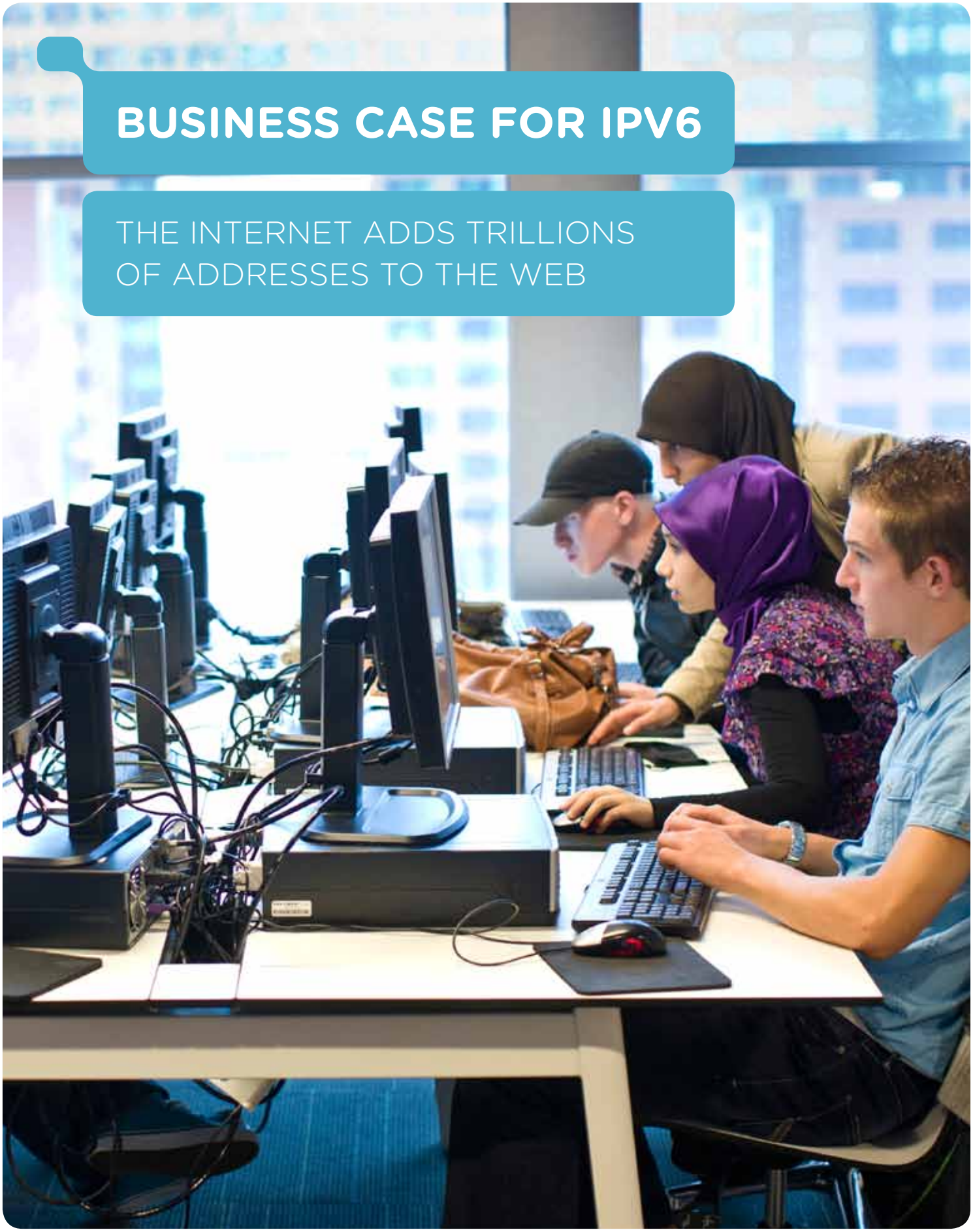
BUSINESS CASE FOR IPV6

THE INTERNET ADDS TRILLIONS OF ADDRESSES TO THE WEB



Jan Michielsen, Aad van Rijn
July 2013

SURF NET

CONTENTS

2. IPV6 -SHOULD YOU INTRODUCE IT OR NOT?

1.1 Lots of questions

There's a lot of discussion about IPv6 and a lot of questions. Why should you introduce it? What will it cost, and what are the benefits? What problems will it solve? Why start using IPv6 right now? What will happen if we do nothing? When will we need to have introduced it?

