Technical Profiles IPv6 for Public Administrations in Europe

Part of a Study on Implementation of the ISA2 Programme Action 2016.10 - IPv6 Framework for European Governments – SMART 2016/0099

Plum Consulting
iDate
Internet Policy Advisors
Synetergy
Erion

10 April 2018

Plum Consulting, London
T: +44(20) 7047 1919, **www.plumconsulting.co.uk**

Table of Contents

Executive Summary

Every IPv6 deployment is different. One of the main reasons for this is that every organisation starts their deployment from a different point. In the case of public administrations, some will already have infrastructure that is ready for the deployment of IPv6 and some will not.

This document looks at different approaches to planning an IPv6 deployment and the steps necessary to determine if the organisation is ready for IPv6 deployment. A key part of this is understanding how to measure IPv6-readiness against an IPv6 deployment strategy.

To appreciate the role of an IPv6 readiness audit and technical profiles, this document provides an overview of IPv6 deployment planning, the different approaches to deploying IPv6 and IPv6 transition mechanisms. A companion document from this project provides guidance on developing an IPv6 addressing plan.

This document is broken into five parts, these are:

- An overview of IPv6 deployment planning. This provides context and general guidance relevant to technical profiles and IPv6 readiness.
- An overview of IPv6 transition technologies. This describes the purpose of the main transition technologies and discusses when and where they can be used.
- A review and summary of existing IPv6 technical profiles. This examines the existing profiles for measuring IPv6 readiness. These include profiles by RIPE, the German government, the US government and the IPv6 Forum.
- Technical profiles for IPv6 hardware. An up-to-date technical profile for IPv6 readiness.
- An appendix summarising RIPE requirements for IPv6 compatibility.

1 Planning the Deployment of IPv6 in Public Administrations

Planning the deployment of IPv6 is often a complex task. It is especially complex in public administrations. Public administrations usually have large and complex network environments. These networks provide a very wide range of services both internally and to the public. Network applications in use in public administrations include those found in any enterprise as well as those that are specific to government.

In addition to the problems of scale and complexity, public administrations looking to deploy IPv6 are also often constrained by other factors. These include budget limitations and the location or responsibility for IT within the organisation.

IPv6 has also been explicitly designed to make its deployment as flexible as possible. It is technically possible to begin a deployment, at the network edge, in a network's core or with specific applications or services. Whilst almost any approach is technically possible, they are not all equally desirable.

For these reasons, planning the deployment of IPv6 in public administrations can take many forms. It can vary in scope, in time-scales and in the approaches that are used.

Despite the wide range of potential variation in IPv6 deployments in public administrations, most IPv6 deployment projects still have a set key common of features. In this section, we provide an overview of these and some of the key factors that you should consider when planning an IPv6 deployment. You should read this in conjunction with the companion document on IPv6 address planning. The IPv6 addressing document looks in detail at IPv6 addressing and it also provides an overview of IPv6 deployment planning with an alternative focus from the one found here. The focus of this document is on the process of IPv6 readiness assessment.

High-Level IPv6 Deployment Planning

First let's take a brief look at the common set of key deployment activities that are found in most IPv6 deployment projects. These are interrelated and are often carried out in parallel. Not all projects will have all these components or carry them out in the same order. An overview of a typical deployment project is shown in *Figure 1*. This shows the key deployment activities of an IPv6 project that are listed here:

- **IPv6 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 of the IPv6 Deployment
- **Key IPv6 project activities:**
  - Obtain IPv6 Address Space

- Initiate an IPv6 Awareness and Education Programme
- Carry out a Readiness Audit and/or Pilots/Trials

This guide is focused on the IPv6 readiness audit part of these activities. However, we will briefly consider here some aspects of the deployment project including, defining the project goals and scope, the deployment strategy and developing a project plan.

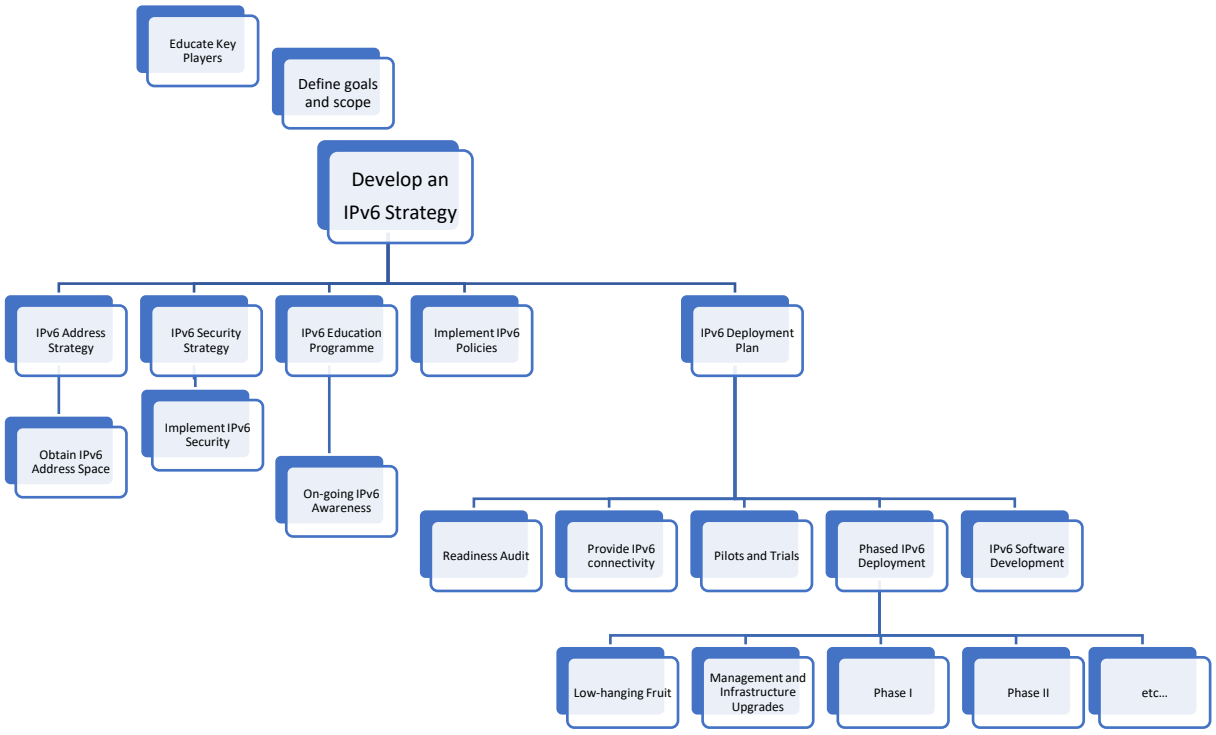

Figure 1 Overview of the IPv6 Deployment Process[1]

Setting IPv6 Strategic Goals

As we have already discussed, IPv6 deployment projects in public administrations can take many forms. However, all need to define clear goals. Understanding the goals of an IPv6 deployment is crucial to success.

The long-term goal of an IPv6 deployment should be an **IPv6-only network**. It is important that everyone involved in the IPv6 deployment appreciates that the aim is not to simply add IPv6 to a network, but it is to eventually eliminate IPv4 for the network. Failure to fully appreciate this can be detrimental to the deployment of IPv6. The maximum benefits of deploying IPv6 are only achieved when IPv6 has been eliminated.

Understanding this goal helps to avoid creating an IPv6 design that is compromised by IPv4. It also limits the risk that staff may view IPv6 as a secondary protocol to IPv4. This can lead to an incomplete deployment and to a lessor service over IPv6 than over IPv4.

[1] Based on Erion's IPv6 Deployment Process and used with permission.

Your goal should be to seek a minimum of parity between IPv6 and IPv4 and you should prefer IPv6 over IPv4 whenever possible.

Later in this document we will discuss how connectivity to the IPv4 internet can still be maintained even from an IPv6-only network.

Whilst IPv6-only should be the long-term goal, it is important to appreciate that it is often impractical to deploy IPv6-only immediately. Therefore, you should also have intermediate goals for IPv6 that are appropriate for the short and medium term, that act as an interim step on the way to migrating to IPv6-only.

The most common IPv6 deployment approach is **dual-stack**. This is because dual-stack deployments keep the existing IPv4 networking whilst deploying IPv6 alongside. If done properly, dual-stack deployments should not interfere with the operation of existing IPv4 services and applications.

There are many ways to deploy a dual-stack solution. The primary one is to use native IPv4 and native IPv6, on the same infrastructure. There are alternatives where an IPv6 service might be provided using transition techniques.

The two most common intermediate goals for an IPv6 deployment project are to:

- **Deploy IPv6 at the edge**
  - On the organisation's public facing services
  - On access and transit at the organisation's network edge
- **Deploy dual-stack**
  - Adding IPv6 to existing IPv4 networks

Defining the IPv6 Deployment Project Scope

An IPv6 deployment can touch every part of a public administration. It will have an impact well beyond IT and technology. The overall deployment project must recognise this and take non-technological areas into full consideration.

However, the deployment project does not have to be all encompassing in scope. There should be a balance between setting the right goals and policies and the scope of the implementation.

Areas that should be considered for inclusion in an IPv6 deployment project are:

- Applications
- Information
- Computing Platforms
- Networking
- Infrastructure Services
- Processes
- Standards
- Security

- Governance
- Buildings
- Sites
- Transport
- Communications
- Media
- Human Resources

For budgetary, or other reasons, the project scope may need to be limited by geography (e.g. specific regions), network infrastructure (e.g. a new data centre), function (e.g. government application), departments or special projects (e.g. Internet of Things - IoT). Even if the scope if limited, the strategic goal of deploying IPv6-only networks across the administration should influence the project design and implementation.

Timescales for an IPv6 Deployment

Deploying IPv6 is not just a project it is also an on-going process. It needs to be built into the operational activities of the organisation. A typical deployment is often made up or many projects or subprojects.

