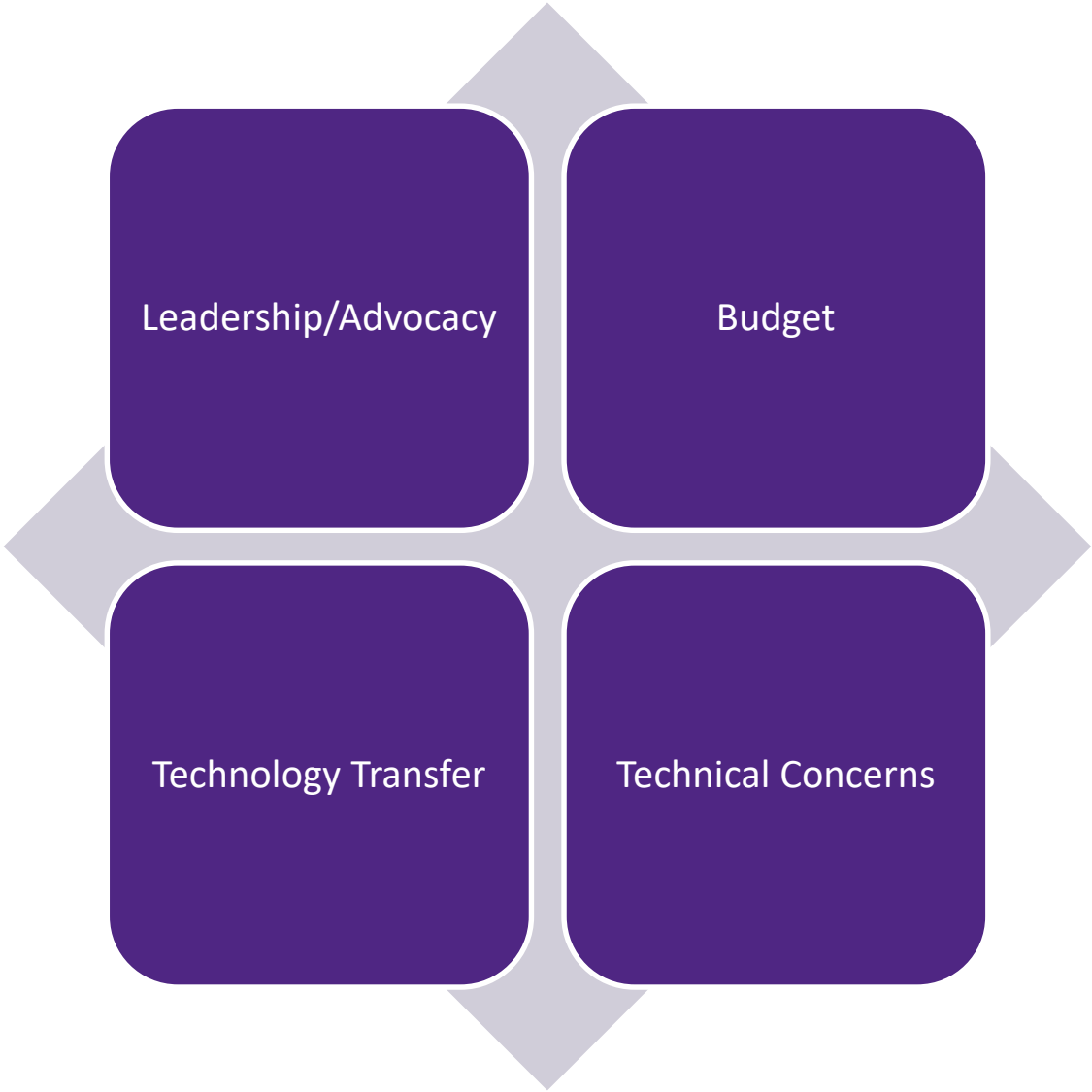
Addressing the Barriers to IPv6 Adoption – Addressing the Barriers to IPv6 Deployment

