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

This document provides a combination of resources for IPv6 address planning and implementation for public administrations.

It beings with a section discussing approaches to planning for IPv6 implementation in public administrations. Three major options are explored and then the methodology for completing the planning work is outlined.

Address planning is an important part of IPv6 implementation work, and a separate companion document provides a guide to doing an IPv6 address plan, how to implement it, how to acquire IPv6 addresses, and the relationship between public administrations and the Regional Internet Registry that serves the European region.

In this document we continue with a discussion of the main transition approaches for moving from existing networks to IPv6 networks. We provide a pair of scenarios for smaller and larger public administrations that are considering making the move from IPv4 networks to IPv6 networking.

Next we examine the issue of readiness. Several previous attempts have been made at developing profiles for IPv6 readiness. We examine profiles built by the RIPE NCC, by the German government, by the US government and also a logo/readiness program. The profile build for the United States Department of Defense is extremely detailed but out of date. The profiles build by RIPE NCC are useful but haven't been updated for years.

Next, we provide up-to-date technical profiles for IPv6 readiness for a variety of equipment and services in an IPv6 network. The goal is to give the public administration an assessment tool for what is needed to move to IPv6. Particular requirements or profiles are grouped into categories – one of the most important being the Fundamental category which is common to all nodes, devices and services that move to IPv6.

Finally, we provide, as an appendix, the RIPE Requirements for IPv6 Compatibility. This is provided for information and comparison purposes. People considering a transition to IPv6 in public administrations in Europe can consider the Technical Profiles provided here in combination with other profiles. In a companion document, we suggest a methodology for requiring support and assessing readiness for IPv6 compatibility.

One of the fundamental requirements for moving public administrations to IPv6 is the ability to assess readiness for the transition to IPv6. Key to that assessment are the profiles that determine IPv6 compatibility. This document describes the key transition technologies and gives a current view of the profiles needed in a public administration for compatibility.

1 Planning for IPv6 in Public Administrations

Planning for IPv6 in Public Administrations is a complex task. For many governments the reasons for introducing IPv6 into their network are different from the reasons for introducing it into public facing services such as web sites and email services. Budget, administrative control and IT support all determine the approach that use to plan for IPv6 in internal network.

In this document, we discuss planning for IPv6 in Public Administrations. We then provide guidelines for doing assessments of IPv6 readiness. Finally we provide technical profiles to assist in the IPv6 audit and to assist in planning a stepwise approach to IPv6 deployment.

The approach in this paper assumes that a public administration has four main areas of interest for IPv6 deployment:

- The core / backbone network that connects the public administration’s resources together;
- The customer/citizen/regulated entity facing network;
- The internal public administration user network; and,
- The public administration’s data centre.

Planning for IPv6 in Public Administrations may mean all of these – or, it may mean that only one or two are taken on as a requirement. For instance, a public administration may choose to have its external services move immediately to IPv6 and dual stack support, while delaying IPv6 deployment for its internal services and network.

It is also possible that external events make IPv6 transition a possibility. For instance, a data centre move might be an impetus for deploying IPv6 in that part of a network. The opportunity to move to IPv6 as part of a physical migration might save a lot of costs for a later migration – which would eventually have to happen anyway.

The four areas of interest above do not represent equal challenges. It is well-understood that implementing IPv6 for customer/citizen/regulated entity facing services is much easier to complete than a migration for the government’s internal network. Deploying IPv6 in an internal network may be a major task that takes three or more years in governments that are migrating at national, regional and local levels at the same time.

For government networks, integrating IPv6 for public-facing services is often the first step. It is also considered a good approach because it is one of the easier stages of integration. Starting with an easier step allows the public administration to use that part of the migration to gather experience and better prepare to tackle the other IPv6 migration tasks that have a higher level of complexity.

Three Approaches: Inside-Out

In public administrations where there is sufficient time and budget, IPv6 migration is possible to plan from the core network out to the public facing services. In general, the core network equipment has the longest history of implementation and the largest likelihood of native IPv6 support. As a result the IPv6 stacks on core network equipment is more mature and the government can often deploy with the least upgrade effort.

In this approach, the complexity of IPv6 integration increases as you move away from the core and toward the edge of the government network. Stacks on network appliances, databases, utility and application software might be less mature or have implementations that are either unavailable or in an early, buggy state. For public administrations that rely on third-party services or applications, vendor support might be in its early stages as well.