IPv6 deployment is usually a lengthy process and it requires patience and commitment from those driving the project. IPv4 is likely to be around for a long time. Even if you move to IPv6-only networks you will still have IPv4 at the edge for a substantial time into the future.

Certain aspects of an IPv6 deployment require hard deadlines. This is particularly true for activities that the rest of the project depends upon. For example:

- 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

Other aspects of the deployment may be on-going processes driven by other activities, but the above need to be carried out early in a project.

Approaches to Deploying IPv6

IPv6 has been designed to be extremely flexible in how it can be deployed. As a result, there are an enormous number of different approaches to deploying IPv6. There are three common categories of approaches to deploying IPv6. IPv6's flexibility means that these approaches can be use separately or in parallel at the same time.

- **Inside-out**

Deploy IPv6 in the core network infrastructure then enable networks and applications

- **Outside-In**

  Enable IPv6 at the network edge and then enable in the core

- **IPv6 Islands**

  Enable islands of IPv6 in specific areas and gradually expand them

The choice of mix of approaches will depend on many factors, both business and technical. Here are some specific examples:

- **IPv6 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.

  You need to obtain IPv6 connectivity as early as possible in your IPv6 deployment. Having IPv6 connectivity does not mean that you must enable IPv6 with all your networks, it is an essential part of making this possible.

  Today, most transit providers and many internet service providers (ISPs) are IPv6 enabled. You will need native IPv6 connectivity from your service providers. You need to beware of immaturity or inexperience within your service providers. Also, you need to beware of second-class IPv6 services from some service providers.

- **Deploying IPv6 on Public Facing Services**

  Deploying IPv6 on public facing services is often much easier than organisations expect. There are two main ways of IPv6-enabling public services. These are; natively by converting the service to dual-stack operation and using transition mechanisms to translate an IPv4-only service to IPv6. Many Content Distribution Networks (CDNs) provide translation or dual-stack services as standard (sometimes by default). Load-balancers often include translation to IPv6 enable IPv4-only services. This is a fast and easy solution to “IPv6-enable” IPv4-only services. It is usually trivial to enable for testing and then move to production later with an extremely limited risk to existing services.

- **Deploying IPv6 in Existing IPv4 Networks**

  Dual-stack is the default and most common method of deploying IPv6. Dual-stack networks support both native IPv4 and native IPv6 and dual-stack nodes can communicate using both native IPv4 and native IPv6.

  Dual-stack deployments usually involve adding IPv6 to an existing IPv4 network (although it is perfectly possible to deploy new networks as dual-stack). If carried this is out correctly there should be no impact on the existing IPv4 traffic or applications. This reduces risks.

  There are disadvantages to dual-stack. Dual-stack networks are more complex because they contain two protocols that have complex interactions with each other. There is an increased administrative overhead because there are two protocols to manage. Each node requires more network resources to support both protocols. There are additional routing complexities and finally there are greater security challenges (both IPv4 and IPv6 vulnerabilities with complex interactions between the two). None of these problems are insurmountable in modern networks and dual-stack remains the easiest and most flexible deployment approach.

- **Deploying IPv6-Only Networks**

  Whilst dual-stack is the default and most common method of deploying IPv6 in existing networks. In new networks you should consider deploying IPv6-only networks. This approach maximises the benefits of IPv6, reduces management overhead and removes the need to invest additional effort in removing IPv4 in the future.

  A new data centre is a good example of a new network that could be implemented as IPv6-only.

  IPv6-only networks can continue to communicate with the IPv4-internet and IPv4-nodes using transition mechanisms (see later in this document).

Whichever approach or approaches are used it is important to remember that IPv4 will need to be supported in some form for an exceptionally long time.

Developing an IPv6 Deployment Plan

There are many approaches to developing an IPv6 deployment plan and each public administration's plan will be different. The process outlined here is one that can scale from local government initiatives, to national IPv6 migration plans. The steps are the same for either case. We suggest five steps to developing an IPv6 transition plan for public administrations:

- Assess the current state of the environment (IPv6 Readiness Audit)
- Define the required future state (the objective)
- Perform a gap analysis (the difference between the current state and the required state)
- Develop a plan to reach the required future state
- Prioritise activities while being aware of external dependencies

This rest of this document focusses on the IPv6 readiness audit, gap analysis, deployment approaches and technical profiles.

The IPv6 Readiness Audit and Gap Analysis

To determine the scale of the work required to prepare for deploying IPv6 you need to determine your organisation's readiness for deploying IPv6. You need to be able to estimate the gap between what you have and what you need to deploy IPv6. Your aim is to identify potential problem areas and plan to resolve them.

Some organisations carry out a comprehensive IPv6 readiness audit others focus only on specific areas of interest where they expect there to be shortcomings. You need to determine what you are going to audit and what you are going to look for.

We recommend minimising the effort required in a readiness audit by placing as much of the responsibility for IPv6 readiness on your suppliers as possible. Ensure that your procurement procedures require IPv6 readiness. Mandate that your suppliers provide equivalence to IPv4 in their IPv6-ready products. Put the onus on them to take responsibility for resolving problems.

The focus of this document is on technical readiness. However, IPv6 readiness is not just about IT infrastructure. IPv6 readiness should cover at least the following:

- **IPv6 support and functionality in:**
  - Network infrastructure
  - Network nodes (desktops/laptops/mobiles/routers/switches etc…)
  - Network services (DNS, DHCP, File-sharing, Single-sign-on, etc…)
  - Line of business applications
  - Security software and appliances
  - Network applications
  - Network management systems and tools
  - Cloud services
  - Web services
  - Hosting services
  - Internet service providers
  - etc…
- **Device resources to support the addition of IPv6** (e.g. CPU and memory)
- **Management tools**
- **Vendor competence in IPv6**
- **Expertise** (education, training and hiring)

IPv6 is not a feature to be deployed. Instead, it is an update of the TCP/IP protocol stack – any device, service, or application that uses this protocol stack is in the scope of the assessment. You should pay attention to bespoke or in-house tools and applications. These are less likely to be IPv6-ready than modern commercial or open-source products which are mostly IPv6-ready.

When assessing the IPv6 readiness of a device you should look to evaluate if the device is:

- IPv6-ready, no hardware or software upgrades are required.
- IPv6-ready but it requires hardware upgrades.
- Hardware is IPv6-ready, but a software upgrade is required.
- Not IPv6-ready.
- Unknown status, further analysis is required.

Several public profiles exist for IPv6. These have been created to assist an organisation in assessing the IPv6-readiness of its IT infrastructure. We will look at these in more detail later in this document. Here is a summary of the current public profiles:

- 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)

A properly conducted IPv6 readiness audit and gap analysis will allow an organisation to plan the IPv6 deployment more accurately. It will help estimate the scale of the cost and provide essential information towards estimating project timescales. In addition, it should provide a readiness matrix that can be used to track the state of IPv6 readiness as upgrades and equipment refreshes take place over the time of the IPv6 deployment.

Furthermore, results of the readiness audit may influence the choice of future suppliers. The act of undertaking a readiness audit will help signal to suppliers the fact that they need to be IPv6-ready if they are to continue as an authorised supplier. The readiness audit will also provide you with some understanding of your vendor's IPv6-roadmaps.

When it comes to services such as IP connectivity and IP transit, your readiness audit will help you evaluate not only the availability of IPv6 services, but also the suitability of those services. For example, you need to determine if service providers are truly providing a native IPv6 service or not.

The Technical Profiles – later in this document – are intended to assist in the assessment of every platform, service, application, and network resource in terms of its IPv6 readiness.

Strategy to Achieve the Future State

The outcome of the IPv6 readiness audit and the gap analysis is a matrix that has the following information:

- The IPv6 requirements for each platform or service in the network
- What it takes to make each platform or service in the network compliant with the required level of IPv6 support
- The process or procedure for making the platform or service in the network IPv6 ready
- The cost and staffing implications for making the platform or service IPv6 compliant

This matrix then supports the development of a plan for moving from the current state of the network to the desired state of IPv6 deployment.

Often, governments will already have established procedures and processes for IT projects. These processes can use the matrix developed in this step as input.

Project Plan Development: Prioritise Activities

Since public administrations often have existing processes for IT projects, there is sometimes no need to create new processes to support IPv6 deployment. Instead, it may be better to integrate the IPv6 deployment into an existing planning cycle with the support of both internal and external stakeholders.

External stakeholders especially may have dependencies that affect the timelines and priorities of the project plan. Since any IPv6 transition project in public administration is a strategic evolution of the IT

environment, it is crucial to integrate the project in the government's existing governance model. This includes, at a minimum:

- Senior management visibility and support: a clear and consistent message of commitment from the senior management is essential to making sure that each group within the organization is prioritizing appropriately the IPv6 related activities.
- Enforcement: adherence to the IPv6 strategy and meeting the project goals should be a measure of the organizational, group and individual performance.
- Cross-functional coordination: All groups within the organization must collaborate in addressing mutual dependencies with respect to IPv6 integration.
- Communicate frequently at all levels: Continued communication on the IPv6 adoption topic reinforces the expressed importance placed on the project and enables its progress to be tracked closely.
- Make IPv6 a natural part of other activities: Raise awareness about IPv6. Reward IPv6-related achievements and innovation.

2 Transition Approaches and Technologies

IPv6 was explicitly designed to ease its deployment into an IPv4 world. The IPv6 techniques that help its deployment in an IPv4 world are called IPv6 transition techniques.

The most important IPv6 transition technique is called dual-stack. IPv6 dual-stacks include support for legacy IPv4. All modern operating systems have IPv6 dual-stacks. That is, they are primarily IPv6 stacks that have support for IPv4.