Mark McFadden
Dr. David Holder (Erion Ltd)
IPv6 Framework for European Governments – SMART 2016/0099
Workshop – Brussels, Belgium
11th October 2018

Categorizing Barriers to IPv6 Adoption



Addressing the Barriers

- Theme One: Administrative Barriers

Lisbon Technology Transfer Workshop

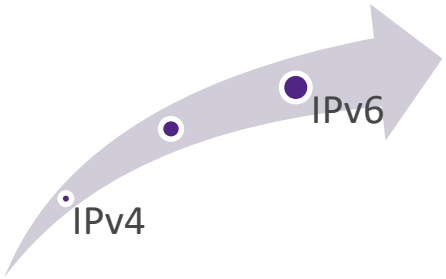
- Discussed how to surmount the barriers to IPv6 deployment
- Concentrated on three key themes:
  - Addressing the Administrative Challenges of IPv6 Deployment
  - Addressing the Budgetary Challenges of IPv6 Deployment
  - Addressing the Technical, Training and Staffing Challenges in IPv6 Deployment
- Let's review these three themes in some detail . . .

Addressing the Administrative Challenges of IPv6 Deployment

- Lisbon Technology Transfer Workshop:
  - 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?

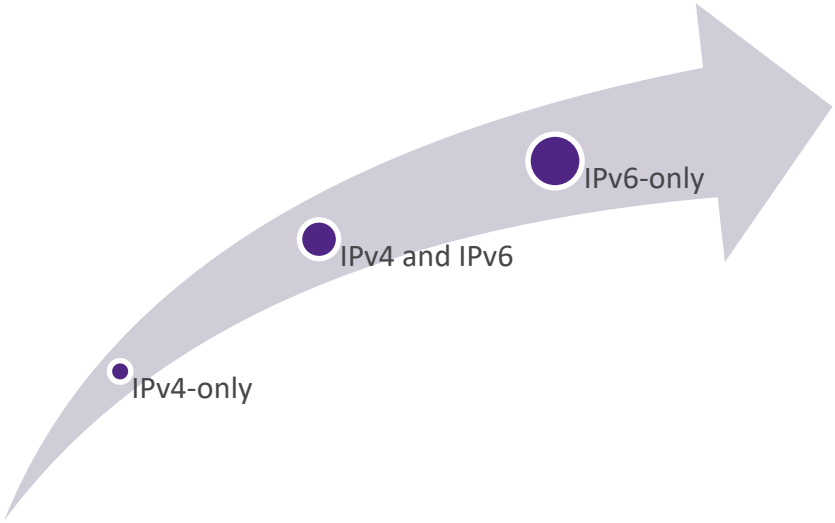
- An IPv6-only network:
  - Has IPv6 as its network layer protocol
  - Does not support *native* IPv4
  - Does not have any *internal* IPv4 connectivity

- 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

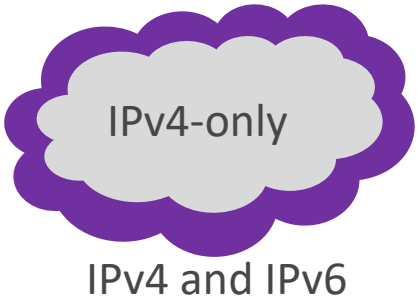
Setting Intermediate Goals for IPv6 Deployment

- 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

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 effect

Addressing the Barriers

- Theme Two: Budgetary Barriers

Addressing the Budgetary Challenges of IPv6 Deployment

- Lisbon Technology Transfer Workshop:
  - The budgetary challenges of IPv6 deployment
  - The fundamental IPv6 budgetary principle
  - Strategic approaches to budgeting for IPv6
  - Minimise IPv6 budget requirements through policy
  - Some IPv6 deployment is zero cost
  - Difficult to avoid costs
  - Case studies in successful budgeting for IPv6 projects

