12 steps for IPv6 Deployment in Governments and Enterprises

ESNOG/GORE23

Mayo 2019

Madrid

@JordiPalet

(jordi.palet@theipv6company.com)

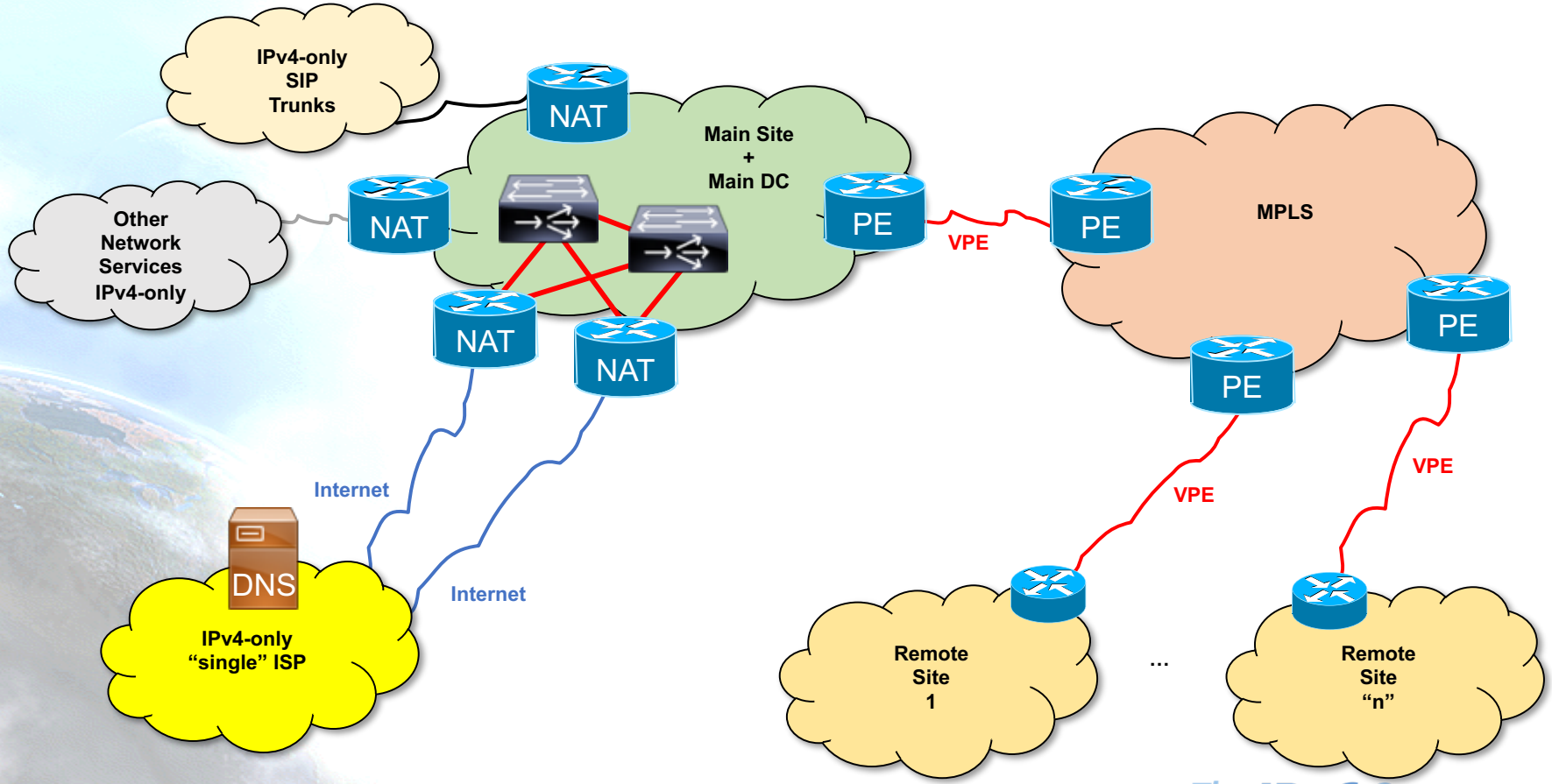
Difficulties and Further Reading

- Each network is a different “animal”
- Major problem: Lack of experienced trainers and engineers
  - IPv6 can’t be deployed like IPv4
  - Need to “unlearn IPv4 to learn IPv6”
- General recommendations can be established
  - Simplifying IPv6 Addressing of Customers
    - https://blog.apnic.net/2017/07/07/isps-simplifying-customer-ipv6-addressing-part-1/
    - https://blog.apnic.net/2017/07/10/isps-simplifying-customer-ipv6-addressing-part-2/
  - Twelve Steps to Enable IPv6 in an ISP Network
    - https://blog.apnic.net/2017/06/08/twelve-steps-enable-ipv6-isp-network/
  - IPv6 For Governments And Enterprises: Impact And Implementation In 12 Steps
    - https://blog.apnic.net/2018/11/22/ipv6-for-governments-and-enterprises-case-study/
    - https://blog.apnic.net/2018/11/23/twelve-steps-to-enable-ipv6-in-government-and-organizational-networks/

Actual IPv4 Deployments

- Common ”bad practices”
- Exaggerated NAT dependency for load balancing/sharing, instead of using BGP
  - Complexity when multihomed
- DNS CNAMEs with extremely low TTLs to make it work
  - Not taking advantage of DNS global caching, so slowing down everything
- Private addresses, instead of RIR “end-user”

IPv4-only with NAT and LB



How to Approach it with IPv6

- The recommendations provided are valid for:
  - Government networks
  - Enterprise/organization networks
  - ISPs that have no LIR/ISP addresses with IPv4
    - They were provided only by the upstream providers
  - There may be other similar cases where this approach make sense
- In the case of Government networks, it make sense to have a “nation-wide” network connecting all the institutions
  - Savings can be in the order of **hundreds of millions of dollars**
    - For just 2.000 municipalities, 300.000.000 USD
    - Expand it to thousands of schools, health-care, police stations, military, courts, etc.

1. Get Training

- IPv6 is not the same as IPv4
- Inconceivable to plan properly the project without experienced training