There aren't any easy answers to all these questions. But in this business case we will try to indicate why IPv6 is necessary; what the risks are if you don't introduce it (Section 1); what phases are involved in doing so (Section 2); and what scenarios you can follow to introduce it (Section 3).

1.2 Arguments for introducing IPv6

We're running out of IPv4 addresses.

The introduction of IPv6 is directly related to the unavoidable fact that we are running out of IPv4 addresses. We'll need more and more IP addresses in the years ahead, for example because of new technologies such as 4G. Uses have more and more devices with which to go online, such as mobile phones and tablets. IPv6 offers sufficient room to allocate an address to all these new devices. That's why IPv6 will become more convenient to use. IPv4 is becoming increasingly less convenient because workarounds are needed to connect devices to the Internet.

Unlike the "millennium bug" or the advent of the euro, no hard-and-fast date can be given for the introduction of IPv6: that date can be different for each individual organisation. IPv6 needs to be introduced before connectivity is lost, or before security problems arise. The table below shows how Europe is running out of IPv4 addresses. The expectation is that we will soon reach phase IV. At that Point, RIPE NCC – the organisation that allocates IP addresses for Europe, the Middle East and parts of Asia – will only be able to allocate IPv6 addresses.

FASE 1	• Lots of IPv4 addresses available. • RIPE NCC distributes addresses according to defined policies.	
IANA's pool of IPv4 addresses is exhausted.		All 5 RIRs are given a final /8.
FASE 2	• RIPE NCC distributes addresses according to defined policies.	
RIPE NCC starts on the final /8 (16 million addresses)		
FASE 3	• RIPE NCC is altered on the basis of the final /8	
All RIPE NCC addresses have been used up (2013/2014)		
FASE 4	• RIPE NCC can now only allocate IPv6 addresses.	

No connectivity to Internet services

IP addresses are allocated within a number of Internet regions (Europe, North America, South America, Africa, and Asia/Pacific). Even if enough IPv4 addresses are still available in one Internet region (or part of it), there can still be connectivity problems. This is because users and services will switch over to IPv6-only if there are no more IPv4 addresses available for other regions, companies or institutions, and IPv4-only devices will no longer be able to connect to them. In particular, connectivity with services in Asia can be at risk because IPv4 addresses have already become extremely scare there. As a result, organisations miss out on "new business", for example student registrations or collaboration with international partners in research or industry.

Temporary solutions are available – for example Network Address Translation (NAT) – that can make it possible to continue using IPv4 for a few more years. Although this does circumvent the address space problem, end-to-end connectivity and security issues will arise at the same time. Such solutions merely postpone the inevitable and ultimately lead to higher overall costs.

Increased IPv6 traffic

Currently, some 0.5% of Internet traffic goes via the Dutch AMS-IX IPv6 Internet node. The past few years have seen major players such as Google and Facebook already switching on IPv6. Operating systems also increasingly prefer IPv6 to IPv4. Expectations are that by 2017 some 50% of European Internet traffic will be on the basis of IPv6; by 2020, the figure is expected to be more than 50% of total traffic worldwide.

The reason for this increase in IPv6 traffic is that providers of IT services and equipment are flocking to implement IPv6, with government bodies imposing regulations that require it. This means that IPv6 is automatically becoming the most commonly used protocol, and switching to it will ultimately become unavoidable.

IPv6 is already present on the network

Suppliers of network equipment and software no longer make it possible to switch off the IPv6 feature of their products, meaning that these will always process IPv6 traffic. At a certain point, there will therefore also be IPv6 traffic on your institution's network. In fact, there is already IPv6 traffic within an IPv4-only network without the end-user being aware of it. It is therefore important to manage that traffic efficiently: to know that it's there, to know whether it's running smoothly, and to know how to make it secure.

1.3 Introducing IPv6 also involves risks

As we have already pointed out, not introducing IPv6 involves certain risks. But if you do introduce it, you need to make changes to the operational environment, and like every change in IT infrastructures this is also not without its risks. You can avoid these risks by preparing your IPv6 implementation properly.

At first, not every provider will have already implemented IPv6 in its products and services. This means that:

- applications and Internet services may no longer work;
- end-users may be unfamiliar with specific IPv6 problems and may call the helpdesk;
- the admin organisation may not have the necessary know-how and skills to quickly identify and solve the various problems;
- there may be major security risks for the end-user.

