conversation between clients and routers. By listening to these conversations, the switch sets up a map of which links need IP multicast streams. Multicasts may be filtered from links that do not need them.
IPAM	An IP Address Management system is a system for planning, tracking and managing the IP address space used in a network. DNS and DHCP are typically included in IPAM to deal with the management. They can notify each other about changes (e.g. DNS knowing of the IP address taken by a client via DHCP, and updating itself accordingly).
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol is an IPv6 over IPv4 tunnel, the purpose of which is to easily be able to activate IPv6 in networks where routers do not support IPv6.
IP6.arpa	IP6.arpa is the IPv6 equivalent of IPv4's in-addr.arpa. In other words, what names do the following IPv6 addresses have; for example, host 2001:67c:dc:43::231 1.3.2.0.0.0.0.0.0.0.0.0.0.0.0.0.3.4.0.0.c.d.0.0.c.7.6.0.1.0.0.2.ip6.arpa domain name pointer mailscanix.pts.se.
IPv6 Only	Device that only has IPv6 activated. Such a device must use NAT64 to communicate with IPv4 Only devices.
Local Internet Registry (LIR)	A local Internet registry, often at a national level, that provides end users with AS numbers and IP addresses (networks). An LIR is often an Internet Service Provider.
MIB	Management Information Base is a virtual database used for managing the entities in a network.
MIM	A Man In the Middle attack is an attack where vulnerabilities in the ARP protocol are exploited in IPv4 and pretend to be a default gateway (area border router) and in this way can eavesdrop on traffic. In IPv6, the attacker pretends to be a router or DHCPv6 server.
MTA	Mail Transfer Agent. A server that transports email, typically via the SMTP protocol. Internet Service Providers often provide their customers with such a service.

Multicast for IPv6	Multicast – a source that sends a datastream to one or more registered recipients. IPv6 NDP is based on multicast.
Multihoming for IPv6	Usually used to create redundancy in Internet connections where there are several operators.
NAT, NAT64	Network Address Translation is a solution that allows several IPv4 addresses to share a public IPv4 address. NAT64 – Address translation between IPv6 and IPv4, must be used together with DNS64 to function well.
Native IPv6	'Real' IPv6, i.e. IPv6 data that is not tunnelled inside an IPv4 packet.
NDP	Network Discovery Protocol is the IPv6 equivalent of ARP in IPv4.
NXDOMAIN	A Non-existent Domain Name is when DNS cannot find information about a domain name in DNS. RFC 1035 (Domain names - implementation and specification) and in RFC 2308 (Negative Caching of DNS Queries or referred to as DNS NCACHE).
PA-IPv6 address	Provider Aggregated IPv6 address. Provider dependent addresses. If you change provider, you must renumber the network.
PI-IPv6 address	Provider Independent IPv6 address. Provider independent addresses; if you change provider, you do not have to renumber the network. Also used to multihome the network.
Regional Internet Registry (RIR)	There are five RIRs around the world covering different geographical zones: RIPE (Europe and the Middle East region), ARIN (North America), APNIC (Asia and Pacific), LACNIC (Latin America) and AFRNIC (Africa). The primary task of the RIRs is to provide LIRs with IPv4 addresses, IPv6 addresses and AS numbers.
Registrar	A registrar offers services relating to a domain name. Examples of services may be the new registration or deregistration of a domain name, a change to a domain name such as change of DNS servers, activation of DNSSEC.
Resolver	A DNS function used to look up DNS data, e.g. what IP address www.pts.se has.
Roaming Clients	External clients who connect remotely via VPN to, for example, an organisation network (e.g. teleworkers or external consultants).
Route6 object	An object that says how an IPv6 prefix is routed on the

	Internet.
Router Advertisement (RA)	An IPv6 router tells nodes in a segment how they should address the IPv6 interface via Router Advertisement. This may involve them using SLAAC, DHCPv6, etc.
Router Advertisement Guard	See RFC 6105.
SAVI	Source Address Validation Improvements, IETF Working Group on SAVI.
SEND	Secure Neighbor Discovery, RFC 3971.
SLA	Service Level Agreement is a contract through which one agrees on the availability of a service (e.g. up-time, reinstatement time, correction period, etc.)
SLAAC	Through StateLess Automatic Address Configuration, the node uses information from RA to automatically set up one or more IPv6 addresses in a network interface.
Teredo	An automatic IPv6 over IPv4 tunnel. Activated from Start in Windows Vista and Windows 7.
UTM	Unified Threat Management is a function in firewalls or other security products that analyses the traffic in more depth. For example, it can filter viruses, ensure that it is HTTP that is being run on port 80, etc.