Title:	Document Version:
Deliverable D2.4 **EU IPv6 Profile – Guidelines for IPv6 Deployment**	1.0

Project Number:	Project Acronym:	Project Title:
297239	GEN6	Governments ENabled with IPv6

Contractual Delivery Date:	Actual Delivery Date:	Deliverable Type* - Security**:
30/06/2013	15/09/2013	R – PU

* Type: P – Prototype, R – Report, D – Demonstrator, O – Other
** Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Responsible and Editor/Author:	Organization:	Contributing WP:
Uwe Holzmann-Kaiser	Fraunhofer FOKUS	WP2

Authors (organisations):

Jens Tiemann, Gabriele Goldacker, Joachim Kaeber, Carsten Schmoll, Dorota Witaszek (Fraunhofer).
Martin Krengel, Gerold Gruber (citkom)

Abstract:

The deliverable contains a set of recommendations for IPv6 features and standards to be used in European administrations. The annex to the deliverable contains available profiles already existing in the EU context, RIPE and the proposition for a profile for public sector in Germany.

Keywords:

IPv6, Governments, Procurement, Standards, Recommendation, Profile

Revision History

The following table describes the main changes done in this document since its creation.

Revision	Date	Description	Author (Organization)
v0.1	4/06/2013	Document creation	Dorota Witaszek (Fraunhofer)
v0.5	26/07/2013	Request for Comments from Gen6 partners	Uwe Kaiser (Fraunhofer)
v0.5	02/08/2013	Comments by UL	Gabriela Georghe et al. (UL)
v0.6	16/08/2013	Addressing comments to v0.5 version	Carsten Schmoll (Fraunhofer)
v0.7	19/08/2013	Management Summery	Uwe Kaiser (Fraunhofer)
v0.8	19/08/2013	Quality control, addressing comments	Carsten Schmoll (Fraunhofer)
v0.9	02/09/2013	Comments, Introduction and summary	Martin Krengel (citkomm)
v1.0	12/09/2013	Integration of last editorial comments	Uwe Kaiser (Fraunhofer)

Disclaimer

Executive Summary

The introduction of IPv6 is a challenge for everybody and every institution. Nobody is changing a running system without need but the shortage of IPv4 addresses and devices communicating only by IPv6 forces every maintainer of communication infrastructures to handle and to use the new protocol. The transition to IPv6 (IPv6-only or Dual-Stack) affects the whole stack: applications, middleware like application servers and hardware of any kind - the Development as well as the operation of services.

This document will support those in public administration planning the transition on how they can find answers to the two following questions: Will my existing equipment support IPv6? and What are the minimum requirements of devices to be interoperable?

There are several documents around describing such requirements on different level: from coarse to detailed, from organisation specific to vendor driven. This document and the accompanying set of requirements are forming a profile which has its roots mainly in the German profile and the ripe-554, the IPv6 Logo program and several documents from US government standards. All recommendations have been evaluated and stripped off from national specific requirements. Even if this profile has been written with public administration in mind if can also be used in other areas.

So this document gives guidance for the evaluation of existing infrastructure and it can be used for procurement processes. But the reader should keep in mind that this document is not the one size which fits all the time. There will be situations where the recommendations have to be changed by making them smoother or by tightening the screws.

This profile will not be accompanied by a certification or validation program. There are several ways to ensure the existence of required capabilities: the device or application is conformant to another existing profile with comparable requirements, it has passed a 'Logo-Program' like the one from the IPv6-Forum or by written agreement of the vendor. Setting up an approval or certification is far beyond the tasks of WP2 and the GEN6 project.

Table of Contents

1. INTRODUCTION

Since the beginning of the Internet, the Internet Protocol version 4 (IPv4) has been used. Today, this protocol is used everywhere, including the internal networks of public administrations and organisations. The Internet and all other networks using IPv4 today face a major technical change, as it is necessary to change to the successor of IPv4, IPv6.

There are two central answers for the often raised question about the major factors driving the migration to IPv6:

- The non-availability of free IPv4 addresses, e.g. in Asia, forces the migration.
- The increasing need for addresses for various devices including sensors and smartphones, but also washing machines[1] etc. communicating via IP networks increases the problem of the exhausted IPv4 address space.

The convergence of both facts accelerates the migration towards IPv6.