Another important advantage of the inside/out approach is that while you work on deployment at the core, the critical government and citizen traffic will still flow over the IPv4 infrastructure and so the IPv6 migration can take place with limited risk and pressure. Implementers can also use the core migration to implement management and security tools and test all aspects of the IPv6 management structure before government and citizen traffic is involved.

Three Approaches: Outside/In

Starting IPv6 migration at the edge is the easiest way to roll out IPv6 to customers quickly. It could be a case where you have a limited supply of IPv4 addresses and are unable to meet growth requirements in an IPv4 setting. It could also be a case where you are deploying an application that requires IPv6.

It is important to understand that the risks to the migration project always increase when you choose this approach. For many public administrations, avoiding this approach when sufficient time and budget is available, is the best course of action. In choosing the outside/in model for migration, urgency is always a critical factor. The risks and costs of this approach are higher because the migration is starting where the complexity is highest. The government adopting this approach will almost always face challenges with interoperability issues and unexpected bugs. It is also critical to understand that this approach enables government user and citizen traffic over the public administration’s network before they have had time to carefully build and test that infrastructure.

Three Approaches: IPv6 Islands

It is also possible to build a migration approach that supports specific applications, customers, or parts of a network as a first step. This can be an approach where “islands” of IPv6 deployment take place in support of particular requirements and tunnels are used to carry IPv6 traffic over IPv4 subnets to interconnect the IPv6 islands.

This is often an approach where economic and budgetary considerations dictate the migration strategy. While it reduces the scope of the migration, it puts off the challenges of supporting IPv6 in the core of the government’s network. It is an approach that is used where there is a specific service, application or technology that requires IPv6, but where the government is not ready to do a full roll out of IPv6 services.

Islands have the advantage of being able to be used as trials in a controlled environment that limit the impact and risks of deployment.

Governments that use external services, such as web hosting or content delivery networks, can work with the provider of those services to enable IPv6. This takes advantage of any IPv6 implementation experience that the service provider has without much in the way of cost to the public administration.

The disadvantage of an island-based approach is that it means that the government has to manage a heterogeneous network, which always increasers operational cost and carries a higher risk of misconfiguration and errors.

High-Level IPv6 Implementation Planning

Planning for IPv6 is not just a network or IT project. It is a multidimensional effort and best practice shows that a comprehensive approach to planning is essential to its success. Because IP addressing and networking is a foundation technology, IPv6 will touch all aspects of the IT ecosystem. The network is the platform that ties together people, services, devices and information resources. The network also facilitates communication amongst people, people's use of services and devices, and their access to information. The network also enables devices to communication with each other (for instance, in the Internet of Things). IPv6 is not just about network infrastructure; it is about all these components and their interactions.

At a high level it is also important to understand that the migration to IPv6 also involves planning for co-existence with IPv4 over a period of time. Since a public administration rarely knows when they will know when (or, if) they will be turning off IPv4 networking, the need to plan for co-existence is essential.

IPv6 Implementation Planning: Defining Objectives

As we have seen in the three approaches to migration above, the impact of IPv6 adoption depend on the scope of the integration. Eventually IPv6 will become a dominant part of the government networking landscape – however, the initial steps in its integration may vary in terms of depth and coverage. For instance, some governments might decide to delay IPv6 migration and deployment and simply update their security policies and monitoring/management capabilities to deal with potential IPv6 threats. Other governments might fully commit to IPv6 and plan a complete and comprehensive strategy for migration throughout all of the IT environment.

Defining the objectives for an IPv6 migration includes four key features:

- Alignment with strategic objectives of the administration;
- Establishment of project goals;
- Establishment of the project's scope; and,
- A project timeline.

Alignment with Strategic Objectives

Any public administration that considers and IPv6 migration should ensure that the implementation has strategic value to the organization. This alignment requires an understanding of both the government's objectives and the capabilities of the new technology. For instance, IPv6 migration may not have immediate and short-term return on investment, but it may be the foundation for other, more significant changes over time.

