PROCESS FOR IPV6 MIGRATION IN LARGE ORGANIZATIONS

Pedro Filipe Martins de Castro
Instituto Superior Técnico, Lisboa, Portugal
pedro.martins.castro@ist.utl.pt

Keywords: Migration, IPv6, Company, Plan, Process

Abstract: The shortage of IP addresses has become the bottleneck for Internet development. IPv4 has no longer the capacity to support the continuous growth of the Internet. For this reason, a new Internet protocol was needed. However, the version 6 of the Internet protocol is not compatible with version 4, hence, transition mechanisms must be used to ensure the transition from IPv4 to IPv6. Enterprises not prepared for this transition will pay a high price. Since most of the enterprises around the globe have no IPv6 knowledge to create a decent road map towards IPv6, we present in this thesis a generic migration process, which provides the necessary guidelines to reach a successful IPv6 migration. This plan is composed by 9 phases: analysis of the current situation, present a study focused on the migration impact for the company, survey of the enterprise's network, analyse IPv6 support from ISPs, estimate the costs of migrating the company's network, migration plan, testbed, identify problems and final implementation. We then apply this process to a specific case.

1 Introduction

Although IPv6 was standardized 17 years ago, its adoption is yet very limited [5]. This happened due to the use of Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT), which disguised the limitations of IPv4 in the last years. CIDR ended with the huge waste of addresses caused by the previous addressing architecture, which was based on classes. And NAT made possible the sharing of the same IP address by different users, ending with one of the Internet principals: every IP address must be unique. However NAT is not a perfect solution, quiet the opposite, it has some drawbacks like the break of end-to-end communications, its complexity and lack of scalability as well as reachability problems.

With the depletion of addresses in Asia-Pacific region in the last year and now in Europe, IPv6 has become the best option to ensure the continuous growth of the Internet. If we look to concepts like Internet of Things, intelligent houses or smart grids, which can take communications to a whole new level, we realize that IPv4 can no longer respond to their demands. To allow the emergence of new concepts like the ones presented, it is mandatory to proceed with the transition to IPv6. It is important to realize that this transition will not happen from day to night, instead IPv6 and IPv4 will operate in parallel for many years as already happens. It is expected that the protocol takes at least one decade to spread across the entire Internet [2]. Even after this time some services may still be available through IPv4.

IPv6 will be the future of the Internet. With the depletion of IPv4 addresses, IPv6 migration is the only feasible option to allow the continuous growth of the Internet. The question now is how much time the transition will last. Many companies like Google, Facebook or Yahoo already gave the first step in order to start this transition by providing their services through IPv6. It will be interesting to see how organizations all around the globe are going to react to the imminent end of IPv4 addresses. Initiatives like the one from U.S Government, who is making an effort to have all its agencies web sites and services available through IPv6 will put them far ahead of organizations and countries that are waiting to see what will happen. Therefore migration mechanisms must be studied and analyzed by organizations and governments to find the best approach to meet their needs. However, people are still very reluctant to invest in IPv6 due to the huge investment needed, the lack of IPv6 knowledge and awareness and the fact that NAT still gets the job done.

Sooner or later IPv6 will be present in every network around the globe, so, in order to minimize the costs and to simplify the transition to IPv6, this article defines a generic migration process that can be used by network administrators as a reference/guideline to introduce IPv6 in their networks. Then, we apply this process to a small part of the Refer Telecom's network. Thus, we will be able to validate our migration process in a real scenario.

2 Background

The evolution of today's networks to IPv6 in the next years is a fact. Due to the use of CIDR and NAT the emergence of IPv6 was delayed more than expected. However now that the last IPv4 prefixes are allocated both in Europe and in Asia, migration won an increased importance.

2.1 IPv6 Advantages

The following list contains some of the most important changes and additions introduced by IPv6 [7]:

Increased number of addresses - The major problem with IPv4 is the lack of address space. IPv6 eliminated this problem by proving an address space with a length of 128 bits instead of the 32 bits of IPv4. Therefore, IPv6 addresses aren't likely to exhaust in a foreseen future. With this improvement, IPv6 solves the scalability issues present in IPv4.

Better support for Non-Unicast Addressing - IPv6 has a new kind of addressing: anycast. Anycast addressing routes a packet to the nearest or more accessible member of a group where every node is identified by the same destination address.

Multicasting has been improved and broadcast was withdrawn from IPv6 since this function could easily overload a network.

Renumbering - It is easier to renumber the IP addresses in networks and sub networks. It is also possible to renumber a router address.

Auto configuration - IPv6 uses SLAAC [8], which enables a host to automatically generate an IPv6 address when it is turned on. Using this address, called Link-Local Address, a host can communicate within its local network without a DHCP server. If there is an IPv6 router, an IPv6 host within the local network can have a global unicast address assigned by this router, automatically allowing access to the Internet. With SLAAC we can have a "plug and play" network which means that a computer will have an IP address as soon as it connects to the network.