It's also the case that IPv4 has been intensively used on the Internet for years now. To a large extent, all the vulnerabilities and glitches in the protocol and in the equipment that uses it have already come to light and been rectified. IPv6 is less "mature" in this regard, and vulnerabilities can be expected to make themselves apparent in the coming period. It's therefore important to regularly check updates etc.

Before introducing it, organisations need to know about IPv6 technology. They also need to check and test whether IPv6 is properly supported within their systems and they need to have the right procedures in place. If all this is tackled properly, then there is little risk of Internet services actually becoming unavailable.

1.4 Recommendation: start using IPv6, and start on time!

We are running out of IPv4 addresses – it's inevitable

As we've already seen, organisations really do need to start using IPv6 because all the available IPv4 addresses will inevitably be used up. It's therefore advisable to get started with IPv6 on time and to tackle it systematically. Doing so costs time and money, but it will be cheaper to start early and be systematic about it than to wait until the last moment.

The cost of postponement

Waiting until the last moment to implement IPv6 will involve the necessary costs. There won't then be the required IPv6 know-how within your organisation, even though IPv6 is already a standard "on" feature of new systems and is therefore in fact already status quo. Malfunctions and security incidents will involve more time and risks if your institution isn't prepared for IPv6. This will imperceptibly increase the amount of work for your ICT staff and consequently the hidden costs too.

Implement IPv6 in good time

Getting an early start with IPv6 means that you can spread the necessary investment and staff deployment out over a longer period, with introduction taking place gradually and with a natural, smooth transition to the new protocol. This will reduce the associated risks and will prevent unfamiliarity leading to unforeseen problems. The organisation will gradually acquire the know-how needed to switch over to IPv6 and it will be possible to make the necessary alterations to your systems gradually.

2. PHASES IN THE IMPLEMENTATION PROCESS

2.1 Introduction

Introducing IPv6 will ultimately be unavoidable, but it doesn't need to be done immediately. During the preparatory phase, the institution can already get it's network "IPv6-ready" without too much money or effort being required.

This section explains the phases that are ideally involved in introducing the new protocol. We focus a lot on the preparatory work, which costs relatively little money or effort (Sections 2.2 and 2.3). The network can become IPv6-ready almost automatically. The foundations can thus be laid for actual introduction of IPv6 (Sections 2.4 and 2.5). This allows the institution to ensure that introduction can take place quickly when the time is ripe.

2.2 Create awareness

The preparatory phase requires "IPv6 awareness" within the organisation, specifically among its ICT staff, management, and the purchasing department. People need to be aware that IPv6 is inevitable, and that relatively little effort is involved in already making the necessary preparations. The prevailing idea should be that there is actually no reason not to get started with IPv6. The arguments set out in Section 1 can be used to create that awareness.

Time required

- Awareness session for sales and IT management stakeholders: 2 hours
- Analysing and revising the current security policy plan: 4 to 8 hours

2.3 Include IPv6 in RFI/RFC and life-cycle management

The next step after creating awareness is to take account of IPv6 when updating and upgrading the network. At every stage in that process, the IPv6 specifications need to be included in the requirements for the necessary features. RFIs and RFCs also need to be assessed for compliance with the prescribed and required IPv6 specifications.

IPv6 can then easily be included in the life-cycle management of the infrastructure. This is a relatively simple but extremely important step: if the institution does not think about IPv6 on time, then purchasing new equipment that supports it may turn out to be very expensive because it may need to happen very quickly, outside the framework of life-cycle management. There's even the risk of disinvestment if equipment needs to be replaced that has not yet reached the end of its economic life.

Equipment and software often have an economic life of at least 3 years. For network equipment such as switches, routers, firewalls, load balancers and blade servers, it's often 5 to 7 years. But within 5 years, IPv6 is expected to have really taken off and to be used in almost every network.

That's why we advise including IPv6 in life-cycle management now, on the basis of the IPv6 specifications included during the previous phase. At the end of its economic life, equipment can then automatically be replaced by equipment that supports IPv6. The network will become IPv6-ready almost automatically. The cost of introducing the new protocol will be spread out over a lengthy period so the investment remains manageable.

Training and/or recruiting staff is also part of life-cycle management. It's important that the people who need to work with the software and equipment can deal with IPv6.