In addition to dual-stack, there are tens of other transition mechanisms that have been created to solve a range of different IPv6 deployment problems. The types of problems that transition techniques help solve and that public administrations may encounter during deploying IPv6 are:

- **No native IPv6 connectivity to the public IPv6 internet**

  It is increasingly unlikely that a public administration will require an IPv6 transition technique to provide IPv6 connectivity for their networks to the public IPv6 internet. In all cases, they should seek native IPv6 connectivity from their service providers. The only place that public administrations might use transition mechanisms to connect to the public internet is when they have roaming nodes or home users in IPv4 networks that wish to connect to the public administration's IPv6 network.

- **Lack of IPv6 support in LAN infrastructure**

  It is unlikely that a public administration will need to use an IPv6 transition technique to carry IPv6 over their LAN infrastructure. Most LAN infrastructure can carry IPv4 and IPv6. If it does not, then the public administration should consider upgrading their LAN infrastructure.

- **IPv6 not supported in routing infrastructure**

  Modern routers support IPv6 by default. Older equipment may support IPv6 but might not have adequate resources to route both IPv6 and IPv4 at the same time. It is unlikely that public administrations will use transition techniques to overcome this problem. If the routing infrastructure is not capable of supporting IPv6 then it is better to replace or upgrade the infrastructure rather than to use a transition mechanism.

- **Need to provide connectivity to legacy IPv4 services from IPv6-only networks**

  As IPv6 is deployed, some networks may be migrated to IPv6-only operations. The nodes in these networks may still need to connect to IPv4-only services on the IPv4 internet. It is likely that public administrations will eventually deploy IPv6-only networks and will need to use transition techniques to provide access to the legacy IPv4 internet.

- **Need to provide connectivity to IPv6-only services from IPv4-only networks (or nodes)**

  As IPv6 is deployed, some services may only be available over IPv6. Legacy IPv4-only networks and nodes may need to connect to such services. In these cases, public administrations will need to deploy appropriate transition mechanisms.

There are many transition mechanisms. Over time the maturity of transition mechanisms has improved, some have been deprecated and others have become irrelevant. You will need to choose the most appropriate mechanisms for your network given current best practice.

Overview of IPv6 Transition Mechanisms

There are three main techniques that underpin many of the IPv6 transition mechanisms. These are:

- Dual-stack
- Tunnelling
- Protocol (and address) translation

Sometimes two or more these techniques are used together in a single transition mechanism. The following sections provide brief introductions to these techniques.

Every transition mechanism introduces additional complexity. This can have an adverse effect on network operations, security, and performance. In some cases, this can be significant. It is always best to try to avoid transition mechanisms. Native transport using IPv4 or IPv6 is always better than tunnelling or translation. This is one of the reasons why many IPv6 deployments are dual-stack. Dual-stack makes it possible for nodes to communicate natively without having to resort to transition mechanisms.

However, it is not always possible to avoid transition mechanisms. The most common scenarios where transition mechanisms are likely to be required are:

- Providing IPv6 connectivity to legacy IPv4 services that cannot easily be upgraded to IPv6
- Providing IPv6 connectivity for roaming IPv6 nodes in IPv4-only networks (public or private)
- Providing IPv4 connectivity to the legacy IPv4 internet for IPv6 nodes in an IPv6-only network

Transition Mechanism: Dual-Stack

All IPv6 nodes are capable of dual-stack operation. That is, they can all communicate using either IPv6 or IPv4 without any translation or tunnelling.

Dual-stack networks are networks that are fully configured for both IPv4 and IPv6. Nodes in a dual-stack network can communicate using either IPv4 or IPv6. They usually use both IPv4 and IPv6, choosing the best protocol each time they communicate.

One of the benefits of dual-stack is that it can usually be deployed on an existing IPv4 network without interfering with the existing IPv4 configuration. For this reason, dual-stack is the most common way that IPv6 is deployed. IPv4-only nodes can operate as normal in a dual-stack network.

Configuring a network for dual-stack operation requires that all parts of the network infrastructure is capable of supporting IPv6. This is both in terms of functionality and in terms of capacity. First, you will need to configure IPv6 connectivity, both internally and to the public IPv6 internet. This means that you must duplicate much of the existing IPv4 network layer functionality for IPv6. For this reason, deploying dual-stack typically requires careful planning and testing. Areas that need to be addressed include:

- IPv6 addressing and IP address management
- IPv6 address and network autoconfiguration
- IPv6 routing and dynamic routing

- IPv6 security including IPv6 firewall configuration
- IPv6 name resolution (specifically DNS)
- IPv6 network management
- IPv6 network services and applications

Since the network will continue to provide connectivity to services and applications over IPv4 you do not necessarily need to enable everything at once. Nodes will only begin to use IPv6 for a connection once the service that they are connecting to is IPv6 enabled and once the IPv6 addresses have been added to DNS.

Most modern equipment and operating systems support IPv6 by default. Some networks that contain older equipment may require equipment refresh or upgrades to support IPv6. Since dual-stack networks must support two protocols, network devices such as routers must have enough capacity (CPU and memory) to process the two protocols.

Today, most IPv4 networks are dual-stack networks because they contain modern operating systems that have IPv6-stacks that are enabled by default. This includes, Windows, Linux, and mobile devices. Therefore, once you have enabled global IPv6 connectivity in your networks these nodes will seamlessly begin to use IPv6 connections to the global internet. (Even before you do this, these nodes will use IPv6 if they can, for example within a subnet using IPv6 link-local addresses.)

Dual-stack is a useful medium-term deployment approach that is common both within public administrations and in enterprises. It can be used as an interim step to migrate to an IPv6-only network. An IPv6-only network is desirable because it removes the need to support both IPv4 and IPv6. Supporting both protocols is a significant overhead. It complicates network administration and increases the resources needed within the network. As the global IPv4 continues to deteriorate, it is advantageous to disable it and focus on IPv6. Removing IPv4 also reduces the load on existing IPv4 specific infrastructure such as Network Address Translation (NAT) and Carrier Grade NAT (CGN) devices. It also makes possible innovative solutions such as secure peer-to-peer connectivity without VPNs.

Transition Mechanisms: Tunnels

Network tunnels carry one protocol within another protocol. They make it possible for a protocol to be carried across infrastructure that does not support that protocol. For example, in an IPv4-only network, an IPv6-in-IPv4 tunnel makes it possible for IPv6 traffic to traverse the IPv4-only network. The IPv6 datagrams are encapsulated within IPv4 datagrams and carried across the IPv4-network. Conversely in an IPv6-only network, IPv4 traffic can be carried over the network in an IPv4-in-IPv6 tunnel. These are called IP-in-IP tunnelling. It is also possible to encapsulate IPv6 or IPv4 within other protocols, for example UDP or HTTPS.

In the early days of IPv6 deployment, when it was difficult to obtain IPv6 connectivity, tunnels were used to connect to the IPv6 internet over IPv4-only networks. This is rare today. However, it is becoming increasingly common for IPv6 to be used to carry IPv4 traffic within IPv6-only networks.

Today, there is a move towards using transition techniques that provide IPv4 connectivity within an IPv6 world, rather than the other way around. This is because, native IPv6 connectivity is easy to obtain and because deploying native IPv6 within today's infrastructures is becoming easier. Recently,

the focus has moved to providing IPv4-as-a-service (IPv4aaS) to conserve IPv4 address resources and reduce the need for IPv4 infrastructure.

Tunnels can be either manual or automatic. Most IPv6 transition techniques use automatic tunnelling where the transition technique tunnels the traffic automatically without the need to manually create a tunnel.

All tunnels impose an additional overhead due to the extra headers used for encapsulation. In addition, if the location of the tunnel end-points are distant from each other, tunnels can have a significant impact on latency. For these reasons, tunnels do not perform as well as native traffic.

The following sections briefly describe some of the tunnelling transition mechanisms.

6to4

6to4 is designed for the scenario where an IPv6 network or an IPv6 node do not have native connectivity to the global IPv6 internet but do have a public IPv4 address. 6to4 automatically tunnels traffic between 6to4 networks, 6to4 nodes and the global IPv6 internet. It uses the public IPv4 address as the tunnel endpoint.

6to4 nodes and networks have a unique, global IPv6 address prefix that is constructed from their unique public IPv4 address and a reserved 6to4 IPv6 address prefix. 6to4 uses 6to4 relays to reach the global IPv6 internet.

6to4 has many disadvantages. These include:

- No built-in security and serious security problems
- Forced to use one global prefix that is not guaranteed to be globally routable
- 6to4 relays have been deprecated

For these reasons, and others, 6to4 should not be used to provide IPv6 connectivity.

6rd

6rd is based on 6to4. It is designed for use by an ISP to deploy IPv6 in its IPv4-only access network. 6rd automatically tunnels IPv6 datagrams over the IPv4-only access network providing an IPv6 service to the ISP's customers. The ISP can provide IPv6 addresses to its customers from any IPv6 address space that it has, such as its Provider Aggregatable (PA) space. As far as the customers and the global internet are concerned, the customers appear to have a native IPv4 and a native IPv6 service (dual-stack).

6rd solves many of the problems of 6to4. Since it is contained with the ISP's access network it is possible to implement some security and because it can use a prefix of the ISP's choice 6rd traffic is globally routable. It is unlikely to be relevant to most public administrations.

ISATAP

The Intra-Site Automatic Tunnelling Protocol (ISATAP) is designed for IPv4-only private intranets that cannot support native IPv6. It uses automatic IPv6-in-IPv4 tunnelling over the intranet to allow ISATAP nodes to communicate using IPv6. ISATAP uses IPv6 addresses that are created by embedding a node's IPv4 intranet address (RFC1918) into a special interface identifier (IID).

ISATAP traffic can reach the global IPv6 internet using ISATAP routers at the edge of the private intranet.