In the future, there will be many devices that will have only IPv6 addresses (instead of an IPv4 address) and which will be only reachable via this address. Already nowadays, disabling of IPv6 is no longer possible for the latest operating system releases. ISPs will provide the remaining IPv4 addresses only for high fees. In the case of changing the ISP, e.g. after a mandated call for tenders, it could be impossible to migrate these existing IPv4 addresses to a new ISP. Thus, migration to IPv6 will not only guarantee availability of a sufficient number of IP addresses, but ensure the future reachability of one's services without a long-term binding to a specific ISP.

The goal of this document is to define a common profile, EU IPv6 profile for public acquisitions involving IPv6. The profile will help organizations in their procurement process when updating their equipment in order to support IPv6 and will be an important step to maintain the interoperability requirements. The main focus of the description is on the common set of recommendations for the support of specific IPv6 features.

Chapter 2 gives an overview on existing, international profile documents. Chapter 3 proposes a specific profile for public tenders within the EU community. Chapter 4 concludes the deliverable.

[1] http://www.pcworld.com/article/32128/article.html

2. EXISTING PROFILES

The protocols concerning the global Internet are written as Standards documents (STDs) and Request for Comments documents (RFCs) by the Internet Engineering Task Force (IETF). Roughly 200 of those documents are concerned with the definition and operation of IPv6, including adoptions of related protocols (e.g. ICMP), so that an interoperation with IPv6 is possible, as it is with IPv4.

Existing IPv6 profiles usually describe mandatory/recommended/optional requirements for IPv6-enabled devices or implementations, based on STD and RFC documents. There may be additional technical requirements in any given use case, for example depending on specific quality- or security-related requirements. 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.

As an overview the following sections name and describe existing profiles.

2.1 RIPE 554

The Réseaux IP Européens Network Coordination Centre (RIPE NCC) supports the technical coordination of Internet infrastructures within Europe. In this framework the IPv6 working group has developed „Requirements for IPv6 in ICT Equipment". These requirements have been documented in November 2010 in "ripe-501" [ripe-501]. As of June 2012 an updated version of this document is available in „ripe-554" [ripe-554].

The ripe-554 document – and specifically the requirements documented therein – can be seen as a supporting collection of best practices for the public sector and commercial companies alike.

ripe-554 identifies the essential devices 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, preferred devices should implement most of the optional requirements, in addition to all the mandatory ones, of course.

ripe-554 is relatively coarse in its characterization of the different RFCs, as it does not differentiate between the various properties inside a single RFC documents – the RFC is assessed as a whole.

2.2 German IPv6 Profile

The Ministry of the Interior made the first step in 2009, reserving an address block that is sufficient for the whole German public administration. This address space ensures that each public administration communicates using its unique subspace in the future. This enables more direct, simpler, and more efficient communication. The management of the German address block is organized corresponding to the German federal structure covering the federal government, the federal states and the municipalities.

The second step was the development of guidelines [IPv6_Migration] to stimulate and support the transition of public administrations to IPv6 addresses. They support the acquisition of new devices and the evaluation of existing hard- and software and help switching to IPv6.

The IPv6 profile for the public administration supports the acquisition of new and the evaluation of existing devices. The definition of necessary/mandatory, useful/recommended and optional features of IPv6 devices enables the detailed specification of selection criteria. Requirements can be specified in terms of device roles (router, firewall …) and usage contexts (stationary, mobile …), simplifying the assessment of the fulfilment. The profiles can also be used to assess existing devices, concerning their usability in IPv6 environments.

The German profile document especially considers the requirements and characteristics of public administrations (e.g. existing network architectures and security requirements) and thus provides the foundation for the focused and structured transition to IPv6 for the administrations.

The profile document for the public administration provides support for the procurement of IPv6-capable hardware and software components. To this goal it specifies which IPv6-standards have to be supported by a networked device or system, in order to fulfil its duties in an IPv6 environment.

The profile document consists of two parts, a tabular profile matrix and a companion document explaining how to read the matrix. The profile matrix contains all the details about the support of required and recommended standards, while the document explains the format and use of the profile matrix and some further details. The profile documents can also be applied to check the IPv6-fitness of existing networked components.

It is very important that IPv6 be introduced into network environments across-the-board, because of the IPv4 address shortage. This means that every new purchase of networked devices or software must take IPv6-capabilities into account to guarantee a level readiness for the future – optimally even for an environment where IPv4 is not available at all anymore.

