Addressing the Administrative Challenges of IPv6 Deployment in Public Administrations

Dr. David Holder (Erion Ltd)
Mark McFadden

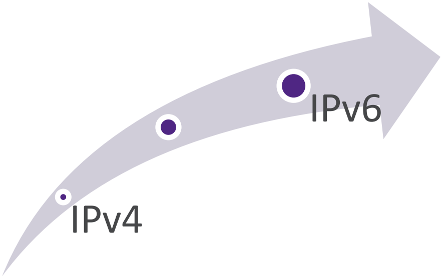
IPv6 Framework for European Governments – SMART 2016/0099
Workshop – Instituto Superior Técnico – Lisbon, Portugal
21st September 2018

Addressing the Administrative Challenges of IPv6 Deployment

- Setting goals for IPv6 deployment
- Justifying the IPv6 deployment
- Planning the IPv6 deployment
- The role of leadership in IPv6 deployment
- Incorporating IPv6 deployment into strategic ICT planning
- Case studies in successful IPv6 deployment

Setting Long-Term Goals for IPv6 Deployment

- Understanding the true goal of IPv6 deployment is crucial to success
- The long-term goal should be an **IPv6-only network**
  - The long-term goal should be to eliminate IPv4 from your networks
  - Failure to understand this can be detrimental to the deployment of IPv6
  - Maximum benefits from IPv6 are achieved when IPv4 is eliminated
- Other long-term goals risk being “IPv4 centric”:
  - Design can be compromised by IPv4 thinking
  - IPv4 may be seen as the primary protocol leading to treating IPv6 as a secondary protocol or “add-on”. This will compromise the deployment
- Seek a minimum of parity between IPv4 and IPv6 **but** prefer IPv6 when possible



What is an IPv6-Only Network?

IPv6-only

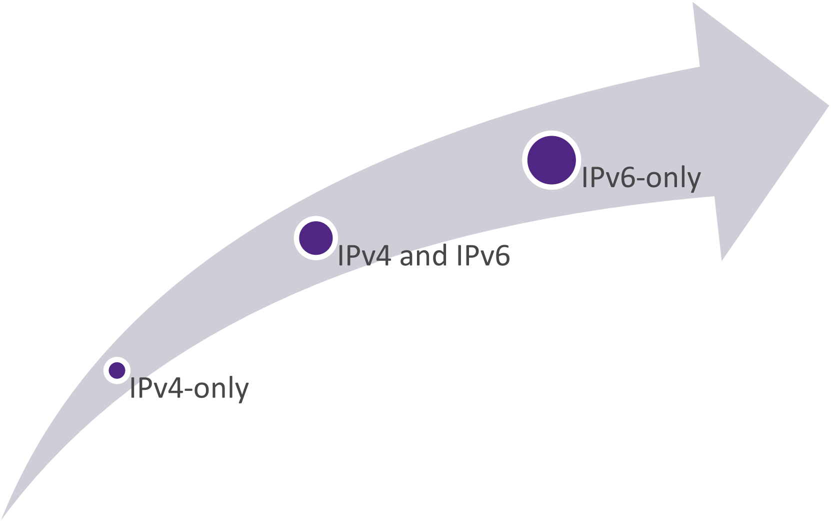
- An IPv6-only network:
  - Has IPv6 as its network layer protocol
  - Does not support *native* IPv4
  - Does not have any *internal* IPv4 connectivity

- Accessing legacy IPv4-only services and content from an IPv6-only network:
  - Usually through some form of translation or encapsulation, e.g.
    - NAT64/DNS64
    - 464XLAT
    - MAP-E or MAP-T
    - DS-Lite
    - There are others

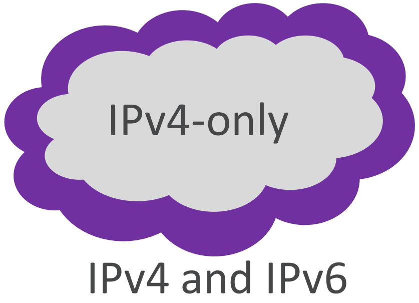
Setting Intermediate Goals for IPv6 Deployment

- It is important to understand that there will be intermediate goals on the path to IPv6-only
    - It is often not practical to deploy IPv6-only immediately
    - A normal deployment will require at least one intermediate step to IPv6-only
    - The most common intermediate step is dual-stack

- Common intermediate goals are:
    - Deploy IPv6 at the edge
        - On public facing services
        - On access and transit at the edge
    - Deploy dual-stack
        - Adding IPv6 to existing networks



What is Deploying IPv6 at the Edge?



- On public facing services
  - Often much easier than organisations expect
  - Public services can be IPv6-enabled in two main ways:
    - Natively by converting the service to dual-stack operation
    - Through translation of an IPv4-only service to IPv6
      - Many Content Distribution Networks (CDNs) provide this service as standard (sometimes by default)
      - Load-balancers often include translation to IPv6 enable IPv4-only services
      - Fast and easy solution to “IPv6-enable” IPv6-only services
      - Usually trivial to enable for testing and then move to production – very limited risk to existing services
- On access and transit at the edge
  - Providing IPv6 at the edge of a network is a key step in providing IPv6 services

What is Dual-Stack?