Establishment of Project Goals

The goals of an IPv6 migration are essential in defining the resources that are needed for its planning and later for its implementation. There are multiple options and they are often specific to the way a government is organized or the way programs and services are delivered to citizens or government users. For public administrations, project goals for IPv6 can vary widely. Examples might include:

- Launch of an individual, targeted project for which IPv6 is not yet important, but for which security policies and monitoring capabilities must be updated to address the presence of IPv6-capable devices; or,
- Establish a governmental test environment for protocol, application, security and equipment evaluation; or,
- Deploy a single application in a government setting that runs over IPv6; or,
- Ensure that end-user devices (computers, tablets, mobile devices) are dual-stacked by default; or,
- Integrate new devices in the government network such as sensors or intelligent devices that require IPv6.

The clear definition of project goals leads to well-defined success criteria and the means for tracking the progress of the project toward meeting them.

Establishment of Project Scope

The goals of the project (above) identify the IT environment elements that would be involved in the IPv6 migration. The scope is a measure of the extent of the project. For example, a government that is ready to interface with regional IPv6 ISPs required localized coverage; but a government distributing video nationally via IPv6 requires national scope.

The project scope can be described in terms of geography (specific localities or regions), network infrastructure elements (home office, small office, campus or core), infrastructure elements (public wireless, broadband, cars, planes, ships, trains), services (content delivers, VoIP), and policies or standards.

We will see later in this document (in the Technical Profiles section) that the IPv6 migration can touch all parts of a government's IT environment:

- Applications
- Information
- Computing platforms
- Networking
- Infrastructure services
- Processes
- Standards
- Governance

Project Timeline

Complete migration to an IPv6-only network will probably take a long time and is likely to be achieved by multiple projects or a single, multithreaded project. Similar to any other technology integration project, planning of each step has to meet the delivery dates while taking into consideration multiple timelines, some under the control of the unit of government, and some not. These include:

- Budget cycle
- Equipment refresh schedules
- Equipment and software certification cycles
- Timelines of related projects
- Manufacturer product and feature delivery schedules
- Technology standards development and adoption

The importance of these various timelines should not be underestimated, because they can significantly impact a government's ability to implement the IPv6 project in time to meet business needs.

IPv6 Implementation Planning: Project Plan Development

There are many approaches to developing an IPv6 transition plan, but the process advocated here is one that can scale from local government initiatives, to national IPv6 migration plans. The steps are the same in either case. We suggest that there are five major steps to developing an IPv6 transition plan for public administrations:

- Assess the current state of the environment;
- Define the future state (the objective);
- Perform a gap analysis (the distance from current state to future state);
- Develop a strategy to achieve the future state; and,
- Prioritize activities while being aware of external dependencies.

This document provides recommendations for each of these steps in developing an IPv6 transition plan. We pay special attention to the assessment of the IT environment: later in this document there is a section on Technical Profiles that attempts to provide a systematic approach to providing this assessment.

Project Plan Development: Assess the IT Environment

Once the strategic business perspective on the IPv6 migration is established and the scope of the project is clear, the next step is to understand the environment in which IPv6 is to be deployed. This is an analysis of the existing IT landscape. Where a government has existing processes for IT projects, many aspects of the IPv6 integration can be covered through minor changes in existing government processes. Established processes and procedures for technology changes should be used to the extent possible.

The assessment process corresponds to a deep analysis of the "Internet deployment" in the public administration. To many governments see this as simply an inventory of the network devices to evaluate their readiness to support required IPv6 features. Instead, the process is often more complex than that – the evaluation of the transport infrastructure is sometimes the least complex aspect of the plan.

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. All these elements of the IT infrastructure, and the policies governing them, must be inventoried in order to understand what they need to support IPv6.

As an example, for device assessment purposes we divide the assessment into possible outcomes:

- The device is currently capable of supporting IPv6 features; hardware and software upgrades are not required.
- The device is running software that supports IPv6 features, but hardware (memory) upgrades are required.
- The device is currently capable of supporting IPv6 in hardware, but a software upgrade is required. Both hardware (memory) and software upgrades are required to support IPv6.
- The device is not capable of supporting IPv6 services.
- The analysis was unable to determine the device's capability to support IPv6; further analysis is required.

When we examine Technical Profiles later in this document, it will become obvious that the assessment can clarify the scope of the government's IPv6 deployment project. The public administration may find that it needs to adjust the roadmap or timeline. It may also find that it can provide a more detailed analysis of potential costs for the project. Some of the finding during assessment may also have an impact on the integration plans for deployment. For instance a service that may have been assumed to work in a dual-stack environment may be found to require replacement.

