IPv6 for Governments and Enterprises: Impact and Implementation in 12 Steps (part 2)

Author: Jordi Palet Martínez (@jordipalet)

In the first part of this article, we analyzed the impact of the deployment of IPv6 on corporate networks, which include governments, companies and organizations. This second part exposes in broad strokes and as a quick guide, the necessary steps to face the IPv6 deployment project.

1. **Experienced training**

   The IPv6 deployment project in any network is a big step towards the future and there we must not take risks. IPv6 is not the same as IPv4. It is inconceivable to properly plan the project, and obviously its subsequent execution, without having properly trained and not only in a theoretical or virtual way, but with “on-site” professionals, with experience in this type of networks, and with deep technical knowledge as well as in standardization, operation of networks, good practices and policies.

   The cost of this training is a small investment that will undoubtedly result in savings and the quality of the subsequent work, avoiding falling into errors that can be very expensive and may require repeating tasks. For example, if investments are made in new equipment, as part of the project, which later turn out to be inadequate, for having "thinking of IPv6 as if it were IPv4" and not having considered many very relevant changes.

2. **Development of the IPv6 deployment and testing project**

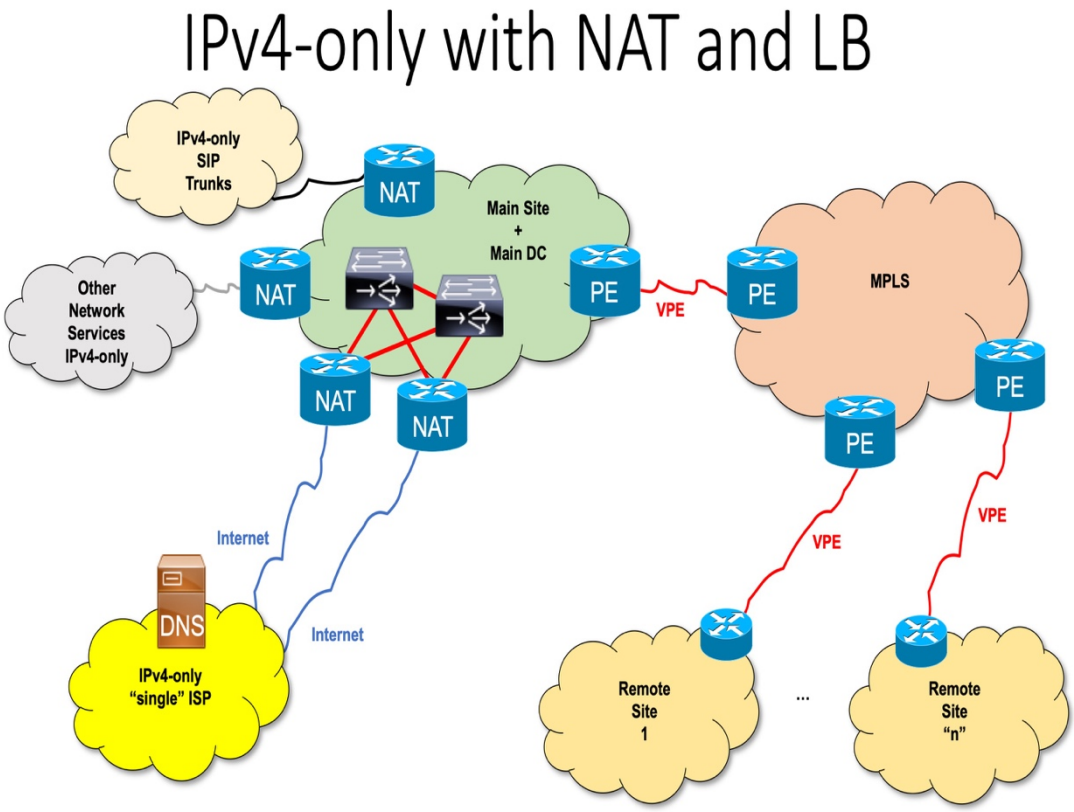
   Once the training is done, and only after that step, when we already have enough knowledge about IPv6, we can work on the IPv6 deployment project. This project should start with an audit of the current infrastructure and future changes planned, in all its aspects, from the client devices, operating systems, applications, network services, servers, security equipment and of course all the equipment which supports the network itself (switches, routers, wireless, etc.).