- Dual-stack is the default and most common method of deploying IPv6 today
- Dual-stack networks support both native IPv4 and native IPv6
- Dual-stack nodes can communicate using both native IPv4 and native IPv6
- Essentially dual-stack networks are bilingual
- Dual-stack is the most flexible deployment approach
- Dual-stack is relatively easy to deploy
- There are disadvantages to dual-stack:
  - Networks are more complex – two protocols with complex interactions
  - Increased administrative overhead – two protocols to manage
  - Greater node and network resources are required to support both protocols
  - Additional complexities in routing
  - Greater security challenges (both IPv4 and IPv6 vulnerabilities with complex interactions between the two)

Dual Stack is the Default

- Dual stack is the norm:
  - All modern operating systems are dual stack
  - Most network equipment is dual stack
  - Most network services are dual stack
  - Many network applications are dual stack
- Dual stack is usually on by default
  - This is an aspect of IPv6 deployment that is largely already done for you

The Wrong Goal for IPv6 Deployment

The **goal** isn’t adding IPv6 to an IPv4 network

However, this is a legitimate tactic

Subsidiary Goals for Public Administrations

- In addition to the IPv6 specific goals, public administrations are likely to have many interrelated goals that interface with IPv6 deployment
- These will vary from administration to administration and even from department to department
  - Goals to support technology
  - Goals to support growth
  - Goals to support education
  - Goals to support strategic objectives

Justifying IPv6 Deployment

- Does IPv6 deployment require justification?
  - Is its deployment an integral part of normal network development?
  - For example, IPv6 is already active in *all* modern operating systems
  - Don’t necessarily seek justification for something you are going to do anyway
- Be clear about what you are seeking justification for
  - A single coordinated project ***is*** best practice
  - However a single all-encompassing project can send the wrong message:
    - IPv6 may be seen as a bigger step than it needs to be
    - IPv6 may not be seen as the natural evolution that it is
    - Presenting IPv6 as a single all-encompassing deployment project can sometimes be a help and sometimes it can be a hindrance
  - Different justifications for different areas of deployments
    - E.g. public vs. internal deployments

Generic Justifications for IPv6 Deployment

- Deterioration of the legacy IPv4 internet
  - Impact of Carrier Grade NAT (CGN) (and NAT44)
  - Impact of routing fragmentation
  - Impact of address squatting
- Exhaustion of your stock of public IPv4 addresses
- Exhaustion of your internal RFC1918 private address space
- Support for deploying the Internet of Things (IoT)
- Restrictions in certain marketplaces (e.g. Apple App Store)
- Peer-to-peer requirements
- Cybersecurity, legal intercept and analytics
- IPv6 is the current standard for the Internet Protocol
- IPv6 forms the basis for key technologies (e.g. mobile – 4G/5G)

Justifying IPv6 Deployment in Public Administrations

- Public institutions rely on the Internet just as much as others
  - And, are affected by trends in the general Internet just as much as others
  - The generic reasons for deploying IPv6 apply equally to public administrations
- The Internet, as a platform for growth and innovation, requires IPv6
  - IPv6 necessary for Internet economy growth
    - The alternatives entail unacceptable risks
    - Limitations on scalability (dense NAT without IPv6)
    - Hurried/unstable IPv6 deployment (wait and rush)
    - Need to promote interoperability where possible
    - As IPv6 becomes norm, IPv6 expertise key for economic competitivity
  - The "end" of IPv4 also brings competition concerns and regulatory issues
    - Governments need expertise, they need to be prepared

Why Doesn’t Anyone Have to Justify IPv4?

- Explicitly justifying the use of legacy IPv4 is extremely unusual – it is assumed
- You should seek parity for IPv6
- It is reasonable to ask – “why are we deploying this over legacy IPv4?”

Justification and Obtaining Buy-In

- For an IPv6 deployment to be successful there needs to be executive, management and ministerial support
- Some aspects of an IPv6 deployment work best if they are centralised, providing common standards and goals, therefore central support and buy-in is crucial

- The departmental and regional structure of a public administration will influence where buy-in needs to be obtained
- There are differences in federal and non-federal administrations

Engage Key Suppliers in the Justification Process

- There are suppliers who are keen to support IPv6 adoption
- Enlist these in your justification process
- For example, in some regions the lack of IPv4 address space is hurting specific industries, these will be keen to support your initiative
- Service providers (fixed line and mobile) can play an important role depending on their stance on IPv6

IPv6 Task Force or Stakeholder Group

- These can be an effective way of coordinating support for IPv6 deployment
- They can bring together government and industry players
- They can create awareness, generate support and assist with the case for IPv6
- They can also bring together key players that are necessary for success such as service providers
- Some public administrations have created IPv6 Task Forces
- Others have provided support for IPv6 Task Forces
- It has been noted that even a single meeting can have a significant affect