As a general rule, IPv6 compatibility in applications is often a bigger problem for governments than IPv6 compatibility in network equipment. As governments use more custom-developed, or highly customized in-house applications, the higher the chance that they will not immediately work with IPv6. The assessment for software and software based services is just as important as the assessment for network equipment.

The assessment is also an opportunity to evaluate third-party vendor portfolios. Whether or not a device, service or application has the required IPv6 support might not be the only criterion for success. Instead, the public administration may want to find out what the third-party vendor's plan, or roadmap, for up-to-date IPv6 support will be in the future. In particular, core network devices and services that have a very long lifetime – such as core routers, firewalls, management and monitoring tools and other infrastructure (DNS, DHCP, IPAM) – need a vendor who guarantees high performance products and a good, future development roadmap.

In an assessment of a government's ISP, it is not sufficient to ask for basic IPv6 connectivity. The public administration will want to know what kind of connectivity they are getting: is it tunneled or native transit? The government will also want to know information about the ISP's peering connection to the rest of the public IPv6 Internet.

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.

Project Plan Development: Future State and Gap Analysis

A clear definition of the future state of the migration is essential. Even prior to the assessment step, we have seen that a clear definition of the project goals is essential to the success of the project. Almost every IPv6 project will find that, after the assessment is completed, there needs to be some adjustment of the anticipated future state – or, final objective – of the transition project.

Later in this document – in the Technical Profiles section – we will see examples of a Feature/Product matrix that examines the platforms and services that went through the assessment and the IPv6 capabilities on the other axis. The matrix can then be used to evaluate that the platforms have the correct hardware or software to support the desired features of the future state of the network.

It is those platforms that have deficiencies in the matrix that become the subject of a gap analysis. Once a public administration determines what platform and feature combinations are required for the IPv6 migration, they can document the configurations needed to achieve the desired IPv6 support goal.

It is this gap analysis that forms the bridge between “what needs to be done” and “how to get it done.”

Project Plan Development: Strategy to Achieve the Future State

The outcome of the assessment 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; and,
- 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. Whether an inside/out, outside/in, or island approach is being envisioned, the matrix provides the source material for building a plan that gets to the desired state of the network.

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: Prioritize Activities

Since governments and units of public administrations often have existing processes for IT projects, there is no need to create new processes to support IPv6 deployment. Instead, it is 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

Part of the Technical Profile for a public administration depends upon the transition approach being used. In this section we consider two different scenarios for public administration transition. Then we discuss specific technologies that make transition to IPv6 possible.

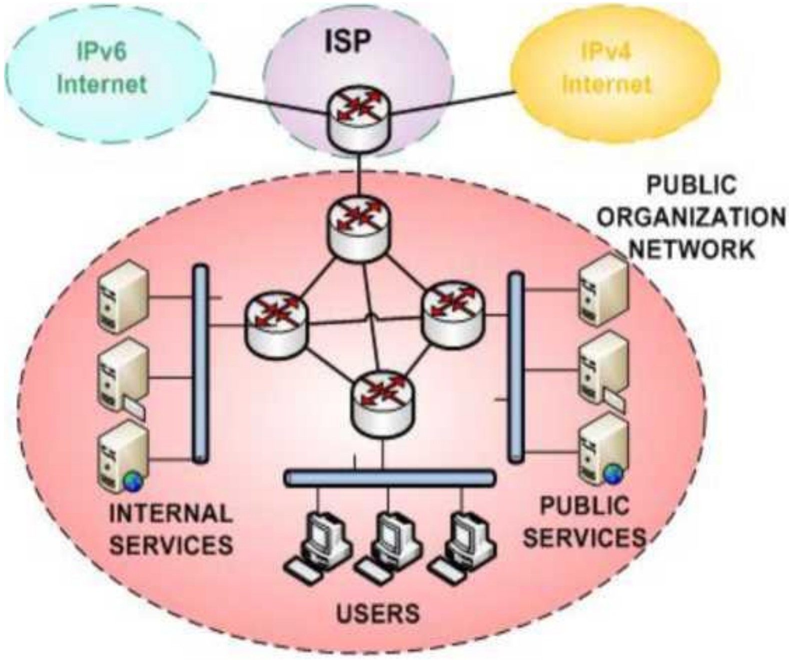
Scenarios for Public Administrations

Small Network, Limited Geographic Distribution

This scenario is for a public administration that is small in size. The network under consideration is not very big and it does not spread over large-scale geographic areas. Often, small networks are part of a larger administrative agency or ministerial department. The larger organization often provides the connectivity service.