The adoption of IPv6 can be done in different ways:

- Based on existing network infrastructure, IPv6 can be added to IPv4 in parts or whole of the network (e.g. the Intranet of a company). Using IPv4 and IPv6 together in a single network is called dual-stack approach.

- In newly created networks (or subnets) with clearly defined tasks and use cases, one can consider to run IPv6 in an IPv6-only configuration. For this to work, all components (hardware, software (OS, applications)) must be able to run without any IPv4 available.

The detailed analysis of the scenarios stands at the start of building an IPv6-capable network, regardless of whether the network is based on existing components or made up of new acquisitions. The network functions to be used are based on this analysis (e.g. stateless autoconfiguration). The definition of scenarios and derived functions is an important precondition for applying the profile documents. They determine which sections of the profile have to be taken into account for the planned network, and in effect, which features are optional, recommended or mandatory.

The publication of these documents at http://www.ipv6.bva.bund.de provides them to all interested parties. The documents are a pragmatic introduction to IPv6 transition and support implementing it in practice.

2.3 Department of Defence Unified Capabilities Requirements

The document called "Department of Defence Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)" [UCR08_2], which is actually from December 2010, describes quite comprehensively a multitude of requirements on IPv6 devices and implementations for procurement by the United States Department of Defence (DoD).

Subchapter 5.3.5 of [UCR08_2] documents the requirements related to IPv6. An integral component of the document is the "DoD IPv6 Standard Profiles for IPv6 Capable Products version 5.0" from July 2010.

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.

2.4 IPv6 Ready Logo Program of the IPv6 Forum

The vendor-driven IPv6 Ready Logo Program [IPv6Ready] of the IPv6 forum encompasses specifications for conformity tests and interoperability tests for IPv6 and related protocols:

- the IPv6 base protocol (including Stateless Address Autoconfiguration (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

For this purpose the IPv6 forum provides test suites for automated evaluation of IPv6 properties. A successful passing of such test suite authorizes a vendor to assign the IPv6 Ready logo to the tested devices series. There exist dedicated IPv6 test centres, which provide running of the test suite as a service. However, the IPv6 Ready logo can also be obtained via provisioning of appropriate self-test results by the manufacturer.

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 detail up to checking single messages and message exchanges between devices. On the other hand the number of referred RFCs in the IPv6 Ready tests is relatively low (36 compared to more than 200 in other IPv6 profiles).

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

We note especially that network protection functions, as provided by packet filters and application layer gateways, are not captured by the IPv6 Ready tests as these functions are not formally standardized in STD and RFC documents.

2.5 A Profile for IPv6 in the U.S. Government

This document [NIST_USGv6], in version 1.0 from September 2008, has been developed by the National Institute of Standards and Technology (NIST), an organization related to the US ministry of trade.

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

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 goes into much 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.

In its goals, the [NIST_USGv6] document comes closest to our IPv6 profile document. Unfortunately, due to its age, some important parts of [NIST_USGv6] are not up-to-date anymore, so that the reader often needs to check for updated or newer RFC documents, to find the latest definitions, when assessing it. Up to the beginning of 2013 no newer version of [NIST_USGv6] has been released.

The NIST document Guidelines for the Secure Deployment of IPv6 [NIST_119], from December 2010, is most of all an IPv6 tutorial, but with a specific focus on IPv6 security issues. It especially informs the reader about those IPv6 security risks, which have not yet been finally solved (e.g. IP first-hop-security issues in Intranets).

2.6 IPv6 Node Requirements and Informative RFCs

Informative RFC documents are divided into different categories:

- Standards Track (Proposed Standard, Draft Standard or Standard)
- Informational
- Best Current Practice (BCP)
- Experimental

Therefore, one could expect that all relevant information for an IPv6 profile are contained within the standards documents, and that BCP documents only contain things like

recommendations for network and device configuration. In practice, the borders between the document types are not that clear.

The reasons for this lie in the process by which standardization in the IETF works: new topics (for example some security mechanism) might be discussed by different working groups, and tackled with different approaches. This wide-spread interest and the participation of different groups till the final version of an RFC have a high influence on the final result. It is this broad consensus process during the writing of an RFC document, which leads to relevant, practically usable protocol definitions in the RFC standards, but also sometimes to (still) open detail questions and a not-so-hard differentiation between the different types (STD, BCP, …) of RFC documents.