- Theoretical knowledge
- On-site hands-on
- Make sure the trainers have previous experience in this type of deployments
- It is inexpensive considering the savings if you get it wrong

2. Create a Deployment Strategy

- Audit the current infrastructure and future planned changes
  - Client devices, operating systems, applications, network services, security equipment, network equipment
- Look for bottlenecks and solution approaches
- Confirm that each step is tested and not affecting the rest of the network
  - Including internal and external users
  - Whether they are connected with:
    - IPv4-only
    - Dual-stack
    - IPv6-only
- Test from different Internet points, not just locally of from your country
- The project may force a rethink of the current network design
- Take advantage of the IPv6 deployment and future evolution (IoT, others)

3. Get Control of the DNS

- The transition is based on DNS
  - Operating Systems and apps need to be able to choose (IPv4 or IPv6)
- You need to have the control of your authoritative zones
- Intensive use of DNS for everything
  - Forget about addresses
- Not having the control delays deployment and testing
  - Increases difficulties

4. Consider Using BGP

- In IPv6 there is no NAT neither private addresses
  - ULAs are a bad idea
  - NPT is an experimental protocol

- The only practical approach is using BGP and Provider Independent addresses
  - Avoids renumbering if you change provider
    - Imagine a Ministry with 5.000 officials renumbering their devices and their VoIP phones every 4 years when a new contract is awarded
  - Allows multihoming, load balancing/sharing
  - Despite possible impact in global routing table

5. Develop an Addressing Plan

- Existing IPv4 addressing plan may be a reference
  - Even better if you start from scratch
    - So the “IPv4 patches” and usage of private IPv4 addresses get’s fixed

- IPv6 space looks unlimited, however make sure to avoid wasting where is not needed
  - Don’t be restrictive
  - But take care with generic guides that recommend using “bits” to facilitate identification of networks/VLANs, services, geography, etc.
    - Often leads to unnecessary waste

