Paper

IPv6 Preparation and Deployment in Datacenter Infrastructure – A Practical Approach

Marco van der Pal

Generic Services – Network Infrastructure Services, Capgemini Netherlands B.V., Utrecht, The Netherlands

Abstract—This article describes the experiences with the initiative to introduce IPv6 into Capgemini's datacenter environment, and to be more specific, the part of the project known as Phase 1: the preparation before actually doing so. Phase 1 comprises of training, testing and research of the IPv6 protocol and its features with the purpose to better understand the consequences of the introduction of IPv6 in a datacenter environment. It was a specific choice to not deploy IPv6 in a production environment, and to build a dedicated test environment first (Proof of Concept). This test environment would accommodate most basic features of IPv6 to safely prepare us for the actual deployment. The technical results of the IPv6 experience were documented in a structured way, useable for future reference. Test results were also used as input to develop Capgemini best practices for IPv6 deployment.

Keywords—best practices, defining showcases, deployment conclusions, guidelines for deployment, setting up a test environment.

1. Introduction

Two years ago some network engineers of Capgemini Infrastructure Outsourcing Services in the Netherlands (IOS-NL) put their heads together to challenge themselves with the implementation of IPv6. They wondered what it would take to implement IPv6 in their IT infrastructure and decided to create a business case. Their main goal was – of course – to address the technical aspects of IPv6.

When thinking of the implementation of IPv6 one would primarily consider it as being a technical challenge. It probably is addressing functionalities. However there seem to be many more obstacles on the road, and these are considered as important as the technical.

IP connectivity in the Capgemini IOS-NL datacenter infrastructure is solely based on IP version 4 (IPv4). IPv4 has been de facto standard for internet communications all over the world for tens of years. IP address space is limited however, and we have reached its boundaries. IPv6 was developed to overcome the IPv4 address space limitations and other shortcomings. Capgemini IOS-NL initiated a project "Introduction IPv6" to investigate IPv6 and to learn about it.

The project will encompass many phases until the goal – datacenter and customer networks fully IPv6 – will be reached. Phase 1 was intended as a learning phase to familiarize ourselves with the numerous aspects of the protocol itself, as well as to experience the consequences of the introduction of IPv6 within our existing datacenter infrastructure. This first phase is also called the Proof of Concept (PoC) Introduction IPv6. Another reason was that this would show us the best approach to safely implement the protocol in a production environment. In Phase 2 we will thus introduce IPv6 in a part of the datacenter network (the edge) "for real". The experience of Phase 1 gives guidelines to several aspects of the implementation of IPv6, among which:

- IPv6 address planning,
- IPv6 assessment of existing infrastructure,
- best practices,
- security,
- IPv4 and IPv6 coexistence,
- migration paths.

2. IPv6: Phase 1

2.1. Background

IPv6 was introduced to overcome the limitations of IPv4: insufficient address space, lack of integrated security features, complex NAT constructions and more.

However, IPv4 and IPv6 are not compatible and can't talk to each other directly. Although the protocols resemble each other at first sight, their philosophy differs. Even more complex is that IPv4 and IPv6 will be running simultaneously and parallel to one another for years. These and other reasons have lead to the initiative to carefully explore the ins-and-outs of the IPv6 protocol in a separate environment, before even attempting to bring IPv6 into production.

2.2. Aim

The Proof of Concept aims to fulfil a number of major goals:

- to gain hands-on experience with implementing IPv6 in a data center environment,
- to gain the knowledge and confidence to be able to build a IPv6 enabled data center,

– to build a representative IPv6 test environment for further development, testing, knowledge transfers and training,

– to develop a new consulting service to customers, known as "IPv6 Audit", to assess the client's infrastructure for its readiness to adopt IPv6.