The Budgetary Challenge of IPv6 Deployment

Budget is the most common barrier mentioned amongst member states

Both small and large member states

Member states see IPv6 as an additional cost

The Budgetary Challenges of IPv6 Deployment I

- Difficulties in obtaining budget for IPv6 deployment is a key barrier to deployment
  - It can be difficult to budget for an initiative that is only a “transition to IPv6”
  - Why pay extra for something you already have – the internet?
- Aligning IPv6 deployment with other strategic activities in the MS is essential
- The budget barrier is a category which includes:
  - Staffing
  - Capital costs
  - Operational costs
  - Planning, design and project management
  - IPv6 readiness audit activities
  - Staff training and technology transfer
- Even MS which begin with an IPv6 budget may find it reduced as time passes

The Budgetary Challenges of IPv6 Deployment II

- Some member states have no clear budget assigned to IPv6 deployment
  - Belgium has no budget assigned to the infrastructure upgrades that are a prerequisite to IPv6 deployment – deploring IPv6 opportunistically as upgrades occur for other reasons
- Some member states have reduced their IPv6 ambitions due to budget cuts
  - In Slovenia economic downturn led to cuts in budgets for IPv6 training

The Fundamental IPv6 Budgetary Principles I

Integrate IPv6 into your normal on-going budgets

Don’t budget for IPv6, just include it in everything that you do budget for!

Regardless of whether you have an on-going IPv6 deployment project ensure that everything is moving to IPv6 readiness through refresh cycles and new purchases

The Fundamental IPv6 Budgetary Principles II

You don’t have to do everything at once

IPv6 is designed to be deployed piecemeal, avoid a single, costly budgetary item

Strategic Approaches to Budgeting for IPv6

- There are a number of strategic approaches to budgeting for IPv6 deployment:
  - Implement strategic IPv6 policies to minimise unnecessary expenditure
  - Carefully limit the scope of your IPv6 deployment project
  - Include IPv6 by default in other non-IPv6-specific network projects
  - Embed IPv6 in to everything that you would normally do with IPv4
  - Utilise zero-cost options whenever possible
  - Make sure that greenfield deployments are IPv6 from day-one
  - Some key project activities should already form a part of other budgets; for example you should already have a security policy that includes IPv6
  - Only specifically budget for key essential IPv6 deployment activities

Minimise Budget Requirements by Policy

- Policy can be used to significantly reduce budget requirements for IPv6 deployment:
  - Mandate that all purchases must be IPv6-ready and capable of IPv6-only operation
  - Mandate that all software development is IPv6-ready and capable of IPv6-only operation
  - Mandate that all ICT job descriptions that include a knowledge of networking and particularly IP specifically require IPv6
- These three policies help address several of the budgetary barriers to IPv6 adoption; staffing, capital equipment costs, operational costs, staff training and technology transfer
- However, whilst these policies minimize these costs, they do not eliminate them completely

Some IPv6 Deployment is Zero Cost

- Not all aspects of an IPv6 deployment incur additional costs
- Maximising zero cost options reduces deployment costs easing budget pressures
- Strategic mandates to avoid future waste are often zero cost (see earlier)
  - Suggested strategic mandates embed IPv6 readiness into business activities
- IPv6 in your existing infrastructure and services is zero cost
  - Modern operating systems are IPv6 by default and are IPv6 enabled by default
  - Windows has an IPv6 stack that provides legacy support for IPv4
  - Equipment refreshes will often be IPv6-ready even if you didn't mandate it
- Optional IPv6 capability in existing services can be zero cost
  - A number of cloud and CDN operators will IPv6 enable your services at the edge for no additional cost (often all this requires is checking a tick box – in some instances the default is for this to be enabled)
  - Most transit providers are IPv6 enabled