Datagram Format - A new header format was created for IPv6 to make routing more efficiency.

QoS - The new header also has QoS related fields: traffic class and flow label. It allows classification of packets.

Improved fragmentation - In IPv4, fragmentation was done by the routers on the path between the source and destination nodes. Now with IPv6 the fragmentation is performed by the source node through the use of ICMPv6. This way the workload on routers is reduced [3] because routers do not have to waste time analyzing the MTU in the link where they will send a packet and fragmenting it if necessary.

Mobility - In IPv6, mobility support is mandatory through the use of Mobile IPv6 (MIPv6). Through the use of extension headers, which added powerful capabilities to Mobile IPv6 and its enormous address space, IPv6 enhanced Mobile IP features. The following list [6] shows some of this improvements when compared to Mobile IPv4:

- Route optimization is a built-in feature for Mobile IPv6, whereas in Mobile IPv4 it is added on as an optional set of extensions that may not be supported by all nodes. This procedure helps to avoid triangular routing.
- Address Auto-configuration and Neighbor Discovery allow mobile nodes to work in any location without the need of special routers (foreign agents).
- Mobile IPv6 takes advantages of the IPv6 protocol itself. It uses the routing header instead of IP encapsulation, therefore it reduces the overhead present in Mobile IPv4.
- In order to avoid the ingress-filtering problem present in Mobile IPv4, the correspondent node uses the care-of address as the source address.
- Utilization of IPSec for all security requirements.

End-to-End communication - In IPv4 this semantics was lost due to the use of NAT. IPv6 brings back end-to-end communications ensuring full network transparency. True end-to-end communication makes it easier to maintain a network and may enable the appearance of new services [1].

Throughput - IPv6 can reach higher throughputs and a RTT than IPv4 under the same circumstances [9].

2.2 Migration Costs and Benefits

With the transition to IPv6, organizations can enhance their business models in several ways. Network management can became much easier for network administrators due to IPv6's ability to configure itself; therefore the costs of internal network management will be lower. Beyond that, new opportunities will emerge, so we will have new ways of making money.

There are some aspects in IPv6 that can really change the way a enterprise works, for example the mandatory support for mobility allows mobile teams to be constantly interconnected; the abundance of IP addresses renders private addresses unnecessary, thus it is no longer necessary to manage NATs. Although the elimination of NAT brings back the transparency of the networks, it plays an important role on the security of users located behind a NAT box, since it is not possible for a machine to initiate communication with a host located behind a NAT box. Therefore enterprises stop having a single entry point for their network. However, the use of NAT is not the only way to achieve this, proxies can be use with the same purpose.

IPv6 can facilitate the "Internet of Things" emergence[1]. This concept refers to a network interconnecting common objects equipped with intelligence modules, so it is not possible for "Internet of Things" to grow within an IPv4 network due to its lack of address space and scalability.

Many economic sectors could profit with IPv6 adoption like: entertainment, leisure, gaming, transportation, health care and education [1].

IPv6 can also facilitate the emergence of smart grids, which use information and communications technology in an automated manner to allow communication schemes for monitoring and managing the generation, transmission and distribution of electricity. Finally, IPv6 can allow the appearance in higher numbers of intelligent houses, since these houses require a considerable number of addresses to interconnect all the devices in them.

The benefits that IPv6 can bring to this sectors are obvious. So, what is holding back the migration? Here are some of the main reasons:

- The huge investment needed to upgrade existent equipment or acquire new equipment with IPv6 capacity;
- Compatibility problems between the two protocols;
- NAT;
- The experience with this new protocol is limited;
- Some security problem may arise;
- Must exist an interoperability with hardware and software used;
- The business return on such an investment is uncertain.

Even if enterprises do not want to spend time and money to make their services available through IPv6 right now, they should at least prepare for this scenario. There will be costs for companies that do not prepare themselves for IPv6:

- By being reactive instead of proactive the costs with the transition will be much higher because there will be no time to prepare a proper migration plan.
- If a company that is already planning the migration has to buy new equipment and services, they can ensure that the equipment bought is compatible with IPv6. Other companies may waste money on equipment that must be replaced in a couple of years because they do not have IPv6 support.
- With the exhaustion of IP addresses in Asia, IPv6 is the only solution to allow new users in that area to access the Internet. Therefore exists here a new market waiting to be explored.
- Companies not prepared for IPv6 can hurt their reputation if their rivals are already prepared for IPv6. For example if a service is made available through IPv6 and Company A cannot provide this service, because they did not prepare themselves for IPv6, they may loose clients to companies that already support IPv6.