   The IPv6 deployment project must carefully study the organization of all its tasks, its interrelationships, bottlenecks and its solutions, and especially, how to confirm that with each step we take, we perform the necessary test to confirm that it works as expected and that it has not adversely affected the rest of the network, nor its internal or external users, whether they connect with IPv4-only, IPv6-only or dual-stack. It is essential to test from various Internet points, to confirm that our network is not only accessible from our immediate

environment, country or region, as we often see cases of networks that have not made these checks and do not have a correct global visibility.

Generally, this project will force a rethink of many aspects of the current design of the network. It will not be necessary to make changes in all the cases, this will depend on each network, but we must take advantage of the IPv6 deployment, as an opportunity, to ensure that the network and its applications and services comply with the requirements that IPv6 may require and the advantages that it can offer in future developments, such as IoT (Internet of Things).

The following steps in this guide should be an integral part of the IPv6 deployment project. We list them as additional steps, to highlight the importance that each of them has in the project.



Network pictured before the IPv6 deployment

3. DNS

One of the most important aspects for an adequate deployment of IPv6 is the control of authoritative DNS zones. The transition to IPv6 is based especially on the fact that the operating system and/or applications are able to choose properly if they must use IPv4 or IPv6. This implies an intensive use of DNS for the entire network, to which we are not always used to with IPv4.

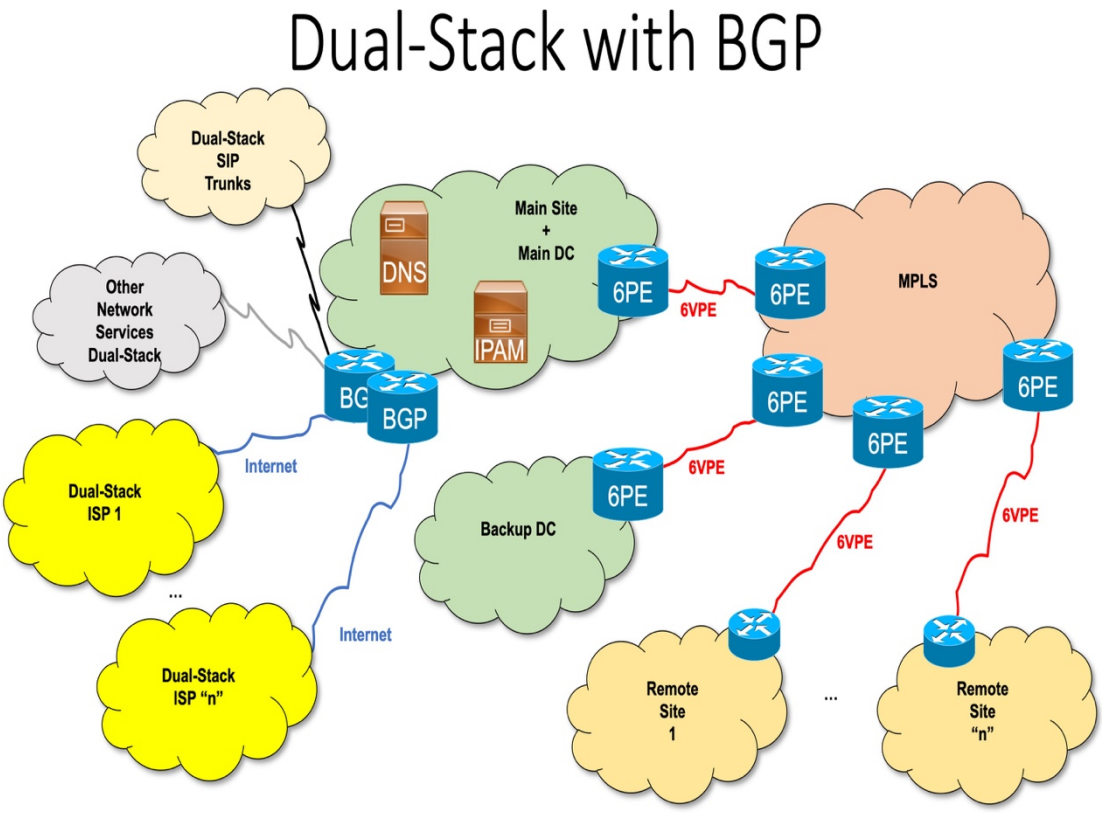
If we do not have control of the DNS, or depend on third parties to make changes, the deployment and testing is very complex, which can generate large and unnecessary delays and difficulties, throughout the project.