Examples of Zero-Budget IPv6 Deployment I

- Microsoft Windows is IPv6 enabled by default
  - The Windows IPv6 stack is an IPv6 stack with legacy IPv4 support
  - Turning off IPv6 in Windows is not tested or supported by Microsoft
  - If you have deployed Windows then you have already deployed an IPv6 operating system environment
- Microsoft Applications
  - Most Microsoft applications have been IPv6-ready since 2008
  - If you use Exchange, IIS etc you are using IPv6-ready products
  - Active Directory is IPv6-ready and is IPv6-enabled by default
- Linux Distributions
  - Linux has had an IPv6 stack for almost twenty years
  - Almost all Linux distributions have IPv6 turned on by default
  - The majority of core applications are IPv6-ready and enabled by default

Examples of Zero-Budget IPv6 Deployment II

- *If* you have a regular equipment refresh, then, since most modern enterprise network equipment is IPv6-ready and is often IPv6-enabled by default, your infrastructure may already be IPv6-ready
  - You will *usually* have little trouble with IPv6 support in networking products from the major vendors
  - There are edge cases, especially if you are doing something unusual
- Suppliers of cloud services and applications rarely charge extra for IPv6 support

Costs That May Be Difficult to Avoid

- A significant proportion of the costs of IPv6 deployment may not need an explicit budget. Even so, there may be costs that cannot be avoided
  - You should budget for project management
  - You must budget for the creation of an IPv6 deployment strategy which includes essential design decisions
  - You must budget for the development of an IPv6 address strategy including an IPv6 address schema and allocation policy
  - You must budget for the necessary IPv6 education and training
  - You *may* have to budget for hardware replacement if you have legacy equipment that is not going to be refreshed in time for IPv6 deployment
  - You *may* have to budget for hardware upgrades if current hardware does not have sufficient resources to support IPv4 and IPv6
  - You *may* have to budget for new management tools
  - You *may* have to budget for IPv6-enabling IPv4-only applications

The Fundamental IPv6 Budgetary Principles III

As much as possible decouple IPv6 from budget

Addressing the Barriers

- Theme Three: Technical, Training and Staffing Barriers

Meeting the Technical, Staffing and Training Challenges of IPv6 Deployment

- Lisbon Technology Transfer Workshop:
  - Common Mistakes
  - Meeting the Technical Challenges
  - Meeting the Staffing Challenges
  - Meeting the Training Challenges
  - Resources Available to Member States
  - Diverse Approaches for Diverse Public Administrations

Avoid the Most Common Mistake: IPv4 Thinking

- Do not understand the impact of legacy IPv4 thinking
- Legacy IPv4 thinking is an important IPv6 deployment project risk
- The extent of the differences between IPv4 and IPv6 is always underestimated
- Example: IPv6 Addresses (remember this is just *one* example out of many)
  - Assumption: The difference between IPv6 and IPv4 addresses is their length
  - Reality:
    - IPv6 addresses have different types from IPv4 (e.g. no broadcast)
    - IPv6 addresses have scope and lifetimes (IPv4 addresses do not)
    - It is normal for an interface to have multiple addresses and legal to have many
    - There are a large number of methods for assigning IPv6 addresses
    - Global public addresses are the norm
    - Addresses may change with time

Meeting the Technical Challenges – First Steps

- Addressing the two most common mistakes in IPv6 deployments:
  - Ensure all staff are competent in IPv6
    - Education is crucial
  - Ensure that staff are working to an IPv6 agenda not an IPv4 agenda
    - Again, education is crucial

Meeting the Technical Challenges

- IPv6 is mainstream, it is common in many products, networks and services today
- Don’t under or over estimate the scale of the technical challenges
- Some technical aspects of IPv6 deployment are easy others are complex and require a good understanding of the technical details
- Pay particular attention to these areas:
  - Hardware and software (including locally developed apps and tools) readiness
    - Recent enterprise hardware and software is likely to be IPv6-ready. Legacy is likely to be problematic. Watch out for performance and resource issues
  - Your address schema and choice of address prefix/es
  - Security ideally you should have this in place already
  - Management (particularly DDI/IPAM and local tools)
  - Technical design decisions e.g. autoconfiguration methods, routing protocols, name resolver configuration and the use of transition mechanisms