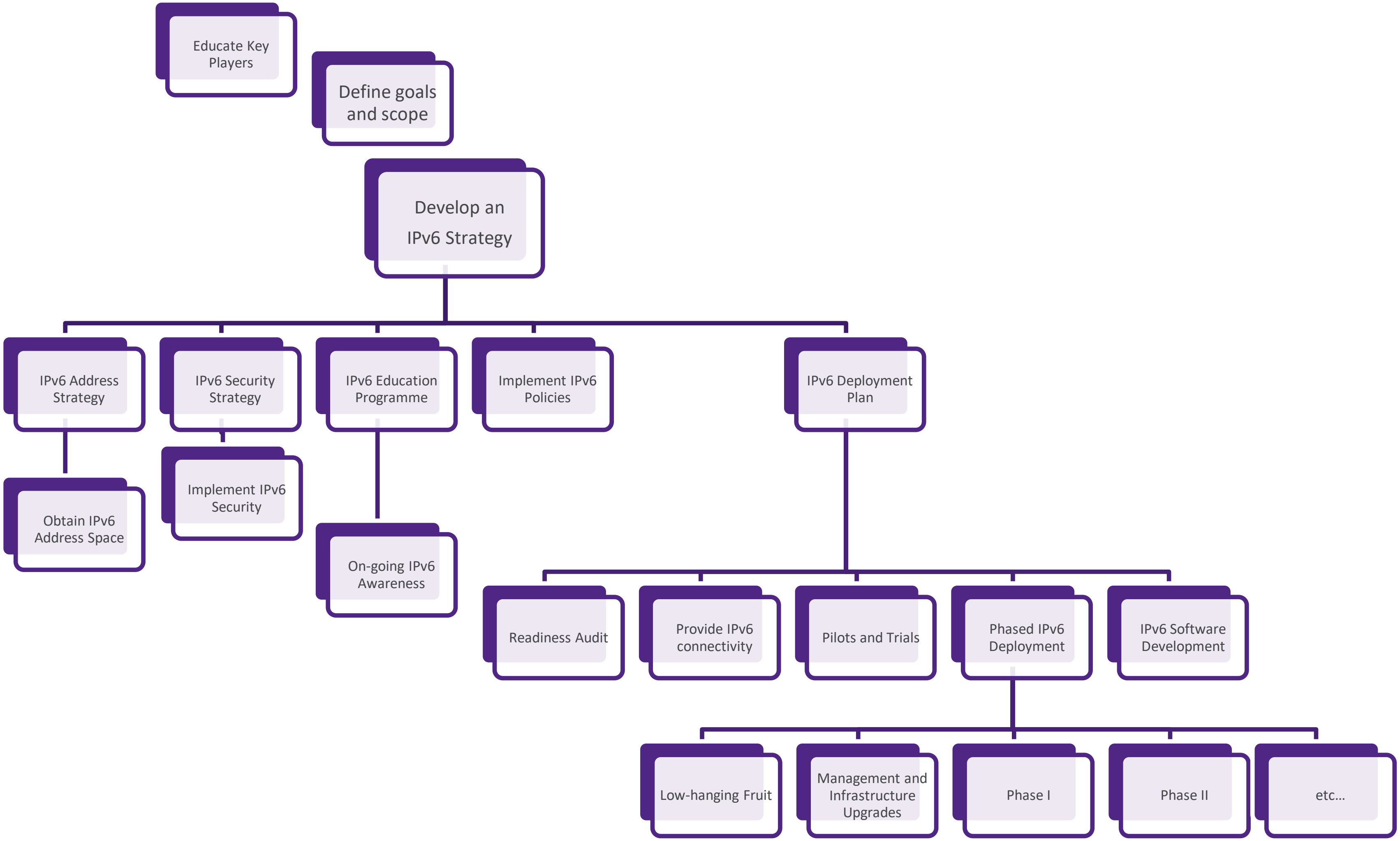
Planning the IPv6 deployment – Key Activities

- Key IPv6 deployment project planning activities:
  - Define the project **goals** and **scope**
  - Plan an **IPv6 Awareness and Education Programme**
  - Define an **IPv6 Deployment Strategy**
  - Create an **IPv6 Address Strategy**
  - Develop an **IPv6 Security Strategy**
  - Plan the phases **IPv6 Deployment**
- These activities are interrelated and are often carried out in parallel
- As a part of these you will also need to:
  - Obtain **IPv6 Address Space**
  - Initiate an **IPv6 Awareness and Education Programme**
  - Carry out a **Readiness Audit** and/or **Pilots/Trials**

Establishing Goals and Scope

- Goals
  - Long-term goal should be IPv6-only
  - There will be intermediate goals such as IPv6 at the edge and dual stack
  - There are likely to be administration specific strategic goals that are IPv6 related
- Scope
  - IPv6 deployment can touch almost every part of a public administration
    - Not just technology
    - The overall project should recognise this
    - However, the deployment project does not have to be all encompassing in scope – balance between setting right goals and policies and implementation
  - Applications, Information, Computing Platforms, Networking, Infrastructure Services, Processes, Standards, Security, Governance, Buildings, Sites, Transport, Communications, Media, Human Resources…