Time required

- Including the IPv6 specifications in an RFI/RFC: 4 to 8 hours
- Including IPv6 in life-cycle management: 4 to 8 hours

2.4 Carry out an IPv6 scan

In order to introduce IPv6, it's important to know to what extent the network is already prepared for the new protocol. What equipment is present, and how far does its support IPv6? Answering that question requires a survey of the current situation in the form of an IPv6 scan. This involves checking each element or group of elements from each supplier to see whether they support IPv6, and to what extent.

The results of the IPv6 scan are then used to determine the cost of equipment and software in the subsequent stages of introduction. Immediately after this phase, one can start planning introduction.

Time required

Depending on the size and extent of the infrastructure, the IPv6 scan will take from one week to several weeks. SURFnet can carry out the scan free of charge (3 days external consultancy) but involvement by the internal organisation will need to collaborate for about 12 to 16 hours; this involves providing information and reviewing results.

2.5 IPv6 within the infrastructure

After the IPv6 scan has been carried out, the institution will know what the situation is and it can then proceed to the next step, namely actual implementation of IPv6 within the organisation. This will involve the following activities:

- training the organisation's staff to work with IPv6;
- creating and testing a new network design;
- upgrading existing equipment and implementing new equipment;
- making changes to the management systems and processes;
- starting actual use of IPv6.

Time required

The efforts required in this phase depend on the introduction scenario that is chosen (see Section 3).

3. SCENARIOS FOR IMPLEMENTING IPV6

3.1 Introduction

IPv6 can be introduced either gradually or suddenly, i.e. by means of an evolution scenario or a revolution scenario (or a hybrid version). The difference between the scenarios is in the time taken and the personnel deployed (mainly internal or mainly external personnel). Each scenario also has a different "character": the evolution scenario takes place in a calm, planned manner, while the revolution scenario is more rushed because not much time is available. The "controlled revolution" scenario is a hybrid version. The various scenarios are dealt with in this section.

The costs involved in getting the equipment IPv6-ready are not necessarily different in each scenario, although proper preparation can cut costs (see Section 2). However, the investments will be made at different times in the various scenarios.

3.2 Evolution scenario (3 years)

Process

In this scenario, all the preparatory work has already been done:
- the organisation has been made "IPv6-aware" (Section 2.2);
- IPv6 has been included in RFI/RFC and life-cycle management (Section 2.3);
- an IPv6-scan has been carried out (Section 2.4).

The next step is for the people within the organisation to regularly devote a bit of time to IPv6. They need to do this well before IPv6 actually needs to be introduced so that the transition is a gradual one. They familiarise themselves with the technology, and they then start actively working with IPv6. This may mean setting up small-scale network designs, for example, and testing them in a controlled test environment within the network. A deliberate decision has therefore been taken not to systematically bring in external expertise in order to implement IPv6.

The costs involved in this scenario will be for employee training, occasional hiring of external expertise, and testing within a controlled environment consisting of a network, firewall, security, servers, and clients.

The advantage of this scenario is that people get to know IPv6 and their knowledge is transferable within the organisation. Once a start has been made with IPv6, it will automatically become a standard part of people's work and it will no longer be necessary to make the costs explicit.

Time required

As an indication, this scenario involves 3 to 4 people devoting 2 to 4 hours a week to getting the network, security, servers, and clients ready for IPv6. Over a 3-year period, this will amount to a total of about 2000 hours. In addition, external expertise will be brought in for about 3 days per quarter.

3.3 Controlled revolution scenario (6 to 12 months)

Process

This scenario involves the organisation starting to use IPv6 bit by bit. IPv6 will already have been included in the RFI/RFC and in life-cycle management. Actual implementation will be delayed, however, until the business or an end-user requests it.

Introduction of IPv6 will therefore be relatively sudden and quick. It will not be possible to have implementation carried out entirely by the organisation's own people. They will not have the know-how or time to do all the necessary extra work during their normal working hours. The institution will need to bring in external expertise and resources so as to complete implementation within an acceptable period of time.

Implementation will need to take place quickly, and costs will be involved in carrying out the project. Internal training will also need to be speeded up. Additional migrations may also be necessary, and short-term investment will be required to replace equipment that is not IPv6 compliant. That may well be equipment that has not yet been written off, which means disinvestment.