Some RFCs of the "informational" type are also referred by our profile matrix document, as these sometimes are the ones which specify relevant parameters for practical use of a protocol. In any case it can be beneficial to read the informational RFCs in your area of interest too. In the remainder of this section we highlight important "overview type" RFCs that are relevant for working with our IPv6 documents and IP6 in general.

RFC 6434 – IPv6 Node Requirements

RFC 6434 ("IPv6 Node Requirements") [RFC6434], 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. 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.

This RFC summarizes different requirements on IPv6 devices (end systems, routers, etc.). It sorts the numerous requirements with regards to protocol layers (Sub-IP layer and IP Layer) and based on protocol mechanisms (for example DNS, DHCP, Mobile IP, and security). RFC 6434 is already the second "incarnation" of Node Requirements (it replaces [RFC4294]). It describes the interaction between protocols and their mechanisms, while pointing to other RFC documents for the underlying details and related requirements. RFC 6434 also defines separate requirement levels, which specify in how far other RFCs (or parts thereof) must be implemented.

RFC 6204 – Basic Requirements for IPv6 Customer Edge Routers

A special class of devices are routers in local networks that provide the connectivity (uplink) towards the external network provider (often synonymous: "Internet provider"). There exist different terms for such a router, depending on the use case: Perimeter router, edge router, and small-office-home-office-router (SOHO-router, see table 1). RFC 6204 („Basic Requirements

for IPv6 Customer Edge Routers“) [RFC6204] describes requirements related to the WAN- and LAN-side of such router, as well as generic networking features of it. This RFC highlights the differing requirements on such a router, for example for local IP address configuration, depending on the intended use case. For security requirements RFC 6204 refers to RFC 6092: "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service" [RFC6092]). While RFC 6204 was still in the making, the closely related RFC 6092 “Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service” [RFC6092] has been in the making. The latter especially focuses on IPv6 in the SOHO use case and the complexity in the interaction between the different protocols in use in this case. This informational RFC is now also final (as of January 2011).

RFC 4864 – Local Network Protection for IPv6

The emphasis of this RFC document lies in the presentation of the security-relevant aspects in typical computer networks, and which IPv6 mechanisms can be used to cover them. Starting point of this document is the observation, that many security issues are “solved” in the IPv4 world using Network Address Translation (NAT). As the use of NAT is problematic (even more so with IPv6), this RFC gives recommendations on how typical security aspects that are commonly addresses in IPv4 using NAT, can be covered in IPv6 networks by using existing IPv6 protocol mechanisms.

RFC6071 – IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

This RFC document [RFC6071] gives an overview about the different RFCs in the area of IP security (IPsec). During the long time of standardizing IPsec, numerous documents on it have been finalized by different working groups. Therefore it is quite tiresome to get an exhaustive overview on IPsec. RFC 6071 gives an overview on the IPsec-related RFCs, including a short description for each and additional background information.

3. SPECIFIC PROFILE FOR PUBLIC TENDER

3.1 The Profile Purpose

The profile should be seen as a checklist to determine the set of requirements that are important for the targeted network. This set can then later be used as input to the functional specification document to be used in procurement. It is not appropriate to just refer to the IPv6 profile in a "must-be-fulfilled" manner; it is merely a basis to lookup the concrete set of requirements. Alternatively such a set of requirements can be used to query detailed feedback from network equipment vendors about the applicability of their devices for the planned IPv6 network, based on a listing of relevant IPv6 standards (request for comments, RFC).

In both cases, one can use the profile as a basis for communication between vendors and customers about detailed technical requirements, in the form of relevant IPv6-standards (request for comments, RFCs) and associated requirement levels. The combination of technical systems in a network which all do fulfil the IPv6 profile does not necessarily lead to a fully functioning network setup – the fulfilment of the profile requirements is however a necessary minimal requirement for successful interoperation.

Note that the concrete configuration of the systems is not part of the IPv6 profile. This effectively means that setting up the networked systems in a useful and compatible way is a separate task, after procuring systems which have all the required features implemented. In practice, even systems which are compatible on paper and do support all the required features, may experience interoperability issues, due to slight differences in IPv6 implementations. Therefore, dedicated interoperability tests are recommended, which test the concrete systems in practice. Before bringing new systems into "live" networks, it is often a useful approach to setup a smaller, limited test bed, which is initially not part of the production network that is to be migrated.