Meeting the Technical Challenges - Hardware

- Most modern enterprise hardware is “IPv6-ready”
- Your existing infrastructure’s support for IPv6 will vary
  - Very old equipment may not support IPv6 at all
    - This equipment will continue to work in a dual-stack environment using IPv4
    - If IPv6 support is required for IPv6 deployment then it will may need to be replaced or supplemented
  - More recent equipment may support different sets of RFC depending on age
    - You may need to carry out an IPv6 support audit
      - This will depend on the functionality required and the equipment involved
  - Hardware resource limitations may be a problem
    - Requirements for just IPv4 are different from requirements for IPv4 *and* IPv6
    - Memory capacity may be exceeded
  - Legacy equipment may support IPv4 in hardware and IPv6 in software

Meeting the Technical Challenges – Software

- Most modern networked software supports IPv6
- Despite this some software does not support IPv4:
  - There remain commercial products that do not support IPv4
  - Legacy versions of software
  - Internal systems:
    - Line of business applications
    - Web applications
    - System and network management tools
- IPv4 applications will continue to work in dual stack environments
- Legacy IPv4 applications can often be accessed over IPv6 using proxies or translation – they appear to be IPv6 enabled even if they are not
- Internally developed software may need to rewritten
- Software providers may need to IPv6 enable their products

Meeting the Technical Challenges – IPv6 Security

- All modern networks are IPv6 capable (and enabled) by default
- IPv6 security should already be a part of your security policy and operations
- IPv6 security is different from IPv4 security and includes many new challenges
- There are implications for all parts of your security infrastructure:
  - Security personnel (training and experience with IPv6)
  - Edge security (firewalls, NIDS etc)
  - Internal security
  - LAN security
  - First-hop security
  - Node security (host, server and network devices)
  - Logging, monitoring, forensics and auditing

Meeting the Technical Challenges - Management

- A key step in deploying IPv6 is upgrading systems and network management tools to support IPv6
- This includes both commercial, open-source and internally developed tools
- Must provide equivalent support for IPv6 as for IPv4
- Must be able to handle differences in IPv6
  - Longer addresses
  - Multiple addresses per node
  - Addresses that change with time
  - Special address formats (URL, URIs, UNCs, Email addresses etc)
- For example, if you are collecting flow data using Netflow or IPFIX then you will need to ensure that you are using at least Netflow v9 and that your exporters, collectors and analysis tools support IPv6

Meeting the Technical Challenges – Design Decisions

- Autoconfiguration methods
- Routing protocols
- Name resolver configuration
- Name resolution
- Choice and use of transition mechanisms
- Platform configuration:
  - Routers and network infrastructure
  - Firewalls, IDS, NIDS and security infrastructure
  - Servers
  - Workstations and laptops
  - Mobile devices
  - Applications
  - Internet of Everything (IoE)

Meeting the Staffing Challenges

- Staff need to be IPv6 aware
- Staff need to be retrained to have an IPv6 worldview (and see IPv4 as legacy)
- Staff who are key to the IPv6 deployment project need to be proficient in IPv6
- Staff who are responsible for network design, planning, deployment, operation, security, support and software development need to be at least as proficient in IPv6 as they are in IPv4
- Network professionals with experience of deploying IPv6 are rare

- Three solutions:
  - Hire people with the necessary IPv6 skills (only useful with new staff)
  - Train existing staff (see later)
  - Use contract resources or consultancy services

Meeting the Training Challenges - Background

- IPv6 education is pivotal to the success of an IPv6 deployment
- All reports of IPv6 deployments attest to the importance of IPv6 training
- Education is essential for architects, administrators, developers and support staff
- You need to:
  - Understand the need for training
  - Identify the groups of staff who will require training
  - Prioritise the training of key players in the IPv6 deployment project
  - Determine when the training will be required
  - Determine how the different groups should be trained
- Beware of:
  - Out-of-date material and guidance (this is common)
  - Appreciate that unlearning legacy IPv4 habits is non-trivial

Meeting the Training Challenges - Approaches

- Three main categories of training approaches:
- No training
  - Hire or contract staff with the necessary skills and experience
- Awareness
  - For staff with limited networking exposure you can provide self-learning materials, documentation, guides, whitepapers, web-sites, videos, Computer based training (CBT) and short introductory sessions
- Formal Training
  - Staff directly involved in network administration, network security, system administration, network support and software development are likely to require targeted formal training. Usually this will be instructor led. We have found that *all* organisations underestimate the IPv6 training that they require.