3 Methodology for the Migration Process

The purpose of this section is to create a migration process, which can serve as a reference/guideline for a team of engineers responsible for migrating their company's network to IPv6. However each network has its own specifications, therefore a specific migration plan must be created for each case. In some cases this plan will be identical to the one proposed here, but in others cases there will be some (or many) modifications depending on the type of network and its requirements. We can look at these steps and view them as a generic set of steps for a transition towards IPv6. The plan proposed aims to ensure 5 objectives:

- An IPv6 enabled network
- Minimize costs
- Minimize the risk associated with the migration to IPv6

- Ensure the smoothness of the process
- Go unnoticed

The migration process presented below was based on the RFC 4057 and 4852, who already define some points to be taken into account when performing a migration to IPv6.

1. Analysis of the current situation
   - (a) Enterprise business
   - (b) Technological maturity of company
   - (c) Critical applications for the business
2. Present a study focused on the migration impact for the company
3. Survey of the enterprise's network
   - (a) Network
   - (b) Equipment
   - (c) Applications
   - (d) Services
4. Analyse IPv6 support from ISPs
5. Estimate the costs to migrate the company's network
6. Migration plan
   - (a) Upgrading or replacing equipment without IPv6 support
   - (b) Addressing plan
   - (c) Phased deployment of IPv6 into the network
   - (d) Treat network's dependencies without IPv6
   - (e) Partial decommissioning of IPv4
   - (f) Decommissioning of IPv4
7. Testbed
8. Identify problems
9. Final implementation

3.1 Anaysis of the Current Situation

The business of the company must be analysed, to better understand the consequences that IPv6 can have to the enterprise. It is easy to realize that some businesses rely on networks more than others. Propose a migration from IPv4 to IPv6 in a small company with a very limited network is an entirely different thing than creating a migration plan for a big company. If we are creating a migration plan for a company with multiple branches, we must take into account the interconnections between all of these branches. It is probably not a good idea to create a migration plan for just one part/branch of a company, because there will probably exist dependencies from other points of the company's network. This could result in a company being able to migrate its central office to IPv6 and communicate with the outside but cannot communicate with other points of its own network, because these points were not consider in the migration plan. For the same reason, clients that want to access services located outside of the central office will not be successful. Therefore a migration plan should only be established if a ”full picture” of the company's network is available. If, for some reason it is not possible to fulfill this requirement, the migration plan should be delayed.

The list of requirements will be different for every company, not only based on their size and business but also in their technological maturity. Other major concern should be the applications and services that the company uses and it depends on. If a critical service or application for the company does not support IPv6, a solution must be found.

3.2 Present a Study Focused on the Migration Impact for the Company

Some companies already are fully aware of the need to migrate to IPv6, making this step a courtesy or even unnecessary. However a large percentage of companies worldwide do not know why they have to migrate to IPv6 or the advantages that this new format of the Internet Protocol can bring. For those companies this is an early but crucial point. If the managers of the company are not convinced that they will gain something by migrating to IPv6, they will not spend money in this project, at least for now. So one must present a study where it shows the benefits that an early IPv6 adoption can bring to the company.

3.3 Survey of the Enterprise's Network

An exhaustive analysis of the enterprise network is needed to better understand what has to be done in order to proceed with the migration. This is one of the most important aspects in a migration plan because in order to obtain a fully functional IPv6 network, the topology of the network must be fully analysed to guarantee that the right decisions are taken. It is not possible to create a good migration plan for an enterprise if we do not have a full knowledge of their network. One must have knowledge of every component of the network and its dependencies to establish a secure and reliable transition.

3.4 Analyse IPv6 Capacity from ISPs

Not all ISPs are prepared for IPv6. Some of them did not even start to plan their transition to IPv6 [4], so the ISP or ISPs of the company must be contacted in order to understand which type of services are they offering through IPv6. After that one can analyse the different offers and decide which ISP(s) has the better offer and is more reliable. It is important to ear the ISPs plans for IPv6 because a migration plan done now can be put in practice only in a few years. By then an ISP that is not offering IPv6 connectivity right now, can have their services fully operational through IPv6.

3.5 Estimate the Costs to Migrate the Company's Network

After the analysis to the company's network and to ISPs responsible for providing Internet and other services to the company, it is a good idea to estimate the costs of this operation, using the information obtained in the preceding steps. The equipment and services that must be upgraded or replaced must be specified. Alternative solutions should be presented for replacing these services and equipment with no support for IPv6.

In this phase one must know what type of approach the company wants to follow. There are four different paths for the company to follow:

- Upgrade entire network to IPv6
- Upgrade some parts of the network to IPv6
- Create a new network
- Keep an IPv4 network able to communicate with IPv6 users

With all this in mind and taking into account the choices of the company it is possible to do a feasible estimation of the costs involved in this operation.