Example IPv6 Deployment Programme



Planning an IPv6 Deployment - Timescales

- Deploying IPv6 is not just a project it is also a process
- Patience is required – IPv6 deployment is usually a long process
  - IPv4 is likely to be around for the foreseeable future
  - Even if you move to IPv6-only networks you will still have IPv4 at the edge
- Certain aspects of deployment require hard deadlines
  - Particularly activities that the rest of the project depend upon, e.g.
    - Creating an IPv6 strategy and implementing IPv6 policies
    - Carrying out an IPv6 training/education/awareness programme
    - Creating an IPv6 addressing plan
    - Obtaining IPv6 address space
    - Provisioning IPv6 internet connectivity
- Others may be on-going processes driven by other activities

Planning the IPv6 deployment – Key Players

- First recognise the need for a change of **mindset**
  - It is normal to underestimate the difference in design and operational best practice between IPv4 and IPv6 – beware of this
- Second ensure that **key players** have a **good** understanding of IPv6
  - **All** reported IPv6 deployments have testified to the importance of IPv6 education – do not underestimate this
  - Make sure planners, designers and architects are educated in IPv6

Planning – IPv6 Awareness and Education

- We will discuss this in more detail in a later session
- IPv6 is different from IPv4 in complex and subtle ways
  - Understanding this, in detail, is key to having a successful IPv6 deployment
  - Successful IPv6 deployments all attest to the necessity of IPv6 training

- Education should take place as early as possible in the process
- Identify and train key players before making key design decisions
- All technical staff will need at least a basic introduction to IPv6

Planning – IPv6 Deployment Strategy I

- Aims and goals
- Overview of deployment options
- Readiness assessment report
  - Summary of findings
  - Review of constraints and requirements
  - Document implications

  - Continued…

Planning – IPv6 Deployment Strategy II

- Guidance on optional deployment
  - How to leverage benefits of IPv6
  - Recommendations of best practice
  - Choice of deployment approaches
  - Catalogue of known risks and potential pitfalls
  - Recommendations on training and communications
  - Prerequisites prior to deployment
  - Configuration recommendations for hardware, software and services
  - How to preserve IPv4 addresses and connectivity during deployment

  - Continued…

Planning – IPv6 Deployment Strategy III

- High-level deployment plan
  - Outline scheduling and priorities
  - Preparation (e.g. policy, training, security, addressing, infrastructure upgrades)
  - External phased deployment
  - Internal phased deployment
  - Set time-line and deadlines

Planning – IPv6 Address Strategy

- An **IPv6 address strategy** is **crucial** to the success of an IPv6 deployment
- You want to get this right – it is important to avoid ever having to renumber
  - Overview of IPv6 addressing
  - Schema design considerations
    - Summary of best practice and local constraints
  - The IPv6 address schema
    - Prefix type, length and source
    - Prefix subnetting structure
    - Types and structures of Interface Identifiers (IIDs)
  - Address allocation and assignment policy
    - Procedures and policies to ensure the efficient and consistent allocation of addresses
    - Specify how addresses will be managed and the tools that will be used

Planning – IPv6 Security Strategy

- You should **already** be securing IPv6 in your network
  - IPv6 security should already be a standard component of your IT security
  - All today’s networks are dual-stack **by default**
  - You have IPv6 vulnerabilities in your networks now
  - There is no such thing as an IPv4-only network anymore
- Develop and implement an IPv6 security strategy **as soon as possible**
  - Overview of IPv6 security
  - Summary of best practice and local security design considerations
  - IPv6 security strategy
    - Procedures and policies defining which security techniques will be implemented, how they will be implemented and where they will be implemented
  - High-level IPv6 security deployment plan

Planning – IPv6 Deployment Approaches

- IPv6 has been designed to make it deployable in a wide range of flexible ways
- There are three main categories of deployment approaches
  - IPv6 deployment flexibility means that they can be used separately or in parallel

- Inside-out
  - Deploy in core network infrastructure then enable networks and applications
- Outside-In
  - Enable IPv6 at the network edge and enabling inwards
- IPv6 Islands
  - Enabling islands of IPv6 in specific areas and gradually expanding them

Planning – Connectivity and Transit

- Native IPv6 transit is a key prerequisite for an IPv6 deployment
- Whilst IPv6 can be deployed without native IPv6 connectivity this does not provide the necessary scalability, manageability, reliability and performance necessary for a government or enterprise deployment
- Most transit providers are IPv6 enabled
- You will need native IPv6 connectivity from your service providers
  - Beware of immaturity or inexperience within your service providers
  - Beware of second-class IPv6 services from some service providers