ISATAP is rarely used today, as it is always better to deploy native IPv6 with an intranet. ISATAP has many problems, including:

- No built-in security and serious security problems
- Treats the whole intranet as a single subnet
- Lack of multicast

Public administrations should avoid using ISATAP.

Teredo

Teredo is designed for IPv6 nodes that are connected to IPv4-only intranets and whose internet connectivity is through one or more layers of Network Address Translation (NAT).

NAT breaks or makes unreliable IPv6-in-IPv4 tunnelling. Therefore, it is not usually possible for a node behind NAT to use any transition technique that uses IPv6-in-IPv4 tunnels. Teredo solves this problem by encapsulating IPv6 datagrams within UDPv4. Due to the complexity of NAT, Teredo must discover the NAT configuration before it can configure the Teredo client. Furthermore, Teredo must use special Teredo addresses to store address information that is necessary to operate through NAT. Teredo also requires additional devices called Teredo servers and Teredo relays to function.

Teredo is only useful for connecting individual IPv6 clients behind NAT to the global IPv6 internet. It has several problems including security issues.

Tunnel Brokers

Tunnel brokers are organisations that provide a service, using several types of tunnels, that can connect networks to the IPv6 internet over the IPv4 internet. They use both manually and automatically configured tunnels. Tunnel brokers are rarely required today as it is usually possible to obtain a native IPv6 service from a service provider.

Public administrations may find it useful to use tunnel brokers for IPv6 testing. However, they should be unnecessary as native IPv6 connectivity is easy to obtain.

Dual-Stack Lite (DSLite)

DSLite is used to provide IPv4 connectivity in an IPv6-only network. DSLite automatically tunnels IPv4 over IPv6. DSLite is designed to be used by service providers in IPv6-only access networks to provide IPv4 access. DSLite enables service providers to deploy an IPv6-only access network thereby removing the overheads of maintaining and operating IPv4 in the access network. DSLite allows them to provide a dual-stack service to their customers.

DSLite is used in some service provider networks and in some mobile operator networks. It is rarely used in enterprise solutions as IPv6-only networks in enterprises tend to use alternative solutions such as NAT64/DNS64 to provide IPv4 connectivity.

Transition Mechanisms: Protocol and Address Translation

Translation transition mechanisms convert datagrams between IPv4 and IPv6. For an IPv6-only node to be able to communicate with an IPv4-only node (or vice versa) both the protocols ***and*** the addresses must be translated.

This is different from Network Address Translation (NAT44) in IPv4 for two main reasons. Not only does it require protocol translation rather than just address translation, it also requires address translation between two completely distinct types of address families.

Unfortunately, since IPv4 and IPv6 are vastly different protocols, translation between the two can sometimes be difficult or impossible. As a result, protocol and address translation suffer from many of the problems of traditional NAT44. These include:

- Breaking end-to-end connectivity,
- Unidirectional communication
- Breaking application layer protocols
- Security issues
- Performance and reliability issues

Just as in NAT44, some of these translation techniques require application layer gateways (ALGs) for certain application protocols. However, despite this, some IPv6 transition mechanisms that use translation are more robust that NAT44.

Protocol translation is typically used in the following scenarios:

- Providing connectivity to IPv4 services from IPv6-only nodes in an IPv6-only network
- Providing connectivity to IPv4 services from dual-stack nodes in an IPv6-only network
- Providing an IPv6 service from an IPv4-only service
- Providing an IPv4 services from an IPv6-only service

The following sections briefly describe some of the IPv6 transition mechanisms that are based on protocol translation.

SIIT

Stateless IP and ICMP Translation is a standard that defines a stateless method of converting IPv4 packets to IPv6 packets and vice versa. Whilst it is not used as a translation mechanism on its own, it is used as a basis for other translators including; NAT-PT, SIIT-DC, 464XLAT and MAP-T.

NAT-PT and NAPT-PT

The Network Address Translation - Protocol Translator (NAT-PT) and Network Address and Port Translator - Protocol Translator (NAPT-PT) were early attempts to create generalised solutions for protocol translation between IPv4 and IPv6. Unfortunately, there were many problems with NAT-PT and NAPT-PT that led to the IETF deprecating the standard in 2007. Whilst NAT-PT is widely implemented on many platforms, it should be avoided. In situations where you might have used NAT-PT in the past, today you would use an alternative such as NAT64/DNS64 or NAT46.

NAT64 and DNS64

NAT64 and DNS64 are designed to be used in IPv6-only networks. They provide IPv6-only nodes with client-initiated access to the global IPv4 internet. In NAT64, address translation is initiated by the DNS ALG (DNS64). If a DNS query returns an IPv4 address, the DNS64 server returns a fake IPv6 AAAA answer to the client. The fake IPv6 address is routed to the NAT64 translator that identifies the IPv6 prefix as one that should be translated to IPv4. As with NAT44, the NAT64 device has a pool of IPv4 addresses that it can use as the source address for out-going IPv4 traffic. NAT64/DNS64 is robust

with a wide range of traffic. However, as with NAT44 some applications will fail if they traverse a NAT64 device.

NAT64/DNS64 is widely available on many platforms and is a viable option for many IPv6-only deployments in public administrations.

464XLAT

464XLAT is designed to be used in IPv6-only networks. In this case, the clients are dual-stack. It provides dual-stack clients in an IPv6-only network with connectivity to the global IPv4 internet using native IPv4.

464XLAT is a double translator. It translates IPv4 datagrams into IPv6 datagrams so that they can traverse the IPv6-only network and it then translates them back to IPv4 datagrams. Since the IPv6 protocol's headers have a superset of most IPv4 protocol headers, this double translation is exceptionally reliable and usually results in the packets traversing the IPv6-network without their headers being unintentionally mangled. For this reason, 464XLAT is more robust that NAT64/DNS64. The only downside is that the nodes on the IPv6-only network are dual-stack rather than IPv6-only.

SIIT-DC

Stateless IP/ICMP Translation for IPv6 data centres is a standard that allows IPv6-only data centres to provide IPv4 connectivity at the edge. A big advantage of SIIT-DC is that it allows operators to build single protocol (IPv6-only) DCs and to avoid having to manage two protocols within the DC.

Public administrations are likely to want to consider SIIT-DC and equivalents for new-build IPv6-only environments such as new DCs.

MAP-T and MAP-E

Mapping of Address and Port (MAP) transition mechanism, MAP-T (Translated) and MAP-E (Encapsulated) are techniques that allow an operator to assign a limited set of IPv4 addresses and ports to a subscriber. IPv4 traffic is ether translated (MAP-T) or tunnelled (MAP-E) over an IPv6-only access network.

MAP-T and MAP-E are based on a standard called Address plus Port (A+P). A+P makes a more efficient use of address space by allowing subscribers to share addresses. Carrier Grade NAT (CGN) also allows for the sharing of addresses amongst subscribers. MAP has several benefits over CGN, for example, MAP is stateless, and MAP works over IPv6-only networks thereby removing the need to support IPv4 in the access network. In addition, the IPv6 addresses used by MAP can be efficiently aggregated and routed by the provider due to the way in which the IPv4 addresses and port ranges are encoded into the MAP address.

3 Technical Profiles, Part One: Existing profiles

There are more than 200 RFCs that relate to the specification of IPv6, its features and its implementation. This number is increasing each year. The Internet Engineering Task Force publishes these standards as Request for Comments documents (RFCs). Many of the documents relate to implementation and best practice, including adoptions of related protocols (e.g. ICMP), so that interoperability is possible in IPv6 networks, just as it is with IPv4.

Profiles are requirements documents. They describe the requirements necessary, recommended optional for IPv6 edge devices, network infrastructure, connectivity, and software. The requirement documents are an essential part of the assessment process for migration to IPv6. Often, the profiles are based on IETF standards and RFC documents. Use of the profiles (and conformance to any one of them) is only one step towards practical interoperability, as it depends also on the actual devices' configuration, and also vendor (in)compatibilities.

The development of profiles has been so useful that several have been developed. It is worth examining previous work in the development of profiles to see what they have provided, how they are different and what value public administrations in Europe can gain by using the profiles. In the next sections, we examine some major profiles in use around the world.

Requirements for IPv6 in ICT Equipment (ripe-554)

The Reseaux IP Europeens Network Coordination Centre (RIPE NCC) supports the technical coordination of Internet infrastructures within Europe. In this framework its IPv6 working group has developed “Requirements for IPv6 in ICT Equipment“. These requirements were documented in November 2010 in “ripe-501.” As of June 2012, an updated version of this document is available in “ripe-554”.

The ripe-544 document is broken into five major parts:

1. Proposed generic text for the tender initiator
2. Lists of mandatory and optional RFC standards support for hardware and software
3. Lists of required standards for distinct types of hardware
4. Requirements for IPv6 support in software
5. Skills requirements for systems integrator

The document is specifically targeted at people developing tender or acquisition documents for IT related equipment that needs to be IPv6 compatible. In the introduction to the document, the authors say,

> *“To ensure the smooth and cost-efficient uptake of IPv6 across their networks, it is important that governments and large enterprises specify requirements for IPv6 compatibility when seeking tenders for Information and Communication Technology (ICT) equipment and support. This document is intended to provide a Best Current Practice (BCP) and does not specify any standards or policy itself.*
>
> *It can serve as a template that can be used by governments, large enterprises and all other organisations when seeking IPv6 support in their tenders or equipment requirements and offer*

guidance on what specifications to ask for. It can also serve as an aid to those people or organisations interested in tendering for government or enterprise contracts."

The document is intended as a collection of best practices for the public sector and commercial companies alike.

Document ripe-554 also identifies the essential device classes: Switches (for end users or enterprises), routers, end systems, security devices (classified as either packet filters, application layer gateways, or intrusion detection systems), CPE routers, mobile devices, and load balancers. For each class it identifies mandatorily and optimally implemented RFCs. During procurement, devices should be preferred that implement most of the optional requirements, in addition to all the mandatory ones.