The evaluation of existing IPv6 profiles showed that these profile documents do indeed not represent competing definitions, but represent complementary approaches, showing IPv6 aspects of components from different points of view and with their main emphasis on different IPv6 issues.

All considered profile documents relate to relevant standards documents (request for comments, RFC) and define features from these standards for different classes of devices, and in different requirement levels. In this way the profiles recommend, which RFCs (all or parts thereof) are mandated, recommended, or optional, given a specific device, network environment and use case.

The existing profiles differ in their terminology regarding requirement level, as well in their depth – where one profile may mandate a complete RFC; another may pick specific features from that RFC only. In our comparison and consolidation work we have aligned the data from the other profiles as good as possible, and have explained differences where needed, to motivate our recommendation.

3.2 EU Profile Proposal

After an analysis and a comparison of these profiles, and identification of common structural elements, the listed requirements can be consolidated in a consistent form, the recommendations for the EU IPv6 profile that is targeted to the public administration sector.
We concentrated on the profiles already existing in the EU context, the RIPE-554 documents and the proposition for the profile for the public sector in Germany. Both profiles differ in structure, presentation and coverage and detail, but broadly there are no contradictions in their recommendations.
We propose to use both IPv6 profiles for hardware components in the European context, the RIPE document at the high level, for general orientation in required IPv6 features, and the German profile, current version presented in this document, with more detailed and more focus on the public sector.
The development of future revisions of both documents should remain consistent with each other.

3.3 EU Profile – High Level

The last version of RIPE (at the moment RIPE-554) is recommended for the general list of IPv6 requirements.

3.4 EU Profile – Detailed Level

The more detailed level of recommendations is based on the proposition of a profile for the public sector in Germany and the documents describing profiles.

This chapter describes the structure of the IPv6 profile matrix document to be used for public sector in Germany and how to "walk it through" in a given use case, in order to derive the right set of requirements. The IPv6 profile matrix (Excel sheet) will be delivered as an extra document.

At first the generic structure of the table sheets from the profile matrix document will be shown and then we have a look at some of these sheets in more detail.

3.4.1 Structure of the Table Sheets

The profile matrix document has been structured along two "dimensions" to make it optimally accessible to the reader. The dimensions are:

- device classes and
- functional categories.

The different device classes are described on a separate table sheet (see also section 3.4.1.1).

The recommendations per functional category themselves are structured hierarchically on each sheet (see also section 3.4.1.2).

In order to avoid redundancies in the descriptions, we at first define the "IPv6 node" as the basis for all other IPv6-enabled devices. The sheets for all other device classed then only note the requirements which are needed in addition to IPv6 node.

3.4.1.1 Device Classes

The currently existing profiles cover a set of devices classes. In RFC 2460 (“Internet Protocol, Version 6 (IPv6) Specification”) [RFC2460] the classes "node", "router", and "host" are defined.

As the German profile was initially targeted at the networks and devices of the public administration, this set had to be extended, leading to the set depicted in Figure 1. The “white nodes” in figure 1 are for structuring only; they do not represent a separate table sheet in the profile matrix.