3.6 Migration Plan

With the information obtained in the preceding phases, a migration plan can start to be defined. In order to proceed with the migration plan it is essential that the costs for migrating to IPv6 have already been estimated. If the document with the costs estimation is not elaborated, it is necessary to perform in this step, the analysis of the network equipment and to choose which type of migration the company wants: upgrade the entire network to IPv6, upgrade some parts of the network to IPv6, create a new network or keep an IPv4 network that is able to communicate with IPv6 users.

As soon as the migration plan gets an approval by the company's administration it is time to start the actual migration. This plan should include all the proceedings that must be followed in order to achieve a successful migration, starting with the training of IT staff and ending with the IPv4 shutdown.

Before starting the transition to IPv6, there are some things that must be done first:

- Every department in the company is informed about the IPv6 migration.
- Give IPv6 training to the IT staff (or else they are not able to migrate the infrastructure and maintain it).
- All software developed inside the company takes IPv6 into consideration
- All software and hardware acquired from that moment on must support IPv6. If the equipment needed do not have IPv6 support and no feasible alternatives are available, the equipment's suppliers should be questioned about their road map for IPv6. If there is none, the equipment can be acquired but the company will have to use mechanisms like NAT64 to allow its use in an IPv6 only network.
- Acquire an IPv6 address block from its LIR.
- Define a lab environment to make some experiences with IPv6. This way, there is no risk to disrupt the services.
- Learn with others mistakes. If possible analyze similar IPv6 migrations in other companies to avoid mistakes and problems that may have occurred.

With all that done we can proceed to the implementation of IPv6 in the network. However this process should be done carefully and divided into different stages:

1. **Upgrading or replacing equipment without IPv6 support**

   All the information needed for this task can be retrieved from point 5 (Estimate the costs to migrate the company's network).

2. **Addressing Plan**

   Since the address format in IPv6 is different from IPv4, a company has to make an all-new addressing plan. This procedure must be done carefully, so that the available pool of IP addresses is not wasted and it is distributed accordingly to the different departments in the company. There are rules that should be followed when designing an addressing plan, just like in IPv4. Due to the size of the IPv6 addresses, it is very important to follow these rules because with such a large space of addresses to use, the probability of the address plan becoming a mess is too high.

3. **Phased deployment of IPv6 into the network**
   After having an addressing plan we can start to migrate the company's infrastructure to IPv6. To achieve a successful migration we should enable IPv6 in the following order:
   - Routers, firewalls and switches
   - Basic network services
   - Workstations
   - Servers

   If the company has a DMZ to protect the internal network from unwanted accesses, we should enable IPv6 in the internal network and only after should we proceed to enabling IPv6 in the DMZ. Therefore we can mitigate network problems created with the use of IPv6 in the network and correct them before proceeding with the migration in the DMZ.
4. **Treat network's dependencies without IPv6**
   There may be in the network some services that cannot be upgraded or even replaced to support IPv6. In these cases, we must find plausible alternatives. If there is no viable alternative we may try to use a solution like NAT64/DNS64 allowing these services to communicate with IPv6 devices.
5. **Partial decommissioning of IPv4**
   When the use of IPv4 has reduced drastically and is no longer relevant we should decommissioning IPv4 from workstations and servers and use DNS64 and NAT64 to allow existing IPv4 users to communicate with the rest of the network.
6. **Decommissioning of IPv4** With the end of IPv4 traffic we are finally able to turn off IPv4. All the monitoring and management over IPv4 can be decommissioning. Translation services like DNS 64 and NAT64 can also be decommissioning. IPv4 addresses are returned to the respective LIR.

3.7 Testbed

The IT department should create a platform to test a scenario as close to the real one as possible. This step is essential because a migration plan is much more reliable if it is based on a carefully defined testbed. The testbed and the migration plan may be elaborated together, this way it is possible to realize almost immediately if the recommendations written are viable or should be replaced.

3.8 Identify Problems

In the testbed all possible situations should be tested in order to discover potential limitations. All the problems encountered like connectivity issues must be registered in this phase, so that problems like these are eliminated when the implementation starts.

3.9 Final Implementation

With a migration plan defined and tested we can finally perform the migration to IPv6 according to the migration plan created.

4 Practical Case

As we mention earlier we applied our migration process to a subset of the Refer Telecom's network. To be more specific this subset is composed by the data centers network of Refer Telecom. We started by analyzing the business areas of Refer Telecom and show them the benefits that IPv6 adoption could bring for a company in its position. The next step was the analysis of the Refer Telecom's network and all its components, where we also analysed the costs that a migration to IPv6 would involve. After all this is done we moved on to the definition of a migration plan, which we will describe here in more detail.