2.3. Starting Points

The starting points for the Proof of Concept Introduction IPv6 are:

- The introduction of IPv6 should be a collaboration between different Capgemini business units and disciplines:
  - IOS, Capgemini Infrastructure Outsourcing Services; the owner of the Capgemini datacenter infrastructure;
  - ITS, Capgemini Infrastructure Transformation Services, providing consultancy to clients;
  - APPS, Capgemini Application Services; provider of complex software applications like Oracle and SAP.
- To be able to examine all features and functionalities of the IPv6 protocol the project is (technically) multidisciplinary. The following solution teams are involved:
  - networking
  - Unix/Linux,
  - Microsoft,
  - applications,
  - consultancy.
- The technical aspects of IPv6 are investigated within a separate test (PoC) environment. The only allowed shared component is remote access to the PoC environment. This ensures that all testing does not in any way affect the customer's production environment.
- Most of the used hardware in the test environment consists of surplus devices, thus available on short notice and resulting in low costs.
- The software used for the demo environment is either for testing or evaluation purposes or is open source.
- The IPv6 test environment is physically placed in a dedicated and easily accessible test room, and will remain available until further notice. This means that modifications to the test environment can be made without using formal procedures.
- The test environment is primarily virtualized to minimize the physical set of hardware.
- The showcases in the test environment have been defined as those that represent the majority of real life situations, but is not intended to cover all possible situations.

3. Goals for the Proof of Concept

3.1. What We Want to Achieve

The primary goal of the PoC Introduction IPv6 is to gain knowledge, expertise and experience of the IPv6 protocol and its features:

- Basic knowledge can be achieved by theoretical study and through training. The members of the IPv6 project team have had a generic 5 day IPv6 training.
- Expertise can be achieved by combining theory and practice, and testing in e.g. workshops.
- Experience can be achieved only by taking theory into practice, and by trying or running into uncommon situations as well. Troubleshooting is an essential part of gaining experience.

In order to gain experience with a complex concept like IPv6 one of the goals was building a dedicated test environment, specifically aimed at working with IPv6 in all its (technical) aspects.
To be able to continuously learn about IPv6 and its features several showcases have been defined. These showcases reflect real-life infrastructure environments, and for these a test environment was built.
Currently we are working on Phase 2 of the project: deploying IPv6 in the edge environment of the Capgemini IOS datacenter infrastructure. As a preparation secondary goals have been defined as follows:

– developing a service to assess an infrastructure for readiness to implement IPv6,

– develop a deployment plan to roll out IPv6 in Capgemini IOS datacenter infrastructure.

The outcome of the Phase 2 will be a recommendation for deployment of IPv6 in Capgemini's datacenter infrastructure in a variety of possible solutions.

3.2. Setting up a Typical IPv6 Environment

To be able to test with IPv6 in a safe manner a separate test environment was built. The idea of having this dedicated test environment is also that it will be used for additional testing (e.g. new features), and for workshops and training purposes. To be able to test the relevance of IPv6 in a typical IT infrastructure, the following key areas have been defined:

– datacenter infrastructure,

– WAN connectivity,

– Internet connectivity,

– office infrastructure,

– IPv6 security.

Each of these areas consists of one or more of the following systems and functionalities that all together cover the most relevant scenarios:

- server systems,
- routers and switches,
- firewalls and general security,
- operating systems,
- client systems,
- Web services and applications,
- Internet connectivity,
- DNS,
- DHCP,
- IPAM,
- IPv4-to-IPv6 and coexistence.

Different scenarios have been defined to represent real life situations. These scenarios have been defined in showcases, which all together discuss most of the relevant key areas of IPv6, according to the needs of the implementation in Capgemini's datacenter infrastructure.