4. BGP

Many current corporate networks with IPv4 do not have BGP with their Internet providers and instead, they depend closely on NAT and even on other mechanisms or solutions, which are not recommended, as they have negative implications, which in the case of IPv4 can be hidden.

However, in the case of IPv6, there is no NAT or private addresses and, therefore, the use of BGP is not only a good practice, but it is essential if we want to have a provider independent addressing and thus avoid renumbering all our network when we change our provider, as usual, every "n" years, in the case of government entities contracts, or for competition reasons in other cases.

Imagine a Ministry with 5.000 officials, each with its own computer, in addition to the entire network infrastructure, and another 5.000 VoIP phones. Is it desirable or even acceptable to have to renumber all that infrastructure every four years? Can we imagine the economic cost and the impact on human resources and the “disconnection” time with citizens, to make this change? Do not underestimate the impact even when we talk about only 500 or 1,000 user devices.



Network pictured after the IPv6 deployment

5. **Addressing Plan Development**

In many cases, the existing IPv4 addressing plan may be a reference for IPv6, but the recommendation is that we start from scratch, because undoubtedly, over the years, IPv4 "patches" will have been made, and in addition It will most likely be based on private addresses that may even be duplicated in different parts of the network. IPv6 again, is an opportunity to do well, even to give us ideas to "fix" the "botched jobs" that we have been applying in the IPv4 addressing plan.

We can say that IPv6 has an almost unlimited address space, but you have to be meticulous and not waste addresses where it is not convenient. In many guides it is recommended to use "bits", to facilitate identification of networks/VLANs, services, geography or several of these aspects, however, we must be very careful with these recommendations, because if it is not studied carefully, each network case is very different, and often this leads to a waste of addresses because the "consumption" of bits in an absolutely ridiculous and unnecessary way.

6. **Obtaining Internet Resources (ASN, IPv4 and IPv6 Addresses)**

If we want to avoid the renumbering that we mentioned before, and be able to have our own addresses with BGP, we have to obtain from our RIR, an Autonomous System number (ASN), IPv4 and IPv6 addressing space.

In the case of IPv4, if the need is adequately justified, it is possible to obtain up to /22, that is 1.024 addresses. This will only be possible while IPv4 addresses remain in the corresponding RIR and whenever it is the first time they are requested, since the entities that had already received IPv4 from an RIR, according to the current policies, will not be able to receive more IPv4 resources. Alternatively, an IP broker could provide them.

In the case of IPv6, if it is an entity that only uses the address for its own network and not for third parties, it is qualified for a minimum of one /48 for each "site" of the network, such as end-user (PI, or Provider Independent). This allows addressing up to 65.536 sub-networks (/64) within each site.

If it is a larger network, which may need to sub-assign addresses to third parties, even to other institutions in the case of a government network, then it will qualify for a minimum of one /32 (allowing 65.536 sites, each with its own /48). Large networks of governments will often require shorter prefixes, for example, /25 or /26, which is possible, since several years ago, because the policies of all the RIRs have been adapted to allow this type of networks.

7. **IP Address Management (IPAM)**

It is common that in IPv4 we use a text document or spreadsheet, if not a notebook, for the addressing plan. The IPv6 address space, and the possibilities of network growth, make it prohibitive to use these mechanisms and force us

to adopt IP addressing management tools, called IPAM (IP Address Management), which can be OpenSource, commercial solutions, or even devices ("appliances").