An example of this scenario is a local University that has its own campus network, but whose connectivity is provided by a national network or through commercial ISPs. In this case the University would have a single connection to the public Internet and it would use that connection for both access to IPv4 and IPv6.

The following figure shows this scenario:

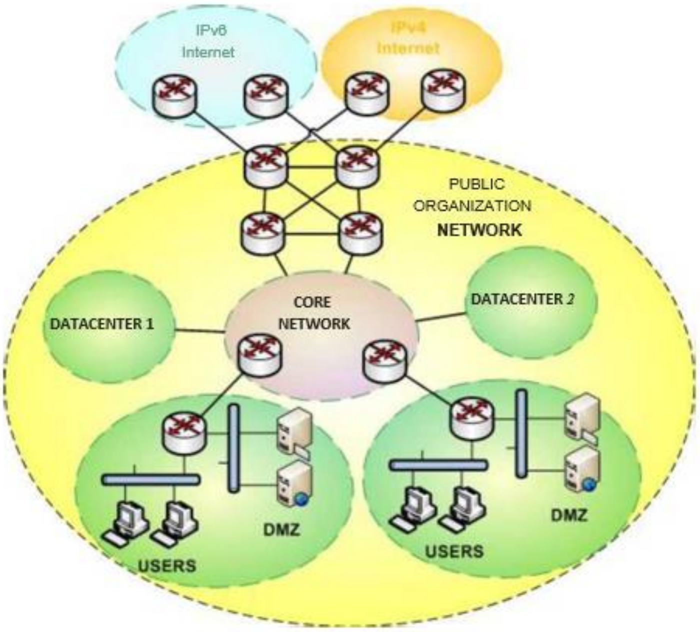


National Network, Broad Geographic Distribution

This scenario is for a public administration that is distributed over a large region or entire nation. The network (especially a national one) could provide connectivity for other organizations and departments. Examples of these happen in many countries in Europe. For instance, the 1990's saw the emergence of National Research Networks in many countries that later evolved into national networks for use by public administrations. Several nations in Europe run their own governmental network that supports both governmental departments and also local institutions throughout the country.

In this approach it is the government's network (not the ISP) that is connected to the public Internet and makes available both IPv4 and IPv6 services.

The following figure shows this scenario:



Transition mechanisms overview

As we saw earlier in this document there are three approaches to deployment:

- IPv4 only where legacy applications and services are allowed to be gradually removed from service. These are networks where the cost of transition is too high or impossible because of the failure of a vendor to provide IPv6 support;
- IPv4 and IPv6 together where the coexistence of both protocols provides a transitional period for moving from IPv4 to IPv6 through inside/out or outside/in deployment plans; and,
- IPv6 only networks where further transition is no longer required. In the IPv6 only networks there may need to be requirements for legacy access to the IPv4 Internet and services.

Transition Mechanisms: Dual-stack

The dual stack-strategy is the most common approach to transition and is often a preference in public administration networks. The approach is based on adding IPv6 capabilities to the network stack of IP devices, allowing them to be able to process IPv4 and IPv6 packets at the same time. This means that the device, which is running both stacks, is able to have both protocol versions work in parallel in the same network. All operating systems that are currently in widespread use on PCs, servers, smart phones and tablet computers, already support IPv4/IPv6 dual stack operation.

It is worth noting that there are different ways to implement a dual stack solution. For instance, mobile phones often only support IPv6 on the wireless interface and not across the 3G network (however, support for IPv6 is required in 5G and LTE networks). IPv6 support in software applications varies widely and needs to be checked. In some cases, IPv6 support is being dictated by external forces. As an example of this, all apps being sold in the Apple Store for iOS are required to support the IPv6 stack.