IPv6 Ready Logo Program of the IPv6 Forum

The IPv6 Ready program is a vendor-driven subprogram of the IPv6 Forum. It attempts to provide certification for IPv6 readiness for a variety of networking equipment. The IPv6 Ready program defines test specifications for IPv6 interoperability and conformance, self-test tools for monitoring conformance, and a certification system for labs that do conformance testing. In Europe, IRISA is an approved lab.

The IPv6 Ready Logo Program has established specifications for conformity tests and interoperability tests for IPv6 and related protocols:

- the IPv6 base protocol (including SLAAC, ICMP, addressing architecture, explicit congestion notification (ECN), Neighbor Discovery (ND) and Path MTU Discovery)
- IPsec and IKEv2
- Multicast Listener Discovery, Version 2
- SNMP MIBs
- Mobile IPv6 and NEMO
- DHCPv6
- SIP

The IPv6 Forum provides test suites for automated processing. A successful passing of such test suite authorizes a vendor to assign the IPv6 Ready logo to the tested devices series. There are eight dedicated IPv6 test centres, which offer conformity and interoperability testing as a service. However, the IPv6 Ready logo can also be awarded by the vendor to itself through a self-certification process, i.e. stating that a devices series has passed the IPv6 Ready tests successfully.

Those tests are - on purpose - incredibly detailed and comprehensive. They take into consideration the targeted role of the system under test, and sometimes go into detail. On the other hand, the number of referred RFCs in the IPv6 Ready tests is small (36 compared to more than 200 in other IPv6 profiles).

The IPv6 Ready tests include also only checks that can be verified using a standardized external interface. Internal variables, such as internal router states are not checked. Passing the IPv6 Ready tests does not automatically imply a fully correct implementation of a required feature.

A Profile for IPv6 in the U.S. Government

Like the RIPE document above, this document was prepared as an attempt to assist people in the US government specify IPv6 compatible equipment for acquisition. According to its abstract:

> *"This publication seeks to assist Federal agencies in formulating plans for the acquisition of IPv6 technologies. To achieve this, we define a standards profile for IPv6 in the USG that is intended to be applicable to all future uses of IPv6 in non- classified, non-national security federal IT systems. The standards profile is meant to: (a) define a simple taxonomy of common network devices; (b)define their minimal mandatory IPv6 capabilities and identify significant configuration options so as to assist agencies in the development of more specific acquisition and deployment plans; and, (c) provide the technical basis upon which future USG polices can be defined."*

This document, in version 1.0 from September 2008, has been developed by the United States National Institute of Standards and Technology (NIST) and has not been updated since 2008.

The document divides networked devices into end systems, routers, and security devices (packet filter, application-layer gateway, intrusion detection / prevention devices) and describes them as follows:

- Host: any Node that is not a Router. A Host's primary purpose is to support application protocols that are the source and/or destination of IP layer communication.
- Router: a Node that interconnects sub-networks by packet forwarding. A Router's primary purpose is to support the control protocols necessary to enable interconnection of distinct IP subnetworks by IP layer packet forwarding.
- Network Protection Device: Firewalls or Intrusion Detection / Prevention devices that examine and selectively block or modify network traffic.

The network-related features are categorized by it into 12 groups: Base features, routing, service quality, transition between IPv4 and IPv6, link-specific features, addressing, IPsec-related features, network management, multicast, mobility support, application level requirements, and special requirements for security devices.

The document then describes the compliance life cycle for IPv6 devices and discussions evaluation of compliance, accreditation bodies, test methods and how vendors can self-certify compliance with standards.

A problem with this profile is that it goes into significant detail concerning the devices' intended usage environment (use cases), and the relations between unique features, based on the defining RFC documents. This approach results in a quite complex document, because many features are required only conditionally, in dependence of others.

The document divides features into mandatory and optional ones. It does not value or prioritize the optional features, however. The document specifies for each feature which RFCs must be implemented to fulfil the desired functionality.

Department of Defense Unified Capabilities Requirements 2013 (UCR 2013)

This document, which was published in January 2013, provides an extraordinary set of requirements and capabilities for a variety of technologies. The goal of the document is to give a comprehensive view of requirements for all IT devices during procurement by the United States Department of Defence (DoD).

Section 5.2.2 is a mapping of RFCs to Unified Capability End Instruments. For every piece of IT equipment, it specifies the required, and optional IPv6 requirements for the US Department of Defence. The document contains a detailed device classification, and it identifies mandatory, recommended, and optional features based on the classification of devices into simple end system / simple server, router, security device (packet filter, application layer gateway), switch, and end system (or specific application).

The document not only lists the required RFCs themselves, but also lists demands on specific functions, and preferences on how given features should be used. In addition, in Section 5.2 of the document, a set of IPv6 requirements is given for every “Unified Capabilities” device – a list that is categorized by device type.

IPv6 Node Requirements

RFC 6434 (“IPv6 Node Requirements”), from December 2011, is an update to RFC 4294 (published in April 2006). It is foremost an informal summary and reference of all the fundamental IPv6 RFCs, their key features, and the relevance thereof. While not exactly a profile, the document divides networked devices into nodes, routers, and end systems. Unfortunately, the document does not regard transit systems (such as security devices without dedicated routing functionality) as a separate class, as all the profile documents mentioned before do. The document is incredibly old but the IETF is in the process of publishing an update in March of 2018. The new update also provides a much more current reference set for RFCs referred to in the requirements.

4 Technical Profiles, Part Two: Profiles for IPv6 hardware

Fundamentals

Fundamental requirements are common requirement profiles for all IPv6 hardware. All hardware in other categories must also abide with the requirements in this section.

There are the following profile categories in the fundamental requirements:

- IPv6 Foundation (profiles F.1 through F.5)
- IPv6 Addressing (profiles F.6 through F.15)
- DNS for IPv6 (profiles F.16 through F.25)
- Transition Mechanisms (profiles F.26 through F.30)
- Neighbour Discovery (profiles F.31 through F.40)
- IPsec Support (profiles F.41 through F.48)
- Key Exchange Mechanisms (profiles F.49 through F.56)
- Link-Layer Requirements (profiles F.57 through F.67)
- Multicast Support (profiles F.68 through F.76)

Figure 4.1: Profiles F.1 to F.15

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	IPv6 Foundation			
F.1		RFC 8200	IPv6 Specification	Mandatory
F.2		RFC 5722	Handling of Overlapping IPv6 Fragments	Mandatory
F.3		RFC 6437	IPv6 Flow Label Specification	Recommended
F.4		RFC 6540	IPv6 Support Required for All IP-Capable Nodes	Recommended
F.5		RFC 7381	Enterprise IPv6 Deployment Guidelines	Recommended[2]
	IPv6 Addressing			
F.6		RFC 2526	Reserved IPv6 Subnet Anycast Addresses	Mandatory[3]
F.7		RFC 3484	Default Address Selection	Mandatory
F.8		RFC 3736	Stateless DHCPv6	Optional
F.9		RFC 3879	Deprecating Site Local Addresses	Mandatory
F.10		RFC 4007	IPv6 Scoped Address Architecture	Mandatory
F.11		RFC 4193	Unique Local IPv6 Unicast Addresses (ULA)	Mandatory[4]
F.12		RFC 4291	IPv6 Addressing Architecture	Mandatory
F.13		RFC 4429	Optimistic Duplicate Address Detection	Optional
F.14		RFC 4862	IPv6 Stateless Address Autoconfiguration	Mandatory[5]
F.15		RFC 7934	Host Address Availability Recommendations	Recommended

[2] Note that the contents of RFC 7381 are guidelines that apply to all IPv6 deployments and not just transitional ones in public administrations

[3] For public administrations this requirement is only relevant for Mobile IP and it is unusual to implement this in public administration networks.

[4] See the companion IP Address Planning document from the ISA2 EC IPv6 project.

[5] Support for Stateless Address Autoconfiguration is essential.

Figure 4.2: Profiles F.16 to F.30

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	DNS for IPv6			
F.16		RFC 2617	DNS Message Extension Mechanism (EDNS0)	Mandatory
F.17		RFC 3226	DNSSEC and IPv6 Aware Messages Size Requirements	Mandatory
F.18		RFC 3596	DNS Protocol Extensions for Incorporating IPv6 DNS Resource Records	Mandatory
F.19		RFC 6106	IPv6 Router Advertisement Options for DNS Configuration	Recommended
F.20		RFC 4033	DNS Security Introduction and Requirements	Mandatory[6]
F.21		RFC 4034	Resource Records for the DNS Security Functions	Mandatory
F.22		RFC 4035	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence	Mandatory
F.23		RFC 6106	IPv6 Router Advertisement Options for DNS Configuration	Recommended
F.24		RFC 6781	DNSSEC Operational Practices, Version 2	Recommended
F.25		RFC 8198	Aggressive Use of DNSSEC-Validated Cache	Optional
	Transition Mechanisms			
F.26		RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers	Mandatory[7]
F.27		RFC 4380	Teredo: Tunnelling IPv6 over UDP Through NAT	Optional[8]
F.28		RFC 6343	Advisory Guidelines for 6to4 Deployment	Optional[9]
F.29		RFC 6877	464XLAT: Combination of Stateful and Stateless Translation	Mandatory[10]
F.30		RFC 7269	NAT64 Deployment Options and Experience	Optional[11]

[6] Support for DNSSEC is mandatory in IPv6-compatible equipment, but not necessarily implemented in public administrations. This document recommends DNSSEC implementation and suggests Profile F.24 as guidance for the operational practices of getting DNSSEC implementation in place.

[7] For public administrations, this requirement means that the transition mechanisms are required to be present; however, dual-stack mechanisms are mandatory, tunnelling and protocol translation (see the description earlier in this document) are optional.