4.1 Migration Plan for Refer Telecom

Taking into consideration the size and dimension of Refer Telecom's data centers it would not be feasible to create a migration plan for its entire network in this work. Therefore Refer Telecom selected a few of their most used services and software (DHCP, DNS, Active Directory, IIS and HP Data Protector) and defined a smaller network environment (Figure 1), which tries to represent a subset of the real one.

This network has 2 internal networks (Porto and Lisbon) interconnected by a Cisco 3750 router. Both these networks have Windows clients and Lisbon's network also has a Domain Controller and a Data Protector cell manager. The domain controller besides running Active Directory also has DNS and DHCP services running. The DHCP service is unique and serves the entire network. The connection to the DMZ and the public network is made through a Checkpoint firewall, which separates the internal network from the DMZ and the public network. In the DMZ there is a web server and an external DNS server. Both these services are available for both the internal and pub-

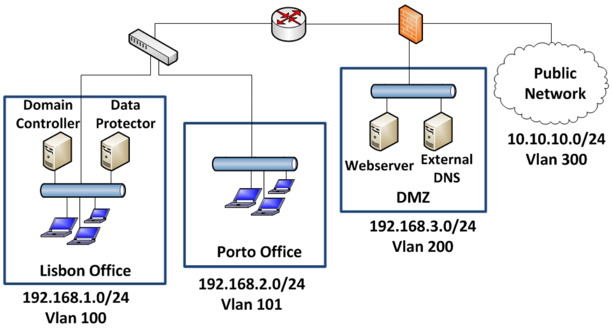


Figure 1: IPv4/IPv6 addresses

Services and equipment	Version	OS
Domain Controller (AD/DHCP/DNS)	2008 R2	Windows Server 2008 R2
HP Data Protector	7.0	Windows Server 2008 R2
IIS	2008 R2	Windows Server 2008 R2
External DNS	BIND 9.8.2	CentOS 6
Porto's Hosts	Windows 7	Windows 7
Lisbon's Hosts	Windows 7	Windows 7
Router	Cisco 3750	IOS 12.2
Firewall	Checkpoint R75.40	GAIA

Table 1: Services and equipment

lic network. To consult the version and the OS of the equipment and services, refer to table 1.

4.1.1 Upgrading or Replacing Equipment Without IPv6 Support

Here is where the document about the estimation of costs comes in handy. This document contains information about all the necessary steps to assure IPv6 support in all network equipment and services. After all the recommendations presented in the document are fulfilled we can move on to the next phase.

4.2 Addressing Plan

Enabling IPv6 in the network is a process that must be carefully planned. It should follow a predefined order and not a random order. Some equipment and services like routers and firewalls must be enabled before any others. But there is something that should be done before all this, which is the creation of an addressing plan. We do not want to give random IPv6 addresses to the migrated hosts instead we should create an addressing plan as efficient as possible.

We will use the following address space: 2001:da12:1234::/48. Therefore we have 16 bits to create subnets since the last 64 bits are used for addressing hosts . Thus we can use all the prefixes from 2001:da12:1234:0000::/64 until 2001:da12:1234:ffff::/64 to create subnets, in a total of 65536 subnets.

We will create an addressing plan that explicitly matches the correspondent IPv4 network. Since all our IPv4 networks are /24 it is extremely easy to create a direct map between an IPv4 address and an IPv6 address. For example if we have a network 192.168.1.0/24, we can use penultimate number to perform this mapping. So the address 192.168.1.0/24 will correspond to the IPv6 address 2001:da12:1234:1::/64. For equipment using static addresses like routers or servers we can also use the last number of the IPv4 address in the IPv6 address. So, a server with the IP 192.168.1.254 will have the IP 2001:da12:1234:1::254 for IPv6. This method is very useful for a network administrator, since he can look at an IPv6 address and immediately associate that address with the respective IPv4 address. As we know is way easier to remember an IPv4 address than an IPv6 address. Without this method it is not possible for a network engineers in big environments to know to what machine a given IPv6 address belongs without consulting information regarding the list of IP addresses. Taking this into consideration we will use the mapping of IPv4 addresses into IPv6 addresses for our network. The mapping of addresses is very interesting regarding servers and routers but for common hosts is almost irrelevant. These hosts will get IPs from DHCPv6 without any relation to the correspondent IPv4 addresses.

4.2.1 Phased Deployment of IPv6 into the Network

The deployment of IPv6 through the network should be done according to this order:

1. Routers, firewalls and switches
2. Basic network services
3. Workstations in the internal network
4. Servers and services in the internal network
5. DMZ

We should focus first on the internal network and once the internal network is fully IPv6 enabled and monitored we can start enabling IPv6 in the DMZ. This order should be followed for two reasons. The first is that by enabling IPv6 in just one part of the network it is easier to perform and monitor the migration. The second reason regards the DMZ itself. The DMZ should be left for last because it requires special attention in terms of security. Since the DMZ is open to the outside, a simple mistake could compromise the entire network whereas the internal network cannot be reached through the outside. Thus a mistake here would not have the same impact as one in the DMZ.