Planning – Readiness Audit/Gap Analysis

- Readiness audit/s
  - You need to estimate the gap between what you have and what you need
  - You need to identify potential problem areas
  - Some organisations carry out a comprehensive audit others only look at specific areas of interest
  - You need to specify what you are going to audit and what you are looking for
  - Gap analysis should cover:
    - IPv6 support and functionality in network infrastructure, nodes, services, security, applications and management systems
    - Resources to support the addition of IPv6 (e.g. memory)
    - Management tools
    - Expertise (see education/training)
  - A number of public profiles exist for IPv6 (see next slide):

Planning – Readiness Audit – IPv6 Profiles

- A number of public profiles exist for IPv6:
  - Requirements for IPv6 in ICT Equipment (RIPE-554)
  - IPv6 Ready Logo Program of the IPv6 Forum
  - A Profile for IPv6 in the US Government (V1, NIST, 2008)
  - Department of Defense Unified Capabilities Requirements 2013 (UCR 2013)
  - IPv6 Node Requirements (RFC6434)
  - IPv6 Profile (www.bmi.bund.de)

Planning –Pilots/Trials

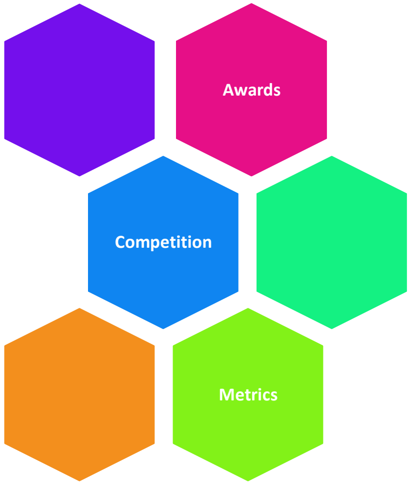
- Pilots and Trials
  - Testing is important
  - IPv6 pilots are beneficial to ensure IPv6 works in your particular environment and with the products and services that you use
  - It is also useful for staff to gain additional experience of IPv6
  - For example, it is useful to deploy IPv6 in one office before rolling out to all other offices

The Role of Leadership in IPv6 Deployment

- Leadership has been identified as a **significant factor** in the success of IPv6 deployment in public administrations
- Encourage the appointment of leadership that:
  - Is highly motivated
  - Understands that IP infrastructure underpins strategic objectives
  - Is an advocate/leader for IPv6
  - Is a single point of contact for IPv6 across all departments/ministries
  - Has a consistent message
  - Avoids competing initiatives and nurtures cooperation
  - Seek to encourage the formation/growth of a national IPv6 group such as an IPv6 Task Force or an IPv6 Council

Motivating IPv6 Deployment

- Many schemes have been suggested and tried for motivating IPv6 deployment
- By far the most effective has been the use of mandates with hard deadlines
  - MS have commented that mandates “without teeth” are not effective
- Other motivational schemes that have been use include:
  - Awarding success with **certifications** and official **awards**
  - Encouraging **competition** between departments/ministries
  - **Measuring** deployment progress on a publicly available web-site

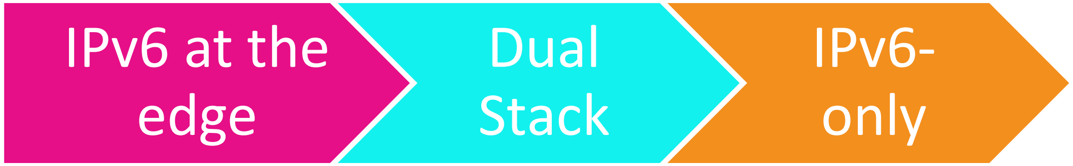


Incorporating IPv6 Deployment into Strategic Planning

- You should have **three** strategic goals:
  - **Long-Term Strategy:** IPv6-only
  - **Medium-Term Strategy:** Dual stack
  - **Short-Term Strategy:** IPv6 at the edge

- Implicit in these goals are the aims:
  - To reduce your dependency on legacy IPv4 infrastructure and services
  - To future-proof your networks

- How should these goals be incorporated into strategic planning?



IPv6 at the edge

Dual Stack

IPv6-only

Strategic Planning - Purchasing

- You should **mandate** that all IP capable purchases must be IPv6-ready and capable of IPv6-only operation
  - It is wasteful to purchase legacy systems that do not support IPv6
  - This mandate should cover all IP capable hardware and software
  - This means **everything** that is networked (lights, freezers, cameras, transport, cloud services, applications)
  - Ideally this policy should already have been in force for at least ten years
  - Educating purchasing departments in what is “IPv6-ready” and what is “networked” can be challenging
  - Explicitly tell your suppliers as soon as possible

- Specifications of what is “IPv6-ready” can be useful, but they are less necessary today as core IPv6 features are normal. You are more likely to cherry-pick specific IPv6 requirements for specific scenarios e.g. security features in a datacentre.