[8] Teredo is not recommended for public administrations who are planning an initial transition to IPv6. See the discussion of transition mechanisms earlier in this document.

[9] This is a guidance document for those considering implementing 6to4 protocol translation (see Profile F.26)

[10] F.28 is a mandatory profile for those who have implemented tunnelling as part of the response to the basic transition mechanism requirement F.26.

[11] This is a guidance document for those considering protocol tunnelling.

Figure 4.3: Profiles F.31 to F.40

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Neighbour Discovery			
F.31		RFC 4861	Neighbour Discovery	Mandatory[12]
F.32		RFC 5942	IPv6 Subnet Model	Recommended
F.33		RFC 3971	DNS Protocol Extensions for Incorporating IPv6 DNS Resource Records	Mandatory
F.34		RFC 6106	IPv6 Router Advertisement Options for DNS Configuration	Recommended
F.35		RFC 4033	DNS Security Introduction and Requirements	Mandatory[13]
F.36		RFC 4034	Resource Records for the DNS Security Functions	Mandatory
F.37		RFC 4035	DNS Security (DNSSEC) Hashed Authenticated Denial of Existence	Mandatory
F.38		RFC 6106	IPv6 Router Advertisement Options for DNS Configuration	Recommended
F.39		RFC 6781	DNSSEC Operational Practices, Version 2	Recommended
F.40		RFC 8198	Aggressive Use of DNSSEC-Validated Cache	Optional

[12] Neighbour Discovery is an essential part of IPv6 deployment for every device on the network.

[13] Support for DNSSEC is mandatory in IPv6-compatible equipment, but not necessarily implemented in public administrations. This document recommends DNSSEC implementation and suggests Profile F.24 as guidance for the operational practices of getting DNSSEC implementation in place.

Figure 4.4: Profiles F.41 to F.56

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	IPsec Support			
F.41		RFC 4301	Security Architecture for the Internet Protocol	Mandatory
F.42		RFC 4302	IP Authentication Header	Mandatory
F.43		RFC 4303	IP Encapsulating Security Payload	Mandatory
F.44		RFC 4304	Extended Sequence Number for ISAKMP	Mandatory
F.45		RFC 4308	Cryptographic Suites for IPsec	Mandatory
F.46		RFC 5529	Modes of Operation for Camellia for Use with IPsec	Optional
F.47		RFC 5858	IPsec Extensions to Support Robust Header Compression over IPsec	Mandatory
F.48		RFC 7321	Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)	Recommended[14]
	Key Exchange Mechanisms			
F.49		RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2	Mandatory[15]
F.50		RFC 4555	IKEv2 Mobility and Multihoming Protocol	Optional[16]
F.51		RFC 5685	Redirect Mechanism for the Internet Key Exchange Protocol (IKEv2)	Mandatory
F.52		RFC 5723	Internet Key Exchange Version 2 Session Resumption	Mandatory
F.53		RFC 5996	IKEv2	Mandatory
F.54		RFC 7383	Internet Key Exchange Version 2 Message Fragmentation	Optional[17]
F.55		RFC 7427	Signature Authentication in the Internet Key Exchange Version 2	Mandatory
F.56		RFC 8019	Protecting Internet Key Exchange Protocol Version 2 Implementations from Distributed Denial of Service Attacks	Optional

[14] RFC 7321 is a guidance document which is updated by RFC 7634 to include the ChaCha20 and Poly1305 suites for IPsec. Those algorithms should be a mandatory part of all profiles.

[15] For public administrations, this requirement means that IKEv2 is a mandatory part of the profile for nodes, routers and infrastructure.

[16] Teredo is not recommended for public administrations who are planning an initial transition to IPv6. See the discussion of transition mechanisms earlier in this document.

[17] There are cases in public administrations where message fragmentation will not be allowed or be filtered at egress notes. In these cases, support for RFC 7383 is optional.

Figure 4.5: Profiles F.57 to F.76

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Link-layer Requirements			
F.57		RFC 2464	IPv6 over Ethernet	Mandatory[18]
F.58		RFC 2467	IPv6 over FDDI	Mandatory
F.59		RFC 2491	IPv6 over Non-Broadcast Multiple Access networks	Mandatory
F.60		RFC 2492	IPv6 over ATM Networks	Mandatory
F.61		RFC 3146	IPv6 over IEEE 1394 Networks	Mandatory
F.62		RFC 3572	IPv6 over MAAPOS (SONET/SDH)	Mandatory
F.63		RFC 4338	IPv6 and IPv4 over Fibre Channel	Mandatory
F.64		RFC 4919	IPv6 over Low-Power Wireless Personal Area Networks	Optional[19]
F.65		RFC 4944	IPv6 over 802.15.4 Networks	Mandatory
F.66		RFC 5072	IPv6 over PPP	Mandatory
F.67		RFC 5121	Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks	Mandatory
	Multicast Support			
F.68		RFC 2710	Multicast Listener Discovery for IPv6	Mandatory[20]
F.69		RFC 3590	Source Address Selection for the Multicast Listener Discovery Protocol	Mandatory
F.70		RFC 3810	Multicast Listener Discovery for IPv6 Version 2	Mandatory
F.71		RFC 4604	Using Internet Group Management Protocol Version 3 and Multicast Listener Discovery Protocol Version 2 for Source-Specific Multicast	Optional
F.72		RFC 6224	Base Deployment for Multicast Listener Support in Proxy Mobile IPv6 Domains	Optional
F.73		RFC 6516	IPv6 Multicast VPN Support Using PIM Control Plane and Selective Provider Multicast Interface Join Messages	Optional
F.74		RFC 7028	Multicast Mobility Routing Optimizations for Proxy Mobile IPv6	Optional
F.75		RFC 7287	Mobile Multicast Sender Support in Proxy Mobile IPv6 Domains	Optional
F.76		RFC 7371	Updates to the IPv6 Multicast Addressing Architecture	Mandatory

[18] For profiles in the link-layer requirements, the requirement is mandatory when the public administration is implementing that link-layer. Clearly, in cases where the link-layer was not in use by the public administration, the requirement is only optional.

[19] This document provides the background to running IPv6 on 6LoWPANs but does not provide protocol specifications.

[20] For profiles in the link-layer requirements, the requirement is mandatory when the public administration is implementing that link-layer. Clearly, in cases where the link-layer was not in use by the public administration, the requirement is only optional.

Edge Systems and Mobile Devices

In an IPv6 network, edge systems are those attached to the network that do not route or forward packets. They may be primarily client devices such as laptop computers, phones, tablets or other devices with human interfaces. They may also be small, low-powered sensors with highly constrained capabilities. They also may be servers such as mail servers, web servers or file and database sharing platforms. In these profiles, we distinguish edge systems that provide infrastructure services (for instance, a DNS server or a DHCPv6 server) from those that do not. The edge systems profiles are for those that do not provide infrastructure services.

In every case, the edge systems being profiled must abide by the mandatory recommendations of the fundamental profiles (F.1 through F.76 above).

There are the following profile categories in the Edge Systems and Mobile Devices requirements:

- Local Link Requirements (profiles E.1 through E.15)
- Mobility Support (profiles E.16 through E.22)
- Application Support (profiles E.23 through E.32)

Figure 4.6:

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Transition Mechanisms			
R.1		RFC 2473	Generic Packet Tunnelling and IPv6	Mandatory[21]
R.2		RFC 2784	Generic Routing Encapsulation	Mandatory[22]
R.3		RFC 2890	Key and Sequence Number Extensions to Generic Routing Encapsulation	Recommended
R.4		RFC 4798	Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)	Optional[23]
R.5		RFC 4891	Using IPsec to Secure IPv6 in IPv4 Tunnels	Recommended[24]
R.6		RFC 6180	Guidelines for Using IPv6 Transition Mechanisms during IPv6 Deployment	Advisory
R.7		RFC 6204	Basic Requirements for IPv6 Customer Edge Routers	Mandatory
R.8		RFC 6992	Routing for IPv4-Embedded IPv6 Packets	Optional
R.9		RFC 7084	Basic Requirements for IPv6 Customer Edge Routers	Mandatory
	System Management			
R.10		RFC 3414	SNMP User based Security Model	Mandatory
R.11		RFC 4087	IP Tunnel MIB	Mandatory[25]
R.12		RFC 4273	Managed Objects for BGP-4	Mandatory
R.13		RFC 4292	IP Forwarding Table MIB	Mandatory
R.14		RFC 4293	Management Information Base for the Internet Protocol (IP)	Mandatory
R.15		RFC 4295	Mobile IPv6 Management Information Base	Optional[26]
R.16		RFC 5643	MIB for OSPFv3	Optional[27]
R.17		RFC 6565	OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol	Optional

[21] Mandatory for SOHO and small office public administration routers.

[22] Mandatory for SOHO and small office public administration routers.

[23] Only in cases where inside/out approaches to transition are being implemented.

[24] In small office situations where encrypted VPNs are not in use for inbound connections, the public administration should treat RFC 4891 as mandatory.

[25] Mandatory in implementations where the router supports IP tunnelling actively.

[26] Mandatory in implementations where the router supports mobile IPv6.

[27] Mandatory in implementations where the router must support OSPFv3.