Routers, firewalls and switches - Routing and security devices should always be the first devices where IPv6 is enabled. First of all, IPv6 must be enabled on the only router present in the network. The router has to be able to respond to any request coming either through IPv4 or IPv6. The same thing goes for the firewall. It has to be configured to process IPv6 packets with the same rigor of IPv4 packets. All the existing firewall rules must be adapted to IPv6 and since Checkpoint cannot inspect extension headers, (except for the fragmentation one) they should be dropped.

Since the switches only work on layer 2, there is no real impact from IPv6 in them. The only part where the IP protocol is used is for management, so we will need to configure IPv6 addresses in their management interfaces.

Basic network services - After enabling IPv6 in the firewall and in the router we need to enable basic network services like DNS and DHCP before having concerns with other devices. There is no reason for migrating services and hosts to IPv6 who rely on DNS and DHCP to work, before those services are IPv6 enabled. As we seen before both of these services run on a single machine, together with Active Directory. Once this machine is IPv6 enabled, we should be able to start creating AAAA records. After that we can move on to DHCP and activate DHCPv6. Active Directory should have no problem working over IPv6 after the machine and the DNS server are configured for IPv6.

Workstations in the internal network - All the workstations in the internal network run Windows 7. IPv6 should be enabled on every PC of the network and should be configured to get an IP address via DHCPv6.

Servers and services in the internal network - Looking at our internal network we can see that in this phase we should enable IPv6 in Data Protector Cell Manager. Data protector works with names not with IP addresses, so as long as our DNS server is well configured and the system where the cell manager is running has an IPv6 address, the cell manager should have no problems working with IPv6 instead of IPv4. Besides the cell manager, the media agent and the system on which we want to run a backup must also be IPv6 enabled and have their names registered in the DNS server. Thus we will be able to perform backups, regardless of the version of the Internet Protocol used.

4.2.2 DMZ

In the DMZ there are two servers that need to be migrated. One runs the web server and the other runs BIND as the external DNS server. To allow connection to the web server over IPv6 we just need to enable IPv6 on the machine hosting the web server. For BIND we need to go a bit further, since BIND has to be configured to handle AAAA records. In the end of this phase all equipment and services should have been configured with dual stack. All network features supported for IPv4 should now be supported using IPv6. If there is any feature of the network who is not working properly over IPv6, we have to point the respective feature and deal with it in the next phase.

4.2.3 Treat Network's Dependencies Without IPv6

As we seen before every component of the network has support for IPv6, therefore we should be able to have the entire network working over IPv6 with no limitations. However, it is possible that when the migration is putt into practice or the testbed is elaborated, we find some special features presented in the IPv4 network that are not supported in IPv6. In this case we have to find a plausible alternative. The alternatives could be:

- Find out if the equipment will have support for that feature any time soon
- Replacing the equipment for another with the same characteristics but with the required feature
- Replacing the equipment for another with similar characteristics and support for the required feature
- Find a way to avoid this problem
- Decommissioning of the equipment

4.3 Partial Decommissioning of IPv4

Once the IPv4 traffic is no longer relevant (somehow compared to today's IPv6 traffic), we should take measures to reduce the company concerns with IPv4 usage. Therefore, IPv4 should first be removed from workstations and then from servers. In order to be able to reach the few IPv4 users spread across the public network, we need to implement NAT64 and DNS64. Here we can use a solution like the one provided by A10networks [1], which is exactly what we need. So by adding this device to the DMZ, it will be possible for both internal and external IPv6 clients to access IPv4 hosts and servers. Although this solution is made to allow IPv6 users to access IPv4 content and not the other way around, this is not an immediate requirement, because nowadays there is

[1] http://www.a10networks.com/products/axseries-NAT64_DNS64.php (last accessed October 1th, 2013)

no IPv6-only content. This will only be a reality in the next decade probably, so by then, this solution from A10networks as well as many others will also provide NAT46 services. As the name suggests, NAT46 is the opposite of NAT64, it allow IPv4 users to access IPv6 content.

4.3.1 Decommissioning of IPv4

When IPv4 is no longer used it is time to proceed to its decommissioning:

- NAT64, NAT46 and DNS64 should be discontinued since they are no longer needed.
- IPv4 should be removed from the firewall and the router.
- IPv4 addresses should be returned to the respective LIR.

After completing this last phase we have finally completed our IPv6 migration.