For dual-stack to work in an end-to-end environment, the IT infrastructure must provide full support for both IPv4 and IPv6 at the network layer. This means that no matter how the data-link and physical layers are provided (connectivity layers), the network layer must support both IPv4 and IPv6. In practice, this means that the typical functions provided for IPv4-based network must also be provided by the IPv6 network. These include:

- IP addresses and IP address management
- IP packet forwarding
- IP routing (where applicable)
- IP packet filtering (in firewalls and end systems)
- Application-specific gateways (also termed: application-level gateway - ALGW)

We will discuss tunnels in a later section, but tunnels make it possible to transport IPv6 packets over IPv4 connections. This is an alternative to dual-stack approaches when there are intermediate network paths that do not support IPv6.

Taking advantage of dual-stack solutions requires significant planning for networks and applications. As we have seen, modern end-user devices are already almost always implemented with both IPv4 and IPv6 stacks. However, the network and application layers are not always as easy to depend upon. In fact, care must be taken to not compromise existing functionality when moving to a dual-stack solution in the network. There are situations where, due to dependencies, the network or application layer determine if an inside/out or outside/in approach to transition would be most effective.

A detailed technical overview of IPv4/IPv6 dual stack operation and related transition techniques can be found in RFC4852 : "IPv6 Enterprise Network Analysis IP Layer 3.“

The advantage of dual-stack approach is that it is an effective long-term solution. The migration strategy for dual-stack means that the work to implement IPv6 at the network and application layers will remain valuable even as the network moves to an IPv6-only solution. This is advantage is so significant that many public administrations choose dual-stack as the default option for IPv6 migration. Using the dual-stack approach, services could be made available to users gradually – in an evolutionary way. For example, using the DNS, applications could decide which protocol version to use – in the case that IPv6 services were available and network support were available, the end device could decide to use IPv6 as the preferred network layer. In fact, many residential and business customers who use broadband already do this in a completely transparent way.

The disadvantages of the dual-stack approach is that it depends on IPv6 support at both the network and application layer. This is not nearly as easy as providing dual-stack support in edge devices. Dual-stack also adds overhead to all the network devices where it is implemented. Support for dual-stack approaches often means that network devices need to have upgrades for memory or changes in line cards. Dual-stack applications also require upgrades to software libraries and sometimes have large memory footprints.

Transition Mechanisms: Tunnels

Dual-stack approaches are often preferable for public administrations. However, there are situations where an organization is simply unable to implement dual-stack style transition mechanisms. In this case, one of the alternatives is an encapsulation technique where one version of the Internet Protocol is encapsulated inside of the other. This is possible in both directions: IPv6 into IPv4 or IPv4 into IPv6. This encapsulation technology is mature and well-understood.

There are two kinds of tunnelling supported in the modern IPv6 Internet:

- Automatic tunnels, where IPv6 packets use a gateway that is located on a special router that does the encapsulation. The advantage is that the links between the IPv6 aware routers do not need to be set up in advance.
- Manually configured tunnels, where the tunnel endpoints are manually configured at the routers which do the encapsulation and decapsulation.

There are a wide variety of IPv6 transition tunneling technologies. Many technologies have appeared to try to solve the problem of IPv6 transition when dual-stack approaches are not available.

6to4

6to4 is a tunnelling strategy that allows separate IPv6 networks to exchange packets without setting up an explicit, manually configured tunnel. In 6to4, specially prepared routers, called 6to4 routers, provide gateways between the IPv6 networks. The IPv6 packets are encapsulated inside an IPv4 packet at the gateway.

Features

- Automatic establishment
- Usually from router to router

Advantages

- Very good scalability
- Automatic tunnel service discovery
- Good support on commercial platforms

Disadvantages

- Poor security

- Difficult to manage
- Client needs a public IPv4
- IPv6 Prefix defined for clients
- Asymmetric model
- Not reliable

6rd

6to4 has some significant problems in practice. First, it relies on the 6to4 prefix to find 6to4 routers. However, the 6to4 prefix is not globally routable on the IPv6 Internet, which means that nodes on some parts of the IPv6 Internet cannot reach 6to4 networks or nodes. 6to4 also has a number of security issues that are difficult to mitigate leaving some network operators to block 6to4 traffic (resulting in the previous problem).