Figure 4.7:

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Local-Link Requirements			
R.18		RFC 3041	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	Mandatory
R.19		RFC 3122	Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification	Recommended
R.20		RFC 3736	Stateless Dynamic Host Configuration Protocol Service for IPv6	Mandatory
R.21		RFC 3775	Mobility Support in IPv6	Recommended
R.22		RFC 3971	Secure Neighbor Discovery	Recommended
R.23		RFC 4294	IPv6 Node Requirements	Optional[28]
R.24		RFC 4389	Neighbor Discovery Proxies	Recommended
R.25		RFC 4429	Optimistic Duplicate Address Detection for IPv6	Mandatory
R.26		RFC 5942	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	Advisory
R.27		RFC 6177	IPv6 Address Assignment to End Sites	Recommended
R.28		RFC 6434	IPv6 Node Requirements	Optional
R.29		RFC 6724	Default Address Selection for Internet Protocol Version 6	Mandatory
R.30		RFC 7217	A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration	Recommended
R.31		RFC 7404	Using Only Link-Local Addressing Inside an IPv6 Network	Advisory
R.32		RFC 7527	Enhanced Duplicate Address Detection	Recommended
	Router Security			
R.33		RFC 2711	IPv6 Router Alert Option	Optional
R.34		RFC 4191	Default Router Preferences and More-Specific Routes	Recommended
R.35		RFC 6105	IPv6 Router Advertisement Guard	Recommended[29]
R.36		RFC 7721	Security and Privacy Considerations for IPv6 Address Generation Mechanisms	Advisory

[28] See RFC 6434 for an update to these requirements.

[29] Also see RFC 6104: Rogue IPv6 Router Advertisement Problem Statement and RFC 7113: Implementation Advice for IPv6 Router Advertisement Guard.

Figure 4.8:

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Alternative Routing Protocols			
R.37		RFC 2080	RIPng for IPv6	Optional[30]
R.38		RFC 4552	Authentication/Confidentiality for OSPFv3	Mandatory
R.39		RFC 5308	Routing IPv6 with IS-IS	Mandatory
R.40		RFC 5310	IS-IS Cryptographic Authentication	Mandatory
R.41		RFC 5340	OSPF for IPv6	Mandatory
R.42		RFC 5838	Support of Address Families in OSPFv3	Recommended
R.43		RFC 6565	OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol	Optional

[30] RIPng is not recommended for public administration implementations of IPv6 networks.

Infrastructure Networking

In an IPv6 network, infrastructure networking provides services to the devices on the local link and often to devices on other links in the administration's enterprise network. Instead or providing routing for packets, these provide services in the network. These devices often act as servers for client requests such as DHCP or the DNS. In these profiles, we distinguish edge systems that provide infrastructure services (for instance, a DNS server or a DHCPv6 server) from those that do not. The Infrastructure Networking profiles are for those that provide infrastructure services.

In every case, the Infrastructure Networking devices being profiled must abide by the mandatory recommendations of the fundamental profiles (F.1 through F.76 above).

There are the following profile categories in the Infrastructure Networking requirements:

- DHCPv6 Services (profiles I.1 through I.9)
- DNS Services (profiles I.10 through I.14)
- RADIUS Services (profile I.15)
- Tunnel Broker Services (profile I.16)

Figure 4.9:

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	DHCPv6 Services			
I.1		RFC 3315	DHCPv6[31]	Mandatory
I.2		RFC 3319	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers	Mandatory
I.3		RFC 3646	DNS Configuration options for DHCPv6	Mandatory
I.4		RFC 3898	Network Information Service (NIS) Configuration Options for DHCPv6	Optional
I.5		RFC 4075	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6	Recommended
I.6		RFC 5908	Network Time Protocol (NTP) Server Option for DHCPv6	Advisory
I.7		RFC 5970	DHCPv6 Options for Network Boot	Optional[32]
I.8		RFC 6610	DHCP Options for Home Information Discovery in Mobile IPv6	Optional[33]
I.9		RFC 6939	Client Link-Layer Address Option in DHCPv6	Mandatory
	DNS Services			
I.10		RFC 2671	DNS Message Extension Mechanism (EDNSO)	Mandatory
I.11		RFC 3226	DNSSEC and IPv6 Aware Server/Resolver	Mandatory
I.12		RFC 3596	DNS Protocol Extensions for Incorporating IPv6 DNS Resource Records	Mandatory
I.13		RFC 6106	IPv6 Router Advertisement Options for DNS Configuration	Mandatory
I.14		RFC 6168	Requirements for Management of Name Servers for the DNS	Advisory
	RADIUS Services			
I.15		RFC 3162	RADIUS and IPv6	Optional[34]
	Tunnel Broker Services			
I.16		RFC 3053	IPv6 Tunnel Broker	Optional[35]

[31] RFC 4477 provides guidance to DNCP implementers who are deploying dual-stack solutions at the edge. Also, RFC 6334 provides guidance for DHCPv6's option for Dual-Stack Lite.

[32] In large public administration implementations where edge devices are supported with remote boot capabilities.

[33] For use in public administration small office settings where staff/clients have access to the network through small intelligent devices (tablets, smartphones, etc.)

[34] Only mandatory where RADIUS is implemented as part of a larger public administration implementation.

[35] Only mandatory in situations where a large public administration implementation requires the deployment of tunnel broker services.

Management Devices

In an IPv6 network a variety of management devices provide services to the network that focus on the management of the network rather than providing services to end nodes. These devices are different from those providing infrastructure services. Instead, these devices often provide security, access control and network management services. These services are sometimes unseen by the consumer/user of network services. The Management device profiles are different from the other profiles because they stress functionality rather than adherence to a standard.

We divide the Management Devices into three large groups: security devices, VPN (access) devices, and network management devices/services.

In every case, the Management devices being profiled must abide by the mandatory recommendations of the fundamental profiles (F.1 through F.76 above).

There are the following profile categories in the Infrastructure Networking requirements:

- DHCPv6 Services (profiles I.1 through I.9)
- DNS Services (profiles I.10 through I.14)
- RADIUS Services (profile I.15)
- Tunnel Broker Services (profile I.16)

Figure 4.10:

Profile	Profile Category	RFC for Specification	Profile Requirement	Recommendation
	Security Services[36]			
M.1			Configuration and management of the security service	Mandatory
M.2			Ability to filter network traffic based on protocol type (IPv4 or IPv6)	Recommended
M.3			AAA for security service access and configuration	Recommended
M.4			Auditing of both IPv4 and IPv6 traffic	Recommended
M.5			Backup services for the security service/device	Recommended
M.6			Load balancing for the security service/device	Recommended
M.7			Automated protection of the security service/device	Mandatory[37]
M.8			Packet analysis by the security service/device	Mandatory[38]
M.9			Fragmentation protection	Mandatory[39]
M.10			Handling of Encapsulated packets	Mandatory[40]
M.11			Handling of extension headers.	Mandatory
M.12		RFC 4890	Recommendations for Filtering ICMPv6 Messages in Firewalls	Mandatory

[36] Note the requirements in Appendix A; Section A.5

[37] The device/service must be able to protect itself against fragmentation attacks, DDOS attacks, attacks with excessively large extension headers, excessive IPv6 options, and manipulation of configuration settings.

[38] The device/service must support port/protocol and address blocking, stateful IPv6 header analysis, handling of packets protected with IPsec, and the ability to detect known attacks, port scanning, host scanning and stateful monitoring of half-open TCP/IP connections.

[39] The device/service must be able to handle and analyze fragmented IPv6 packets, auditing for sources of fragmented packets and the ability to reassemble fragmented packets for further analysis.

[40] The device service should be able to handle tunneled packets and do stateful analysis of IPv6 in IPv4 tunnels as well as IPv4 in IPv6 tunnels. The device/service must also be able to detect IPv6 in IPv6 encapsulation.

Appendix A: RIPE requirements for IPv6 Compatibility

A.1 Requirements for “host” equipment

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- DHCPv6 client [RFC3315] *
- SLAAC [RFC4862] *
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]
- If support for mobile IPv6 is required, the device must support “MIPv6” [RFC6275, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]

- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

A.2 Requirements for consumer grade "Layer 2 switch" equipment

Optional support (management)

- MLDv2 snooping [RFC4541]
- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]

A.3 Requirements for enterprise/ISP grade "Layer 2 switch" equipment

Mandatory support:

- MLDv2 snooping [RFC4541]
- DHCPv6 filtering [RFC3315]
- Router Advertisement (RA) filtering [RFC4862]
- Dynamic "IPv6 Neighbor solicitation/advertisement" inspection [RFC4861]
- Neighbor Unreachability Detection [NUD, RFC4861] filtering
- Duplicate Address Detection [DAD, RFC4429] snooping and filtering.

Optional support (management):

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]

- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- IPv6 Routing Header [RFC2460, Next Header value 43] filtering *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- UPnP filtering

A.4 Requirements for "router or Layer 3 switch" equipment

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- SLAAC [RFC4862] *
- MLDv2 snooping [RFC4541]
- Multicast Listener Discovery version 2 [RFC3810] *
- Router-Alert option [RFC2711]
- Path MTU Discovery [RFC1981] *
- Neighbor Discovery [RFC4861] *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- If a dynamic interior gateway protocol (IGP) is requested, then RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the equipment must comply with "Authentication/Confidentiality for OSPF-v3" [RFC4552]
- If BGP4 protocol is requested, the equipment must comply with RFC4271, RFC1772, RFC4760, RFC1997, RFC3392 and RFC2545
- Support for QoS [RFC2474, RFC3140]
- If support for tunneling and dual stack is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213]

- If support for tunnelling and dual stack is required, the device must support Generic Packet Tunnelling and IPv6 [RFC2473]
- If 6PE is requested, the equipment must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If mobile IPv6 is requested, the equipment must support MIPv6 [RFC6275, RFC5555] and "Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture" [RFC4877]
- If the IS-IS routing protocol is requested the equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]
- If MPLS functionality (for example, BGP-free core, MPLS TE, MPLS FRR) is requested, the PE-routers and route reflectors must support "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)" [RFC4798]
- If Layer 3 VPN functionality is requested, the PE-routers and route reflectors must support "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN" [RFC4659]
- If MPLS Traffic Engineering is used in combination with IS-IS routing protocol, the equipment must support "M-ISIS: Multi-Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)" [RFC5120]

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- Route Refresh for BGP-4 Capabilities [RFC2918]
- BGP Extended Communities Attribute [RFC4360]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Generic Routing Encapsulation [RFC2784]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 tunnels [RFC4891]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]

- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size Requirements [RFC3226]
- 127-bit IPv6 Prefixes on Inter-Router Links [RFC6164]
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

A.5 Requirements for "network security equipment”

Equipment in this section is divided into three subgroups:

- Firewall (FW)
- Intrusion prevention device (IPS)
- Application firewall (APFW)

For every mandatory standard the applicable subgroups are specified in parentheses at the end of the line.