5 Validation

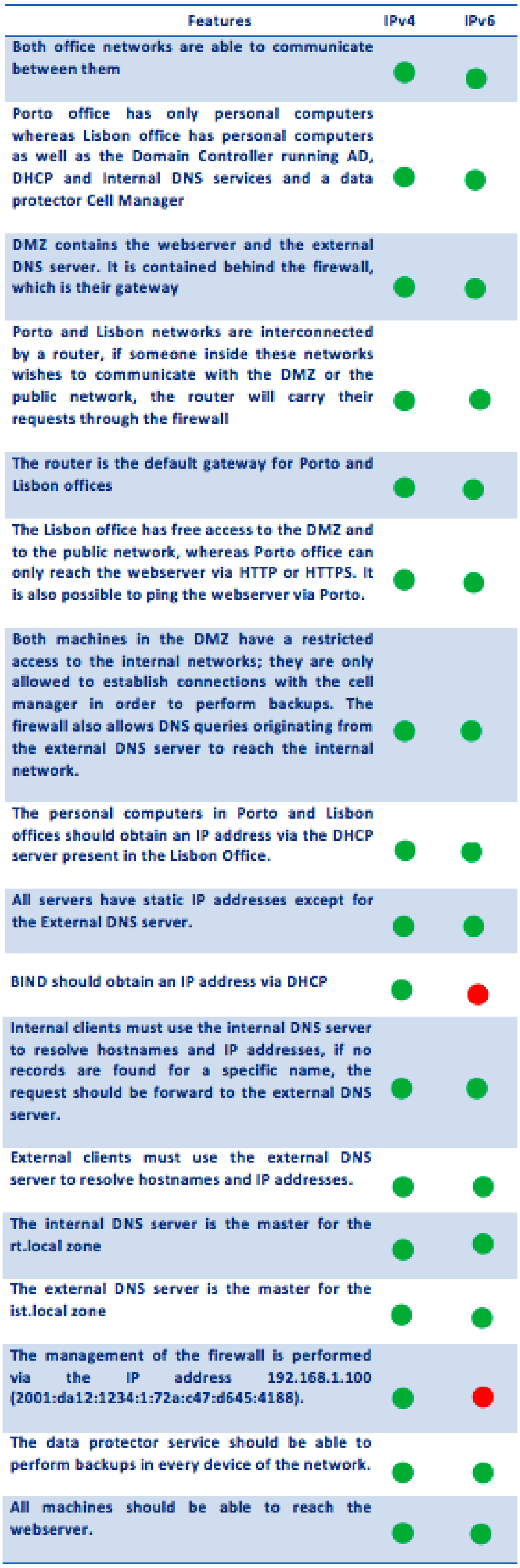
To validate our migration plan we created a Testbed where we could simulate the transition from IPv4 to IPv6 in an environment as close as possible to the one present in Figure 1. Due to space and equipment limitations we had to create a virtual network to simulate the real one. To do it, we used VMware ESX 5.1. First we created the IPv4 network with all its features (to check this features you can look at Table 2) and then we tried to enable IPv6 in the network following our migration plan. The result is present also in Table 2 where we can see if all the network features are now supported for both IPv4 and IPv6.

There were only 2 features that we were not able to implement in IPv6: firewall management over IPv6 and DHCPv6 relay. In both cases checkpoint R75.40 does not have IPv6 support.

Resolving the first problem (firewall management over IPv6) is very simple. We just need to upgrade our Checkpoint from R75.40 to R76. R76 brings several new IPv6 enhancements and managing the firewall using IPv6 is one of them.

The problem concerning DHCPv6 relay is a bit harder to solve because none of Checkpoint firewalls has DHCPv6 relay implemented. Therefore we must find an alternative and these are the ones we can use:

- Find and alternative firewall who support DHCPv6 relay
- Implement a DHCP server in the DMZ
- Use static addressing instead of DHCP



Features	IPv4	IPv6
Both office networks are able to communicate between them	🟢	🟢
Porto office has only personal computers whereas Lisbon office has personal computers as well as the Domain Controller running AD, DHCP and Internal DNS services and a data protector Cell Manager	🟢	🟢
DMZ contains the webserver and the external DNS server. It is contained behind the firewall, which is their gateway	🟢	🟢
Porto and Lisbon networks are interconnected by a router, if someone inside these networks wishes to communicate with the DMZ or the public network, the router will carry their requests through the firewall	🟢	🟢
The router is the default gateway for Porto and Lisbon offices	🟢	🟢
The Lisbon office has free access to the DMZ and to the public network, whereas Porto office can only reach the webserver via HTTP or HTTPS. It is also possible to ping the webserver via Porto.	🟢	🟢
Both machines in the DMZ have a restricted access to the internal networks; they are only allowed to establish connections with the cell manager in order to perform backups. The firewall also allows DNS queries originating from the external DNS server to reach the internal network.	🟢	🟢
The personal computers in Porto and Lisbon offices should obtain an IP address via the DHCP server present in the Lisbon Office.	🟢	🟢
All servers have static IP addresses except for the External DNS server.	🟢	🟢
BIND should obtain an IP address via DHCP	🟢	🔴
Internal clients must use the internal DNS server to resolve hostnames and IP addresses, if no records are found for a specific name, the request should be forward to the external DNS server.	🟢	🟢
External clients must use the external DNS server to resolve hostnames and IP addresses.	🟢	🟢
The internal DNS server is the master for the rt.local zone	🟢	🟢
The external DNS server is the master for the ist.local zone	🟢	🟢
The management of the firewall is performed via the IP address 192.168.1.100 (2001:da12:1234:1:72a:c47:d645:4188).	🟢	🔴
The data protector service should be able to perform backups in every device of the network.	🟢	🟢
All machines should be able to reach the webserver.	🟢	🟢