Purchasing and the Meaning of “IPv6-Ready”

- Historically there was a need to carefully define the meaning of “IPv6-Ready”
  - The immaturity of IPv6 implementations meant that you had to validate that core features were implemented in a product or service
  - Evolving IPv6 standards meant that newer features or defaults might not be implemented or enabled in products or services
- Today this is less of a problem
  - The majority of IPv6 enterprise products are mature
  - Whilst all standards continue to evolve, the IPv6 core standards are “stable”
- There are still exceptions
  - Rather than checking adherence to all of the standards, specify the exceptions
    - Recent standards and defaults
    - Specific specialise features (e.g. security features)

Purchasing and Wording the Policy

- Use an abstract purchasing policy and wording in tenders
  - Specify that IPv6 support must be at least equivalent to IPv4
  - Avoid details – these change
  - Only specify special requirements and exceptions
  - Push the problem onto the vendor, leave it to them to guarantee that they meet your requirements
    - Specify penalties/actions if they fail to deliver
    - Remember you are only purchasing from vendors who claim to support IPv6, you should take them at their word and they should be willing to back this up
    - Make it clear that it is their responsibility

Educating Purchasing Departments

- This remains a challenge
- Purchasing may not understand that a product is network enabled, never mind that it has IPv4 or IPv6
- Educating purchasing departments remains a “best-effort” exercise
  - Make sure that they are aware of the IPv6-ready purchasing mandate
  - Help them understand what might be networked
  - Emphasise the importance of compatibility and interoperability
- There still remains the problem of “stealth” purchases
  - There are a huge range of often unusual products that are networked
  - Some may be purchased outside of normal channels that lack checks for IPv6
  - Some organisations that have tried to raise the awareness of IPv6 through poster campaigns etc – the effectiveness of this with a generic audience is unknown

Strategic Planning – Software Development

- You should **mandate** that all IP capable software development must be IPv6-ready **and** capable of operating in IPv6-only networks
  - It is **wasteful** to continue to develop systems that do not support IPv6
  - You will only have to rewrite them in the future which is likely to be more costly than getting it right at the start
  - Ideally this policy should already have been in force for at least ten years
  - You will need to educate software developers on how to write IPv6-ready code
    - Warning: there are multiple ways of “IPv6 enabling” applications. Giving software developers a choice is a bad idea – set standards
    - Warning: there is a lot of incorrect advice on well-known web-sites – set standards
  - Note that you will still need to IPv6-enable legacy applications (including bespoke tools and management systems)
    - However, in a dual-stack environment IPv4-only S/W will continue to work

Strategic Planning – Hiring

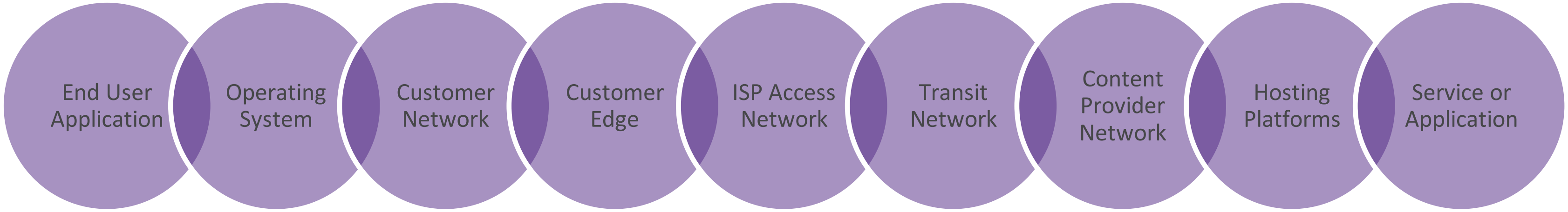
- You should **mandate** now that all ICT job descriptions that include a knowledge of networking and particularly IP specifically require IPv6
  - It is wasteful to continue to hire staff that only know legacy IPv4
  - Look for evidence of formal training and experience with IPv6
  - If the post is focussed on networking then they should be able to demonstrate a good knowledge of IPv6
  - IPv6 skills are in short supply – this is a problem
    - Upskilling your existing staff is going to be essential

Case Studies in Successful IPv6 Deployment

- Public administration case study
  - Germany
- Commercial case study
  - Facebook

IPv6 Context of Case Studies

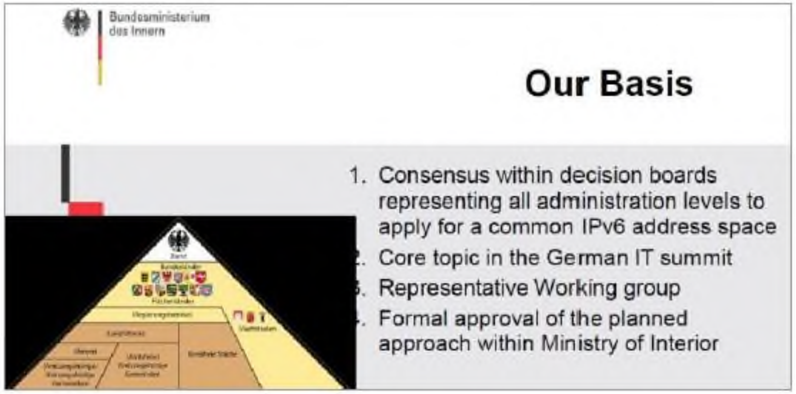
- Dual stack users: **50% to 85% of traffic** is over IPv6 today
- Over **20% of users** globally have IPv6 connectivity
  - Google statistic – Google does not operate in China affecting the figures there
- Annual **doubling** of IPv6 enabled users
- Over **50%** of *top* web-sites are IPv6 enabled
- IPv6 has been reported by Facebook to be **10-15% faster** than IPv4
- Almost **100%** of nodes are IPv6 capable
- Major players are IPv6 enabled: Facebook, LinkedIn, Google, YouTube, Netflix
- Many mobile networks are IPv6 enabled (or IPv6-only) – 4G (some report that over **90%** of traffic is IPv6)