Features

- Automatic establishment
- Based in 6to4 but inside an ISP and with some changes
- Anycast IPv4 addresses

Advantages

- Security supported (same as for IPv4)
- An ISP's own prefix could be used
- Very good scalability
- Automatic tunnel service

Disadvantages

- Site needs a software change in the CPE
- A new element is needed:
- 6RD relay, with little support by vendors (although improving)

ISATAP

Another approach to automatic tunnelling is the Intra-Site Automatic Tunnel Addressing Protocol, (ISATAP). ISATAP is a special approach that allow for IPv6 connectivity for dual- stack nodes over an IPv4-based intranet. Instead of forcing the effort onto routers in the network, the end nodes use the dual-stack implementations to build tunnels for themselves. ISATAP is designed specifically for private intranets and not for the public IPv4 Internet.

Features

- Dual-stack nodes build tunnels for themselves
- No need for special configuration at the router

Advantages

- Relatively easy to set up
- Does not rely on special router configurations

Disadvantages

- Designed for private intranets and not public IPv4 networks

Teredo

Teredo is the protocol that was designed to allow for IPv6 hosts to communicate with each other regardless of whether layers of NATs were in between the two endpoints. Crucially, it is designed to provide clients that are on an IPv4 Intranet behind one or more layer of NAT with IPv6 connectivity.

Many networks in Europe are built using NATs. Residential users, for instance, have a home access box that functions partly as a NAT. There are two significant issues when trying to tunnel IPv6 in IPv4 over NATs:

- NATs provide the interior network with private address space. Thus, home computers or gaming equipment get assigned private address space when turned on.
- Most NATs filter out certain kinds of packets based on implementation choices.

Features:

- Automatic establishment
- Usually from host to router
- Generates signalling traffic to get information about used NAT and obtain an IPv6 address Encapsulates IPv6 in UDP/IPv4

Advantages:

- Works well through NAT
- Very good scalability
- Automatic tunnel service discovery

Disadvantages:

- Poor security
- Difficult to manage
- IPv6 Prefix defined for clients
- Asymmetric model
- Not reliable

Static / Tunnel Broker Approaches

These are configured tunnels, where the tunnel endpoints are manually configured at the routers which do the encapsulation and decapsulation.

Features:

- Static establishment
- Supports authentication

Advantages:

- Good scalability
- NAT traversal possible

Disadvantages:

- No good management tools
- Tunnel service discovery configured manually
- Poor performance if other tunnel endpoint is topologically distant

Transition Mechanisms: Translation

Where dual-stack and tunnelling strategies are unavailable, there remains a third option: translation.

A completely different transition strategy is to provide translation: a device that will translate an IPv4 packet into and IPv6 packet; and vice versa. This strategy seems to be a simple enough proposition: where needed Internet–connected devices translate, or have access to a device that can translate, between IPv4 and IPv6 networks.

For instance, as new networks are given IPv6 addresses, the legacy networks will need access to the new services. That way, an older device can still communicate with new services on the IPv6 Internet as long as a protocol translator is available.

Like tunnelling, translation would be a transitional approach to deploying IPv6. As more and more of the network was IPv6-enabled, the need for translation would gradually disappear.

Clearly, there would be a need to provide translation in the other direction as well. A new node in an IPv6-only network should still be able to connect to IPv4 legacy applications or services (e.g., a search engine available on an IPv4 only web site). In this instance, the host computer's IPv6 network packet would need a service to translate into IPv4 packets.

Address translation has been in use for a long time. The Network Address Translation (NAT) devices that act as the boundary in most residential and small business offices use private IPv4 address space on the interior network and then use the NAT box to translate the private address to a single or limited number of public addresses.

Adding protocol translation seems like it should be a natural extension of NAT. The result was a standardized protocol translation tool called NAT-PT (Network Address Translation - Protocol Translator). Unfortunately, in practice, NAT-PT has been found to have some serious problems – and in a fairly dramatic event, the IETF moved to deprecate its use in 2007.

Key problems with translation as defined by NAT-PT include:

- Problems with any protocols that embed IP addresses or port numbers directly in packet payloads;

- Problems with protocols25 that base integrity mechanisms on source or destination IP addresses;
- Problems with state management and timeouts at the box doing the NAT-PT translation;
- Problems with packet reconstruction in the case of fragmentation;
- Inability to handle multicast traffic; and,
- The requirement to use the DNS as a tool for address mapping.

The problems with NAT-PT caused the IETF to abandon this style of translation.