3.3. Showcases

Before we set up a test environment we first identified the key functionalities of IPv6 to investigate. These topics are considered to cover most relevant aspects of real life scenarios. The identified topics were bundled to address as many topics as possible in a single showcase.
These showcases demonstrate the capabilities of IPv6 and its basic functionality. The IPv6 showcases will teach us the similarities and differences with its predecessor IPv4.
The showcases have been defined to represent the majority of functions we're using in the Capgemini datacenters, as well as those that we expect to see in client environments. An example of a defined showcase is to hosting an IPv6 enabled website in a Demilitarized Zone (DMZ).
One of the first services we expect to be requested by clients is to host an IPv6 enabled website. In our showcase we simulate both the home user who will surf to an IPv6 enabled website as the service provider hosting the IPv6 enabled website. In a variation on this environment we also try to simulate a corporate environment where the client is an office user instead of a home user. Corporate environments usually contain proxy servers, so we include that as well.
The following functionality will be implemented (Fig. 1):

- an IPv6 enabled home user with an IPv6 capable browser,
- DNS functionality to point the client to the website,
- IPv6 Internet connectivity for both the client and the web server,
- routing, subnetting and firewalling functionality for IPv6 at the datacenter side,
- a (simulated) WAN connection with IPv6 capability to connect the corporate client to the datacenter,
- an IPv6 enabled web server,
- an IPv6 enabled proxy server.

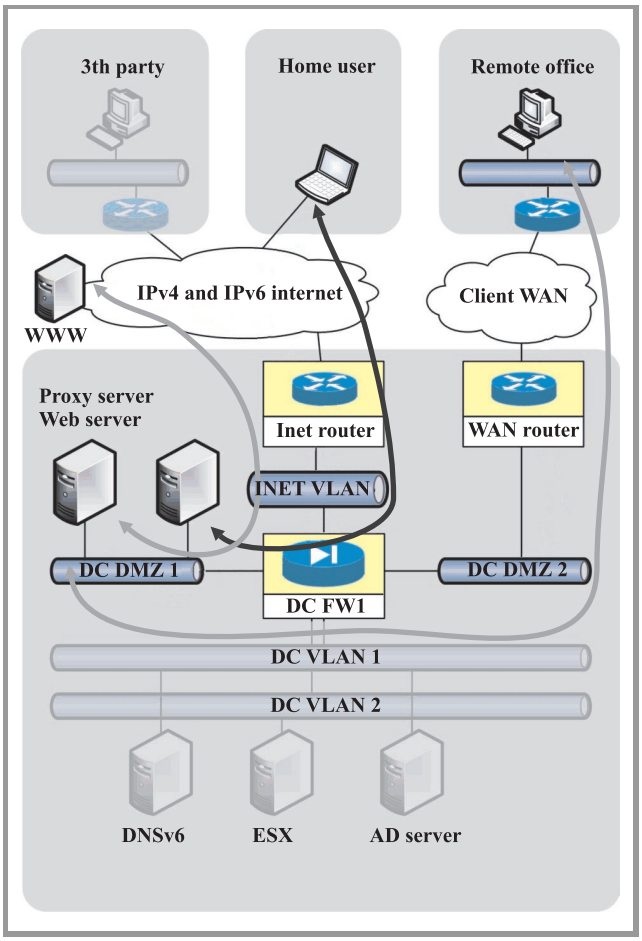

Fig. 1. Showcase example of Capgemini datacenter.

The expected results of this showcase are:

- Demonstrate that a home user can browse using IPv6 to a website hosted in Capgemini datacenter environment.
- Demonstrate this by either using a website which shows which IP address the connection is coming from, or by showing log files. In the alternative case where a proxy server is involved, show the logging of the proxy server as well.

One of the advantages of this approach is that multiple combinations of IPv4 and IPv6 functionality can be tested within one showcase. We accomplished this by pre-provisioning a set of VLANs within every area (Remote office, DMZ, production VLANs, etc.) according to the following VLAN plan.