Time required

Based on hiring 2 FTEs of external expertise for a period of 9 months and deploying 1 to 2 FTEs of the organisation's own staff for 3 to 6 months, this scenario will take 3000 to 4000 hours.

Risks

One major risk with this scenario is that rapid introduction will cause malfunctions in the operational systems. The operational management systems and processes will also need to be altered simultaneously. There is also the risk that this scenario will turn out to be much more expensive in the long run than the evolution scenario.

3.4 Revolution scenario (3 months)

Process

In this scenario, the institution waits to introduce IPv6 until it has become absolutely necessary to do so (for example because connectivity to Internet services is under threat). The preparatory phases will not have been implemented early on, meaning that IPv6 will need to be introduced suddenly, unexpectedly, and extremely quickly.

In this scenario too, it will not be possible to have implementation carried out entirely by the organisation's own people. They do not have the time to acquire the necessary know-how during their normal working hours and to carry out testing.
The institution will therefore need to bring in external expertise and resources so as to complete implementation within an acceptable period of time. That period will also be significantly shorter than in the controlled revolution scenario, and more will need to be done. After all, the organisation will not yet have any IPv6 know-how and IPv6 will also not have been included in its life-cycle management.

Besides accelerated training and instruction for the organisation's own staff, there will be costs for carrying out the project. Additional migrations may also be necessary, and short-term investment will be required in order to replace equipment that is not IPv6-compliant. That may well be equipment that has not yet been written off, which means disinvestment.

Time required

Based on hiring 8 FTEs of expertise for a period of 3 months, this scenario will take more than 4000 hours.

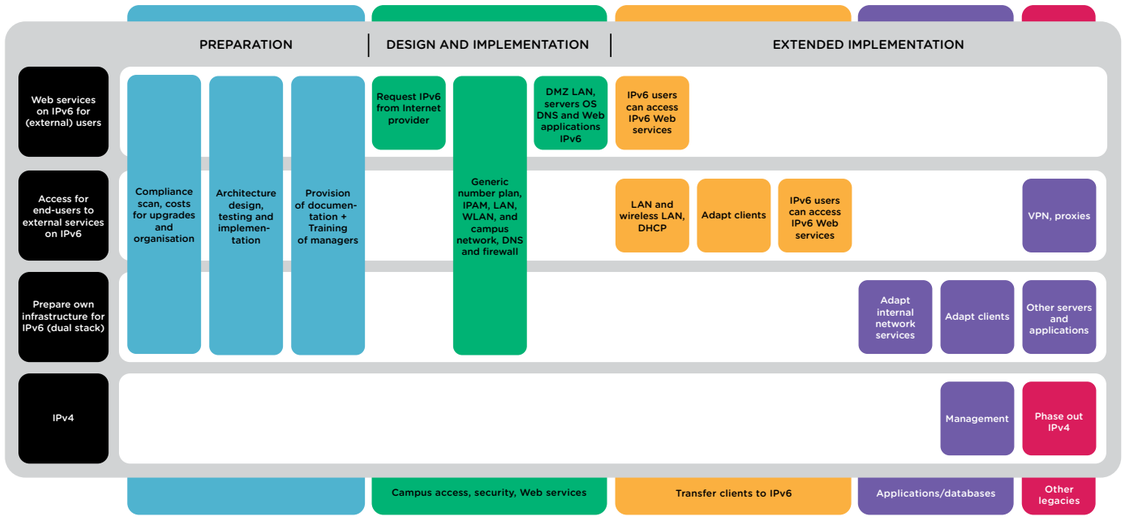
Risks

One major risk with this scenario is that rapid introduction will cause malfunctions in the operational systems. The operational management systems and processes will also need to be altered simultaneously. There is also the risk that this scenario will turn out to be much more expensive in the longer term than the evolution scenario.

4. OVERVIEW OF TIME INVOLVED

This business case describes all the main steps involved in the introduction of IPv6. The work involved is shown in the diagram below. This indicates the phases for the main activities. The length of the various phases depends on the scenario selected.

The introduction of IPv6 will have an impact on various parties within the organisation; they have therefore been included in the table.



SURFnet
Radboudkwartier 273

PO Box 19035
3501 DA Utrecht
The Netherlands

T +31 (0)30 2 305 305
F +31 (0)30 2 305 329

admin@surfnet.nl
www.surfnet.nl