Table 2: IPv4 vs IPv6 features

We will use static addressing just like we used in the testbed because it is the more economic and simple solution. This way we do not need to replace the firewall nor adding a new machine to the DMZ. And since we are talking about a DNS server, we should remember that is considered a good practice to use static addresses in network servers.

6 Conclusion

IPv6 will replace IPv4 as the predominant Internet Protocol in a near future. It could take 5, 10 or 20 years but this is inevitable. Organizations around the globe must be prepared for this change and make sure they have the ”know how” to be able to succeed when they decide to migrate to IPv6.

We have shown the differences between the two protocols and the new challenges brought by IPv6 not only to service providers but to enterprises as well. The world is finally understanding the need to change and the diversity of new horizons that IPv6 will bring. IPv6 traffic as been growing exponentially in the last years and with the investment being made by ISPs and organizations worldwide this positive trend will continue in the next years. Therefore, many companies already started to plan their transition towards IPv6, however this number is yet very low when compared to companies where nothing has been done to prepare the company's network infrastructure to IPv6. These companies are the main target audience for our work, since this article proposes a generic migration process for a company that pretends to introduce IPv6 in its network. Network engineers responsible for migrating their companies networks to IPv6 can use the migration process proposed here as a reference/guideline to help them in this task.

After the development of the migration process, we applied it to a subset of the data centers' network of Refer Telecom and created a lab environment representing a subset of this network to validate our migration process. By implementing our migration process in a real scenario, we were able to see its usefulness but also the need to adapt it to the network and organization in question. Every single company has its own network specifications and rules, so we must be able to adapt the defined migration process to each individual case.

Unfortunately, due to the size of Refer Telecom, it was not feasible to create a migration process for its entire network in this work. Although the first 5 points of the migration process were made for the whole network, it was not possible to do the same for the migration plan (point 6 of the migration process). Instead Refer Telecom selected a few of their most used services and equipment and created a subset of its network to be used in our plan. So the migration plan was created for this smaller network defined by Refer Telecom. With the help of virtualization software we were able to replicate this network and prove the effectiveness of our plan.

Even without a migration plan for the entire network, it is now possible for Refer Telecom to proceed with IPv6 migration in their data centers with the help of this work. If Refer Telecom wishes, the next steps for this work will be the definition of a migration plan for the entire network and then the actual implementation of IPv6 in their data centers.

REFERENCES

[1] Daniel O. Awduchev. Benefits of IPv6 for Enterprises. White paper, Verizon Business, 2010.

[2] E. Davies, S. Krishnan, and P. Savola. IPv6 Transition/Co-existence Security Considerations. RFC 4942 (Informational), September 2007.

[3] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), December 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564.

[4] O. Dobrijevic, V. Svedek, and M. Matijasevic. Ipv6 deployment and transition plans in croatia: Evaluation results and analysis. In *Software, Telecommunications and Computer Networks (SoftCOM), 2012 20th International Conference on*, pages 1 –7, sept. 2012.

[5] Roch Guérin and Kartik Hosanagar. Fostering ipv6 migration through network quality differentials. *SIGCOMM Comput. Commun. Rev.*, 40(3):17–25, June 2010.

[6] Fayza Nada. Performance analysis of mobile IPv4 and mobile IPv6. In *The International Arab Journal of Information Technology*, volume 4, pages 153 –160, April 2007.

[7] Srinivasan.Nagaraj, B.Kishore, K.Koteswara rao, and G. Apparao. A comparative study of ipv6 statistical approach. *International Journal on Computer Science and Engineering (IJCSE)*, 2:1367 – 1370, 2010.

[8] S. Thomson, T. Narten, and T. Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862 (Draft Standard), September 2007.

[9] Yingjiao Wu and Xiaoqing Zhou. Research on the IPv6 performance analysis based on dual-protocol stack and tunnel transition. In *Computer Science Education (ICCSE), 2011 6th International Conference on*, pages 1091 –1093, aug. 2011.