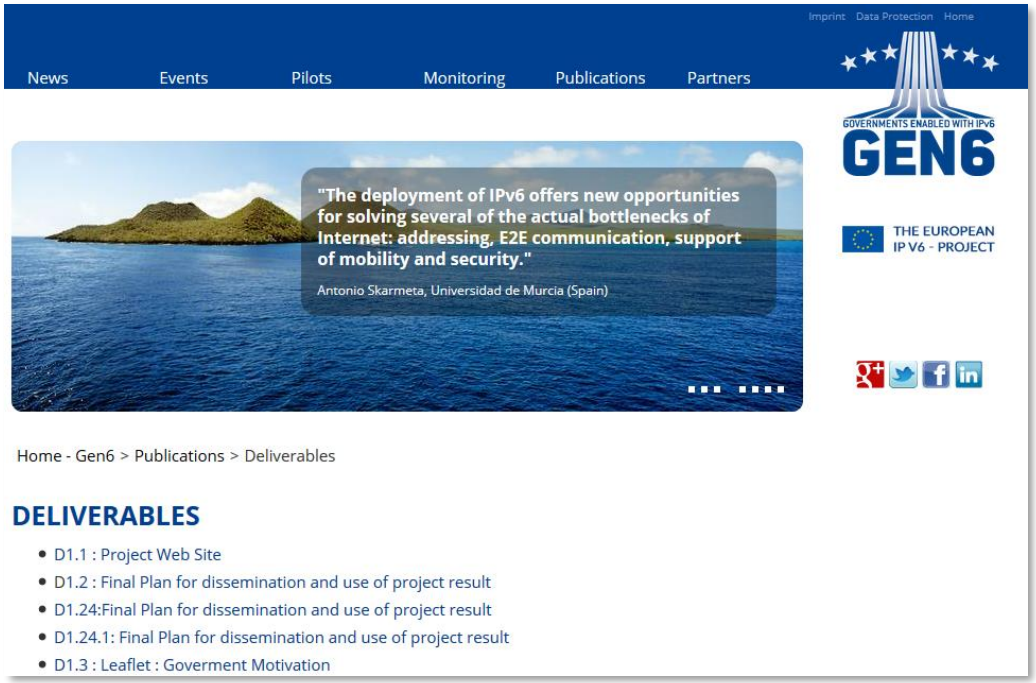
Embed IPv6 into all network related training and induction materials

IPv6 Resources Available to Member States

- GEN6 part of an ISA2 project that piloted IPv6 deployments in member states
  - Includes training/education/case study materials to help member states
  - http://www.gen6-project.eu/
- IPv6 Framework for European Governments – SMART 2016/0099 (this project)
  - Provides documents to assist in IPv6 technology transfer and deployment
    - Synthesis of the status of IPv6 in European member states
    - Guidelines and process: IPv6 for public administrations in Europe
    - Technical profiles: IPv6 for public administrations in Europe
    - IPv6 address acquisition in Europe
    - Interim report on this project
    - Future resources to be added include materials from this workshop
  - http://ipv6gov.eu/

Resources Context – ISA2 Pilot Project

- A previous ISA2 project piloted IPv6 deployments in a selection of member states
- Part of that project – called GEN6 – was building training / education / case study materials that would help Member States as they considered IPv6 deployment
- The GEN6 materials are online and available at:
  - http://www.gen6-project.eu/



Questions?