Often these solutions allow to coordinate with DNS and even with DHCPv4 and DHCPv6.

8. Assignment and Audit of Addresses

One of the most important aspects when deploying IPv6, is to understand the differences between the different mechanisms of address assignment, such as autoconfiguration with SLAAC, DHCPv6, or the combination of both and even the use of multiple addresses in each interface. It is also necessary to understand what devices or operating systems can use one or the other and in what circumstances.

In those networks in which it is required to "audit" which device, or which user, is accessing certain applications or services of the network, which is usual in government networks or financial entities, among many others, these aspects have a special relevance and represent very significant changes with respect to IPv4, which can impact on applications, databases and network security mechanisms.

9. Network Infrastructure Devices and Clients

When auditing the equipment that constitutes the network itself, the servers, client's equipment, operating systems, etc., it tends to be simplified, thinking that it is enough for the manufacturer to indicate "supports IPv6".

This is a serious error, since there is no clear definition that it is "IPv6 support", since in the end, this depends exclusively on the context where said device or operating system will be used. That is, what RFCs must comply according to their location and functions in each specific point of the network.

It is about avoiding that we find equipment whose manufacturer indicates "supports IPv6", but when we perform the deployment, it does not support one or several RFCs that are fundamental for said equipment to meet the requirements that were expected of it, in a certain location or function in the network.

10. Impact on applications and services

This is undoubtedly the most complicated aspect of the deployment of IPv6. We can find applications that use literal addresses, applications that use old libraries without IPv6 support, applications that store 32-bit fields in databases, and an endless list of other problems.

All these applications could continue working when we deploy IPv6 coexisting with IPv4 (double-stack), but will not work when IPv4 is removed from the

network and, this will happen, rather sooner than later. While maintaining dual-stack in the network, those applications that depend on IPv4, for security or audit purposes, will not work correctly when users access them with IPv6. Likewise, many applications would be impacted when external users only have access to IPv6.

In short, this forces us to make a study of the applications to classify them and adopt appropriate solutions to each "group" of said classification.

11. A Long-Term Network: Transition Mechanisms

The deployment of IPv6 should not be considered exclusively depending on the coexistence with IPv4. While generally, at present (not in a few years), the logical step initially, is that both protocols coexist, the very near future is that the networks are IPv6-only.

This implies that the entire deployment project must contemplate both situations, and solve the problems that arise in both cases, with the aforementioned special affection of the applications, since some of them can't be modified (the manufacturer no longer exist, no access to the source code, the change is very expensive, etc.), and in some cases, adopt transition mechanisms that allow coexistence initially, and finally an "IPv6-only" network.

12. Contracts with Operators and Connections with Other Organizations

Often, and especially in large networks, we have several Internet providers, which generally do not collaborate with each other. It also happens that there are other different providers for voice, or other services. As we have indicated before, it was solved with NAT, in the case of IPv4.

With the deployment of IPv6, we will have to renegotiate those contracts, both data, voice and other services, so that they not only have IPv6 support (initially in double-stack mode, in the future they could be IPv6-only), with BGP. Only in cases of a single common provider for all services, we can avoid the use of BGP, although it is still convenient and good practice to have multiple paths with different providers, and to announce our own addressing space in our autonomous system.

Once we have taken all these steps into account, and only then, we can finish preparing the detailed IPv6 deployment project and then start its execution. Depending on the size of the network, it may take several months, even years, for the most complicated aspects, such as the analysis and adaptation of all applications.

It is important to keep in mind that there are many other aspects, besides those indicated in this guide. For example, it will be necessary to prepare a purchasing guide, so that future acquisitions and contracts fulfill the appropriate requirements in each case regarding IPv6 support, think about trainings for software developers (internal or external collaborators), prepare a roadmap to maximize the usage of the IPv6 deployment, etc. It is logical to assume that the network will have IoT (Internet of

Things) services in the future, and for example, in the case of government networks, think of SmartCities.

All these aspects, and many others, will undoubtedly give us a vision and dimensioning very different from that of our current network with IPv4, hence the importance of training and consulting with previous experience in government and corporate networks with IPv6, since this guide is only a starting point.