Mandatory support:

- IPv6 Basic specification [RFC2460] (FW, IPS, APFW) *
- IPv6 Addressing Architecture [RFC4291] (FW, IPS, APFW)
- Default Address Selection [RFC3484] (FW, IPS, APFW)
- ICMPv6 [RFC4443] (FW, IPS, APFW) *
- SLAAC [RFC4862] (FW, IPS) *
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *
- Inspecting IPv6-in-IPv4 protocol-41 traffic, which is specified in: Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (IPS)
- Router-Alert option [RFC2711] (FW, IPS)
- Path MTU Discovery [RFC1981] (FW, IPS, APFW) *
- Neighbor Discovery [RFC4861] (FW, IPS, APFW) *
- If the request is for the BGP4 protocol, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545 (FW, IPS, APFW)
- If the request is for a dynamic internal gateway protocol (IGP), then the required RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol. (FW, IPS, APFW)
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)

- Support for QoS [RFC2474, RFC3140] (FW, APFW)
- If tunneling is required, the device must support Basic Transition Mechanisms for IPv6 Hosts and Routers [RFC4213] (FW)

A Network Security Device is often placed where a Layer 2 switch or a router/Layer 3 switch would otherwise be placed. Depending on this placement those requirements should be included.

Functionality and features that are supported over IPv4 should be comparable with the functionality supported over IPv6. For example, if an intrusion prevention system is capable of operating over IPv4 in Layer 2 and Layer 3 mode, then it should also offer this functionality over IPv6. Or if a firewall is running in a cluster capable of synchronising IPv4 sessions between all members of a cluster, then this must also be possible with IPv6 sessions.

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- DHCPv6 client/server/relay [RFC3315] *
- Extended ICMP for Multipart Messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- Stateless DHCPv6 [RFC3736] *
- DHCPv6 PD [RFC3633] *
- BGP Communities Attribute [RFC1997]
- BGP Capabilities Advertisement WITH-4 [RFC3392]
- (QOS) Assured Forwarding [RFC2597]
- (QOS) Expedited Forwarding [RFC3246]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- Cryptographically Generated Addresses [RFC3972]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- Using IPsec to Secure IPv6-in-IPv4 Tunnels [RFC4891] (FW)
- OSPF-v3 [RFC5340]
- Authentication/Confidentiality for OSPF-v3 [RFC4552]
- Generic Packet Tunneling and IPv6 [RFC2473]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- DNS extensions to support IPv6 [RFC3596]
- DNS message extension mechanism [RFC2671]

- DNS message size requirements [RFC3226]
- Using IPSec to Secure IPv6-in-IPv4 Tunnels [RFC4891]
- Multicast Listener Discovery version 2 [RFC3810] *
- MLDv2 snooping [RFC4541] (when in L2 or passthrough mode) *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

A.6 Requirements for CPE equipment

Mandatory support:

- RFC6204 (Basic Requirements for IPv6 Customer Edge Routers) *

Optional support:

- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- If support for mobile IPv6 is required, the device needs to comply to “MIPv6” [RFC6275, RFC5555] and “Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture” [RFC4877]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- SLAAC Privacy Extensions [RFC4941]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) [RFC5969]
- Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion [RFC6333] If support this then also must support Dynamic Host Configuration protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite [RFC6334]
- The A+P Approach to the IPv4 Address Shortage [RFC6346]
- IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5739]
- IPv6 Host-to-Router Load Sharing [RFC4311]

- Default Router Preferences and More-Specific Routes [RFC4191]

A.7 Requirements for mobile devices

Mandatory support:

- IPv6 basic specification [RFC2460] *
- Neighbor Discovery for IPv6 [RFC4861] *
- IPv6 Stateless Address Autoconfiguration [RFC4862] *
- IPv6 Addressing Architecture [RFC4291] *
- ICMPv6 [RFC4443] *
- IPv6 over PPP [RFC2472]
- Multicast Listener Discovery version 2 [RFC3810] *
- IPv6 Router Alert Option [RFC2711]
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]

Optional support:

- Privacy Extensions for Stateless Address Autoconfiguration in IPv6 [RFC4941]
- Path MTU Discovery for IPv6 [RFC1981] *
- Generic Packet Tunneling for IPv6 [RFC2473]
- DHCPv6 [RFC3315] *
- Stateless DHCPv6 [RFC3736]
- DHCPv6 option for SIP servers [RFC3319]
- IPv6 Prefix Options for DHCPv6 [RFC3633]
- Prefix Exclude Option for DHCPv6-based Prefix Delegation [draft-ietf-dhc-pd-exclude]
- Default Address Selection [RFC3484]
- IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] *
- IKEv2 Mobility and Multihoming Protocol MOBIKE [RFC 4555]
- IPv6 Host-to-Router Load Sharing [RFC4311]
- Default Router Preferences and More-Specific Routes [RFC4191]

References:

- 3GPP
- Internetworking Between Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN) [3GPP TS 29.061]
- GPRS Service Description [3GPP TS 23.060]

- General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access [3GPP TS 23.401]
- Signaling flows for IP multimedia Call control based on SIP and SDP [3GPP TS 24.228]
- IP multimedia call control protocol based on SIP and SDP [3GPP TS 24.229]
- IP Based Multimedia Framework [3GPP TS 22.941]
- Architectural Requirements [3GPP TS 23.221]
- Packet domain; Mobile Stations (MS) Supporting Packet Switching Service [3GPP TS 27.060]
- IPv6 migration guidelines [3GPP TR 23.975]
- IETF
- IPv6 for Some Second and Third Generation Cellular Hosts [RFC3316]
- Recommendations for IPv6 in 3GPP Standards [RFC3314]
- IPv6 in 3rd Generation Partnership Project (3GPP) [RFC6459]

A.8 Requirements for load balancers

A load balancer distributes incoming requests and/or connections from clients to multiple servers. Load balancers will have to support several combinations of IPv4 and IPv6 connections:

- Load balancing IPv6 clients to IPv6 servers (6-to-6) must be supported
- Load balancing IPv6 clients to IPv4 servers (6-to-4) must be supported
- Load balancing IPv4 clients to IPv4 servers (4-to-4) should be supported
- Load balancing IPv4 clients to IPv6 servers (4-to-6) should be supported
- Load balancing a single external/virtual IPv4 address to a mixed set of IPv4 and IPv6 servers should be supported
- Load balancing a single external/virtual IPv6 address to a mixed set of IPv4 and IPv6 servers should be supported

If a load balancer provides Layer 7 (application level / reverse proxy, defined as ‘surrogate' in section 2.2 of RFC3040) load balancing then support for the X-forwarded-for (or equivalent) header in HTTP must be provided in order to make the source IP address of the client visible to the servers.

Mandatory support:

- IPv6 Basic specification [RFC2460] *
- IPv6 Addressing Architecture [RFC4291] *
- Default Address Selection [RFC3484]
- Unique Local IPv6 Unicast Addresses (ULA) [RFC4193]
- ICMPv6 [RFC4443] *
- Path MTU Discovery [RFC1981] *

- Neighbor Discovery [RFC4861] *
- DNS protocol extensions for incorporating IPv6 DNS resource records [RFC3596]
- DNS message extension mechanism [RFC2671]
- DNS message size requirements [RFC3226]
- Deprecation of Type 0 Routing Headers in IPv6 [RFC5095] *

Optional support:

- IPv6 Router Advertisement Options for DNS Configuration [RFC6106]
- Extended ICMP for multi-part messages [RFC4884]
- SeND [RFC3971]
- DS (Traffic class) [RFC2474, RFC3140]
- Cryptographically Generated Addresses [RFC3972]
- SNMP protocol [RFC3411]
- SNMP capabilities [RFC3412, RFC3413, RFC3414]
- SNMP MIBs for IP [RFC4293] Forwarding [RFC4292] and DiffServ [RFC3289]
- Multicast Listener Discovery version 2 [RFC3810] *
- Packetisation Layer Path MTU Discovery [RFC4821]
- NAT64/DNS64 [RFC6146, RFC6147]
- If support for IPsec is required, the device must support IPsec/IKEv2 [RFC4301, RFC4303, RFC4302, RFC5996] * and Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2) [RFC5685]
- If support for BGP4 is required, the equipment must comply with RFC4271, RFC1772, RFC4760 and RFC2545
- If support for a dynamic internal gateway protocol (IGP) is required, the RIPng [RFC2080], OSPF-v3 [RFC5340] or IS-IS [RFC5308] must be supported. The contracting authority shall specify the required protocol.
- If OSPF-v3 is requested, the device must support "Authentication/Confidentiality for OSPFv3" [RFC4552] (FW, IPS, APFW)
- IPv6 Host-to-Router Load Sharing [RFC4311] (FW)
- Default Router Preferences and More-Specific Routes [RFC4191] (FW)

A.9 Requirements for IPv6 support in software

All software must support IPv4 and IPv6 and be able to communicate over IPv4-only, IPv6-only and dual-stack networks. If software includes network parameters in its local or remote server settings, it should also support configuration of IPv6 parameters.

All features that are offered over IPv4 must also be available over IPv6. The user should not experience any noticeable difference when software is communicating over IPv4 or IPv6, unless this is providing explicit benefit to the user.

It is strongly recommended not to use any address literals in software code, as described in “Default Address Selection for Internet Protocol version 6” [RFC3484].