Table 1
VLAN overview

	VLAN types	Global IPv6 Address
1	IPv4 only	
2	IPv4 + IPv6 ULA	
3	IPv4 + IPv6 Global	Manual
4	IPv4 + IPv6 ULA + IPv6 Global	SLAAC
5	IPv6 ULA	
6	IPv6 Global	SLAAC + DHCPv6
7	IPv6 ULA + IPv6 Global	DHCPv6

When testing a specific scenario it is easy to look at the same from a slightly different perspective by just moving the (VM) system to another VLAN. This will give extra meaning to the way IPv4 and IPv6 coexist in e.g. a dual-stack environment (Table 1).

3.4. Documenting Knowledge and Experiences

Since the primary goal of the project was to gain knowledge and experience with IPv6 and its features, it was of high importance to document as much as possible. This doesn't mean however to rewrite existing documentation from vendors. Every showcase was built upon vendor documentation for a specific subtopic of the entire showcase. The intention of our documentation was in bringing it all together. That would result in the following:

Design Principles. When proposing and building a (client) solution it is advised to follow design principles. These will make sure that the solution fits in a broader range of Capgemini concepts and adaptations, and will thus increase a successful delivery.

Best Practices. Every showcase would give specific results in specific situations: these were gathered to form a set of best practices, substantiated with the reason why to use it in that situation.

Do's and don'ts. When deviating from best practices it is of major importance to know what another solution would lead to. The do's and don'ts gives handles in these situations.

The documentation principle was summarized in the following statement *If it isn't documented, it didn't happen!*

To make sure all testing in the several showcases was documented in a uniform way, a test protocol was used. This protocol guides you through a series of steps to document the following:

- To document feature testing in a unified and consistent way.
- To guide the test owner through the deployment of every feature the following must be documented per test:
  - which feature is tested,
  - what are the test requirements,
  - explain starting position,
  - explain expected results,
  - describe test results with, e.g., screenshots, configurations, etc.,
  - describe unexpected behaviour,
  - describe adjustments (if any),
  - what are the advantages/disadvantages of the solution,
  - conclusion (in terms of usability, manageability, scalability, future proof, difficulty, etc.).
- To be able to use the test results in future deployments and/or to recreate the test for future use.
- As input for a Capgemini blueprint for IPv6 in the datacenter
- As input for the development of in-house trainings.

To make sure all documentation was gathered and easily accessible a Wiki was set up. The Wiki contains all project documentation, technical details about the test environment, test results, best practices, etc.

3.5. Knowledge Transfer to Capgemini Staff

The IPv6 protocol is not solely a networking technology, hence the reason to put together a project team with members from different technology areas. However, specific IPv6 knowledge can be relevant in one team only, or in multiple teams with a different main point.
The idea is to gather specific IPv6 knowledge for all technology areas, with generic theoretical knowledge for everyone, and more specific knowledge for individual teams or groups of people. The result would be a set of IPv6 technology training modules, of which some are mandatory for some technology team, and other modules would be optional.
The knowledge and experience gained in the project and in future projects will be used to develop a training program specifically aimed at the target audience. Theory and practice will be combined with use of the test environment to visualize the different topics.
In this way theory and practice will accumulate to maximize the learning effect. Individuals interested to gain more expertise on the subject are eligible to use the existing test environment. One of the conditions would be that any new experiences would be documented and shared.

4. Conclusions

The experience and the lessons learned in the proof of concept have lead to the following major conclusions:

IPv6 is a very complex protocol. It differs from IPv4 in many areas, most important its philosophy on the use of IP addressing functionalities. Another important aspect is the compatibility issues that arise when IPv6 wants to communicate to IPv4 and vice versa. All possible solutions to

overcome this issue have their technical limitations and/or are limited on, e.g., scalability or manageability.

IPv6 is evolving. New technologies are being developed, from which many address the compatibility issues between IPv4 and IPv6, primarily aiming at migrating towards IPv6. Also standards have changed in the last decade, which means that different implementations for same functionality coexist, possibly resulting in different behaviour.

IPv6 addressing is very much different from that in IPv4. Therefore IP Address Management (IPAM) and DNS are most important, not only in a normal datacenter or office environment, but moreover in, e.g., Cloud environments, where provisioning and control are key.