6. Obtain your own Internet Resources

- To avoid renumbering and be able to use BGP
- Get an ASN, IPv4 and IPv6 addressing space from your RIR (or NIR)
- IPv4 may not last too much, and depending on your region policies, you may be able to justify a maximum of /22 (1.024 addresses)
- IPv6, not an issue. If the network use addresses for its own infrastructure and not for third parties, it qualifies for a minimum of one /48 for each “site”, as “Provider Independent” (or End-User, depending on the policy terminology)
  - This allows up to 65.536 sub-networks (/64 each) per site
- For larger networks, which may need to sub-assign addresses to third parties, even other government institutions, they qualify for a minimum of a /32 (event easily can justify /25, /26, or whatever is needed)
  - Allowing 65.536 sites, each with its own /48

7. Use an IPAM

- In IPv4 is common to use a text document or spreadsheet to manage addresses
- The IPv6 addressing space requires adopting an IP Address Management (IPAM) tool
  - OpenSource, commercial, appliances, etc.
- Often IPAM allow coordination with the DNS, DHCPv4 and DHCPv6

8. Assign and Audit Addresses

- Make sure to understand the possible assignment choices
  - Autoconfiguration with SLAAC
  - DHCPv6
  - Combinations of both
- What devices/OSs need to connect to your network?
  - Not all them may support DHCPv6
- Do you require auditing which device gets “what” address(es)?
  - Does that impact in apps/network resources access control or login those addresses in databases?
    - It is often the case in government and enterprise networks
  - Does need to be related to some other network access control mechanisms?

9. Verify IPv6 Support

- Vendors confirming “IPv6 support” for network devices, client/server Oss, etc. is not enough

- There is not a clear definition of what it means “IPv6 support”, it depends exclusively on the context where every device or OS will be used
  - What specific list of RFCs need to comply with

- It is about avoiding that we find equipment that “support IPv6” but is not able to fulfill our needs in the planned network location

10. Test Impact on Apps/Services

- Probably one of the most complicated tasks
  - Apps that use literal addresses or old libraries without IPv6 support
  - Apps that store addresses in 32-bits fields or databases
  - Apps that allow input or displaying 32-bits decimal-only addresses
  - ... and many more developer mistakes

- All apps will continue working if we deploy dual-stack, but will not be able to respond to IPv6 or to log IPv6 addresses for security or audit purposes

- It is needed to study and classify apps, so to group them in solution approaches