IPv6 Case Study: Germany

General IPv6 development :
33.8% (Google) - 27.6% (Akamai)
Public IPv6 development : 25.6%

- History
  - Decision to adopt IPv6 was made in the public sector in 2007
  - National IPv6 plan for Germany launched in 2009
- Key Stakeholders
  - The migration process is driven by:
    - Federal Ministry of the Interior (BMI)
    - Federal Office of Administration (BVA)
  - These coordinate the IPv6 working group
- Drivers to Adopt IPv6
  - Exhaustion of IPv4 address space
  - Opportunity to replace legacy networks to create an integrated, efficient and highly secure communications infrastructure for all areas of government



Bundesministerium
des Innern

Our Basis

1. Consensus within decision boards representing all administration levels to apply for a common IPv6 address space
2. Core topic in the German IT summit
3. Representative Working group
4. Formal approval of the planned approach within Ministry of Interior

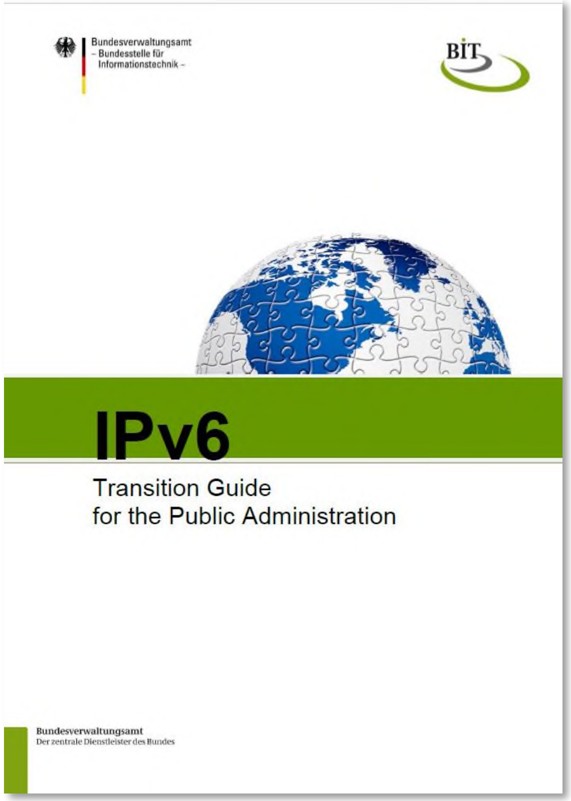
Source: BMI

IPv6 Case Study: Germany - Planning

- Project Scope
  - IPv6 deployment scope is public only
- Features
  - The BMI is not forcing public administrations to adopt IPv6 but is facilitating and encouraging the move to IPv6
- Key Initiatives
  - Procurement policies
  - IPv6 address space plan
  - IPv6 address space prefix
  - Migration documentation and reference documents
  - Training materials (in German and specific to Germany’s deployment)
  - Several deployments

IPv6 Case Study: Germany – Migration Plan

- Germany has created an IPv6 Migration Plan (Germany/English)
  - Dated 2013
  - Contains a lot of useful information:
    - Motivation for public administrations
    - Overview of transition to IPv6
    - Addressing concepts
    - Transition techniques
    - Security
    - Transition of Infrastructure
    - Transition scenarios
    - IPv6 special considerations
    - Checklists



Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

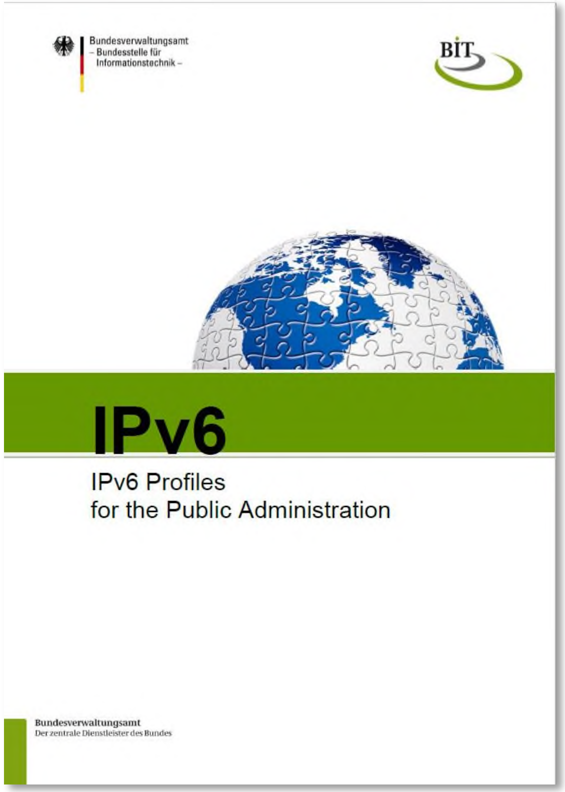
IPv6

Transition Guide
for the Public Administration

Bundesverwaltungsamt
Der zentrale Dienstleister des Bundes

IPv6 Case Study: Germany - Procurement

- Germany has developed IPv6 profiles (German and English) to facilitate the procurement of IPv6-ready equipment and software
  - Dated 2013
  - These are based on the Slovenia profiles
  - Overview of existing profiles
  - Hardware
  - Software
  - There is also a profile spreadsheet



Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

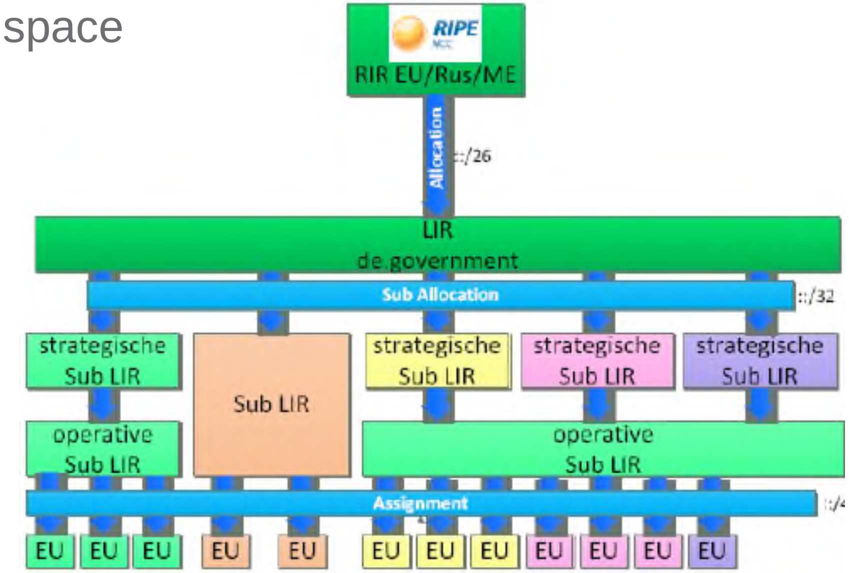
IPv6

IPv6 Profiles
for the Public Administration

Bundesverwaltungsamt
Der zentrale Dienstleister des Bundes

IPv6 Case Study: Germany - Addressing

- Germany is a federal government
- The federal government is a Local Internet Registry (LIR)
- Along with other RIPE members the federal government sought changes to RIPE policy to make it match the needs of governments and not just ISPs
- A /23 prefix has been obtained for government
- An IPv6 address plan for Germany has been created
    - Clear definition of government address space
    - Efficient routing
    - Route aggregation
    - Direct inter-ministry communication



Source: BMI

IPv6 Case Study: Germany - Deployments

- A number of IPv6 deployments have taken place within Germany
- **Example**
  - GEN6 pilot IPv6 enabling municipal datacentres and infrastructure

    See http://ipv6gov.eu/wp-content/uploads/2018/05/Workshop-1-05-DE-Case-Study-Gerold-Gruber.pdf

  - Key points:
    - The importance of management awareness and support
    - IPv6 training for all staff is crucial
    - Get IPv6 addresses and create a local schema/plan
    - Carry out preparations – testbeds – operational preparation – etc
    - Enable IPv6 in the access networks
    - Enable infrastructure and infrastructure services
    - Enable applications and security

IPv6 Case Study: Facebook

- History
  - Began with limited deployment in 2010
  - Today internal networks are IPv6-only
- Key Stakeholders
  - Enterprise commitment to IPv6 at all levels
- Drivers to Adopt IPv6
  - Exhaustion of public IPv4 address space
  - Exhaustion of internal IPv4 address space
  - Concern about the impact of the deterioration of IPv4 would have upon the service they provider to customers (particularly CGN)
  - Saves money on the need for internal CGN devices
  - Particularly important for the mobile market (majority of LTE traffic is v6)

IPv6 Case Study: Facebook - Deployment

- Project Scope
  - Everything must be IPv6-only capable - all Facebook apps must support IPv6
  - Management and operations is over IPv6
- Features
  - Migration was phased – now have IPv6-only fabric
  - Dual stack was a problem – exceeded 1000 BGP sessions limit
  - Now moving to a /64 per server rather than /64 per rack
  - Have reported 10-15% faster response for IPv6 users on mobile networks
- Key Initiatives
  - Migrated all tooling and management to IPv6 ***first***
  - IPv6-only is largely complete
  - Now working on eradicating legacy IPv4-only equipment

Questions