Translation, in the context of solutions for the transition and migration, should be the last resort. They are complex, do not provide comprehensive protocol support and are exceptionally difficult to make operationally reliable.

Translation could also be used to allow communication from IPv6-only to IPv4-only devices. NAT64 allows multiple IPv6-only nodes to share a public IPv4 address to access the IPv4 Internet. It has been specified so that it only supports TCP, UDP and ICMP. Implementation of IPv6-only networks will be something slightly more common in the future as IPv4 addresses become completely unavailable and IPv4-to-IPv4 translation techniques become more expensive than implementing IPv6 by itself.

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 possibly 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 different 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 a majority of the optional requirements, in addition to all the mandatory ones, of course.

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 - very detailed and comprehensive. They take into consideration the targeted role of the system under test, and sometimes go into great detail. On the other hand, the number of referred RFCs in the IPv6 Ready tests is relatively 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 by 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 different 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 in order 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 Defense (DoD).

Section 5.2.2 is a mapping of RFCs to Unified Capability End Instruments. In effect, for every piece of IT equipment, it specifies the required, and optional IPv6 requirements for the US Department of Defense. The document contains a detailed device classification, and it identifies manda¬tory, 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 on RFC 4294 (published April 2006). It is foremost an informal summary and reference of all the fundamental IPv6 RFCs, their main 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 very 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[1]
	IPv6 Addressing			
F.6		RFC 2526	Reserved IPv6 Subnet Anycast Addresses	Mandatory[2]
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[3]
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[4]
F.15		RFC 7934	Host Address Availability Recommendations	Recommended

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

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

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

[4] Support for Stateless Address Autoconfiguration is essential, but in the case where DHCPv6 is implemented, the autoconfiguration of addresses using SLAAC represents a serious security issue for public administrations. DHCP support is optional, but often preferred in public administration networks.

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[5]
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[6]
F.27		RFC 4380	Teredo: Tunnelling IPv6 over UDP Through NAT	Optional[7]
F.28		RFC 6343	Advisory Guidelines for 6to4 Deployment	Optional[8]
F.29		RFC 6877	464XLAT: Combination of Stateful and Stateless Translation	Mandatory[9]
F.30		RFC 7269	NAT64 Deployment Options and Experience	Optional[10]

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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[11]
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[12]
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

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

[12] 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[13]
	Key Exchange Mechanisms			
F.49		RFC 4307	Cryptographic Algorithms for Use in the Internet Key Exchange Version 2	Mandatory[14]
F.50		RFC 4555	IKEv2 Mobility and Multihoming Protocol	Optional[15]
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[16]
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

[13] 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.

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

[15] 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.

[16] 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[17]
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[18]
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[19]
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

[17] 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.

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

[19] 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[20]
R.2		RFC 2784	Generic Routing Encapsulation	Mandatory[21]
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[22]
R.5		RFC 4891	Using IPsec to Secure IPv6 in IPv4 Tunnels	Recommended[23]
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[24]
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[25]
R.16		RFC 5643	MIB for OSPFv3	Optional[26]
R.17		RFC 6565	OSPFv3 as a Provider Edge to Customer Edge (PE-CE) Routing Protocol	Optional

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

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

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

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

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

[25] Mandatory in implementations where the router supports mobileIPv6.

[26] 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[27]
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[28]
R.36		RFC 7721	Security and Privacy Considerations for IPv6 Address Generation Mechanisms	Advisory

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

[28] 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[29]
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

[29] 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[30]	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[31]
I.8		RFC 6610	DHCP Options for Home Information Discovery in Mobile IPv6	Optional[32]
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[33]
	Tunnel Broker Services			
I.16		RFC 3053	IPv6 Tunnel Broker	Optional[34]

[30] 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.

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

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

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

[34] 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 particular standard.

We divide the Management Deices 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[35]			
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[36]
M.8			Packet analysis by the security service/device	Mandatory[37]
M.9			Fragmentation protection	Mandatory[38]
M.10			Handling of Encapsulated packets	Mandatory[39]
M.11			Handling of extension headers.	Mandatory
M.12		RFC 4890	Recommendations for Filtering ICMPv6 Messages in Firewalls	Mandatory

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

[36] 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.

[37] 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.

[38] 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.

[39] 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 tunneling and dual stack is required, the device must support Generic Packet Tunneling 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].