While working on IPv6 even more IPv6 topics will show to be interesting. It is advised to investigate these other topics as well, or at least examine them for relevancy. Besides of that, and as stated: IPv6 is evolving, so it may be relevant to keep an eye on other new (migration) technologies as well.

IPv6 is gaining popularity in the internet community. There may be other arguments that will require speeding up deployment of IPv6 in the Capgemini datacenter environment. A phased approach will give insight in deploying IPv6 in a real-life environment, and will pave the way for gradually deploying IPv6 across the entire datacenter infrastructure. This approach gives the time to learn and gain experience, even before they are sorely needed.

The project Introduction IPv6 was an infrastructure project only, mainly focusing on network, systems and OSs. This enabled us to investigate some of the IPv6 topics, but some have not had the attention they need. It is suspected that many applications and scripts have IPv4 hard-coded in the source code. It is thus to be expected that most or all of these applications will not work in an IPv6-only environment. If it is possible to work around these incompatibilities or whether the source code needs an update is unknown. It is highly advised to cooperate with the applications team to further investigate the possibilities with applications like these.

If a client requests to deploy IPv6 in the network infrastructure, one needs to know the possibilities and support of IPv6 in the current infrastructure systems and applications. Is IPv6 supported at all, and if so, which features do work, and which don't? Also make sure these features work in conjunction with one another, and be sure to examine the subtle distinctions of a vendor stating that their implementation supports IPv6. What are the demands on the current infrastructure design? What is the expertise of the IT staff? What home-made applications are used? And also what would it need to migrate towards IPv6? Expert consultants are needed to address these questions. It is therefore advised to investigate the possibilities to develop new services that can address these client demands: an IPv6 Audit to assess the network infrastructure and related services, and IPv6 Migration Services to accompany a client to successfully deploy IPv6 in the network infrastructure.

Because of the complexity and philosophy of IPv6 it is highly recommended to already start with setting up a training program to technical staff. Make sure that the training is fit for the attending people, e.g., a Windows admin does not require IPv6 knowledge on OSPF. A properly set up program will make sure that IPv6 philosophy is already in the mind of people and that the complexity will not be underestimated when running into IPv6 in real-life. Another aspect is that non-technical staff should be made aware of IPv6. Think of increased complexity and management efforts, the migration process and corresponding timeline, IPv6 support in (new) hardware and software, procurement, etc.

The PoC "Introduction IPv6" gave us a peek only at the possibilities of IPv6 and its features.
This peek was enough to experience some very basic functions of IPv6, and gave us enough ideas about complexity and possible issues. However this was only the first phase of a complete project with many phases to reach the ultimate goal of having a datacenter and customer networks full IPv6 deployed.
Finally, do not underestimate the efforts to be taken to deploy IPv6. For a good understanding of the possible obstacles on the road, read the paper of some engineers of Google who are migrating their enterprise network towards IPv6 [1].

References

[1] H. Babiker, I. Nikolava, and K. K. Chittimaneni, "Deploying IPv6 in the Google enterprise network. Lessons learned" [Online]. Available: http://static.usenix.org/events/lisa11/tech/full_papers/Babiker.pdf

Marco van der Pal is a network Consultant with Capgemini in The Netherlands. He has over 15 years of networking experience. He is member of the datacenter network team, and as such responsible for a network stretching 3 datacenters. He is working on network architecture, design and implementations. Marco van der Pal started his career as a network engineer, primarily on the equipment of Cisco Systems, but also on 3Com, NBase, Juniper and HP Networking. He achieved CCIE certification on Routing & Switching in 2000, and is now CCIE Emeritus. Mr. Van der Pal has been working on IPv6 for 3 years.
E-mail: marco.vander.pal@capgemini.com
Generic Services – Network Infrastructure Services
Capgemini Netherlands B.V.
Utrecht, The Netherlands