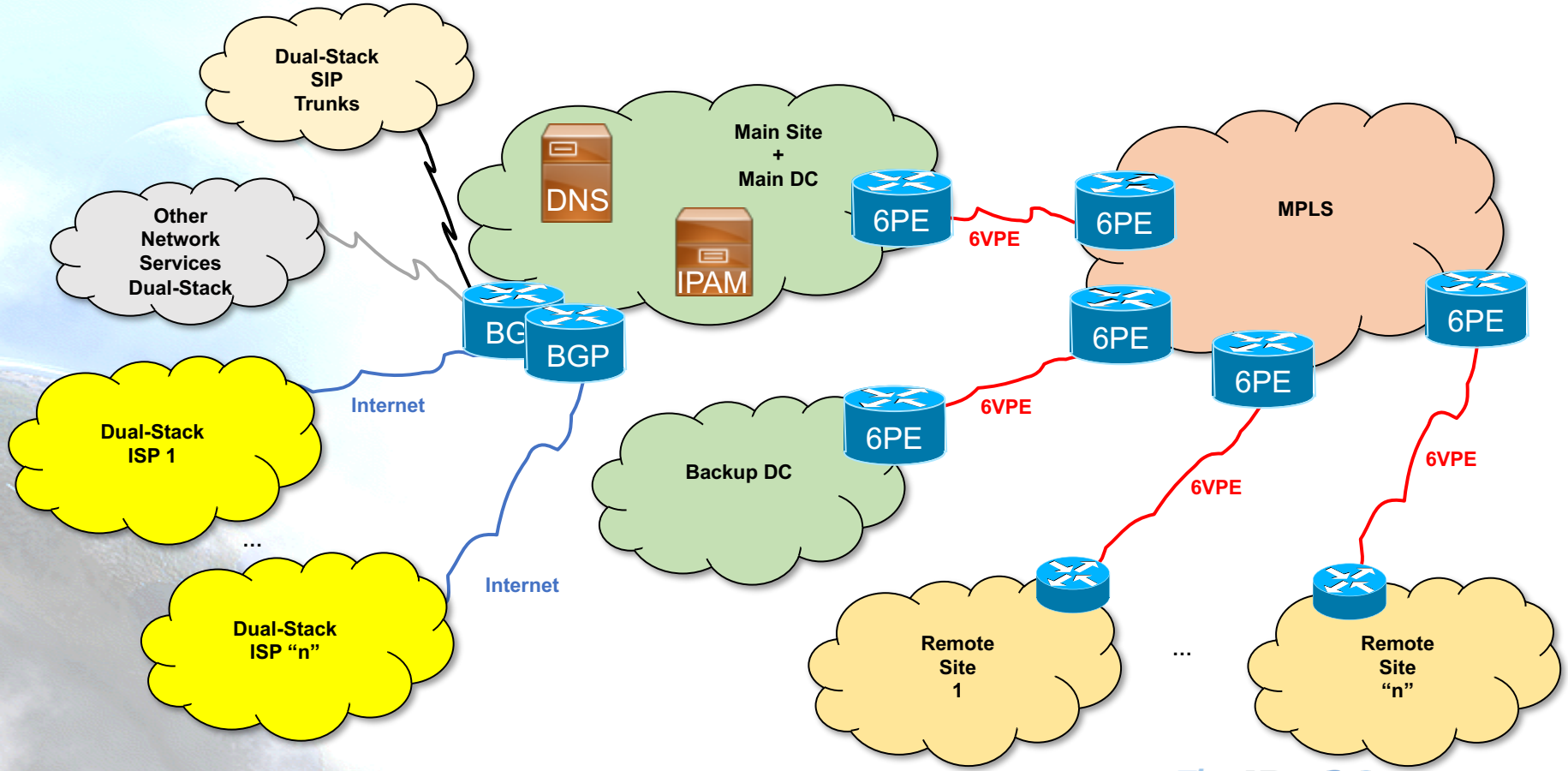
11. Create a Long-Term Network

- Do not invest in a dual-stack “only” project
  - This is just the initial step of the long-term IPv6 deployment strategy
- Your network will become IPv6-only, sooner or later
  - Plan it now for it
  - Avoid investing twice
- In some case, IPv4aaS transition mechanism may be an option
  - Non existing vendors or product no longer updated
  - Apps source not available

12. Check Contracts with 3rd parties

- Often, as bigger is a network, more contracts with service providers (data, voice, other services)
  - The are competitors, don't expect they cooperate
  - NAT was solving the problem for IPv4
- Renegotiate contracts, ask for BGP with dual-stack support and future IPv6-only
- Same with other third parties (business partners, customers, providers, …)

Dual-Stack with BGP



Good for Operators?

- Operators need to be ready for this
- It is a business opportunity
- More customers will need to have BGP
- Operators may provide the service
  - LIR account service management
  - BGP service management

Summary (1)

- Training FIRST
  - A transition plan requires an in-depth IPv6 knowledge, about the actual network and future evolution
- IPv6 is not the same as IPv4, can't be deployed in the same way
- Isn't only about changing the network configuration:
  - **IT REQUIRES REDESIGNING THE NETWORK**
- IPv6 requires rethink the network:
  - The IPv4 addressing plan (and create the IPv6 one)
  - Contracts with Service Providers (data, voice, others)
  - Become an AfriNIC member either as LIR/ISP for big government networks or as "end user" if is only a small entity
  - Requires BGP, DNS, IPAM
    - Affects the configuration of clients and devices
  - It requires a study of the intra-government connections
    - How small entities are going to deploy IPv6?

Summary (2)

- Scenario:
  - Transition to IPv6 as an intermediate step to “IPv6-only”
- Profound study of the network, **applications**, addressing plan, how addresses are assigned and managed, security, auditory, etc.
- APNIC membership
  - Request also ASN and IPv4 (while it lasts!)
- Deployment and testing plan
- Verify your deployment, step by step, from different Internet locations, not just locally

Thanks!

Contact:

@JordiPalet
jordi.palet@theipv6company.com