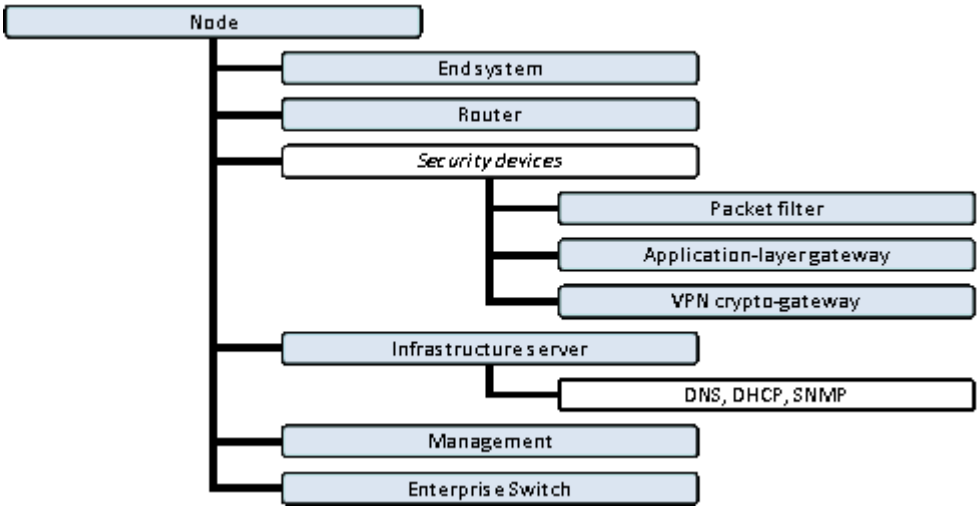

Figure 1: Hierarchy of device classes

These subclasses make up a generic instance of this class. The “node” sheet as the basis defines all requirements which affect each IPv6-capable device. A concrete device may indeed

implement the features of more than one device class. Take for example a current SOHO-DSL-Gateway – it usually implements functions from the following device classes: router, packet filter, DNS- / DHCP-Server, and possibly other infrastructure servers as well. Therefore, to collect all requirements for a given device, multiple table sheets have to be taken into consideration (cf. Figure 2).

Security devices (in the public administration) play a special role: even though they are based on “node” as well, their practical implementation may in fact deviate from some “MUST” type recommendations from the node sheet, if this is a functional necessity for their operation.

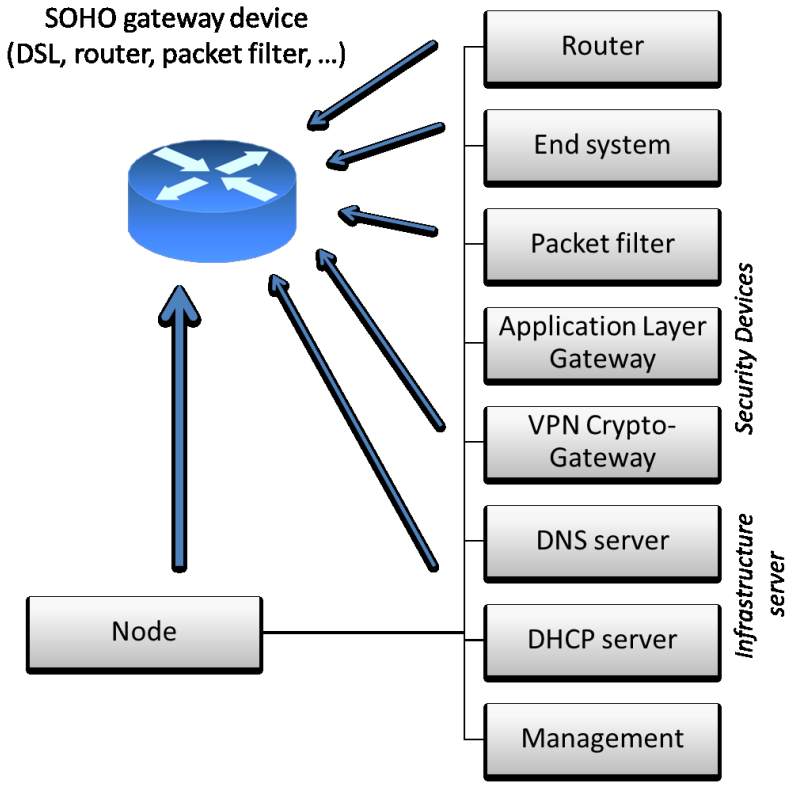

Figure 2: Complex Device Example Based on the SOHO Router Use Case

The German IPv6 profile adheres to the following principles:

- Each feature is (as much as possible) only listed in one device class, since device classes inherit from one another (cf. Figure 1). An exception from this rule happens, when the recommendation level increases in a more specific device class, e.g. from the node sheet to the router sheet.

- The recommendation level can only be increased when going from a base sheet to a derived sheet that inherits the recommendations. For example, there are some features related to Stateless Address Autoconfiguration (SLAAC) which are "recommended" for node but "mandatory" for end systems. The only exceptions to this rule are security devices. In special cases, they may also downgrade a

requirement, i.e. not implement a feature which is a “mandatory” in the node sheet.

- The features listed in the "Management" table sheet do not represent a device class of its own; rather the sheet documents relevant aspects of a management interface across different devices classes.

As an introduction to the use of the IPv6 profile matrix the reader should have a look at the following table (Table 1). The first two columns list concrete devices (grouped by device class), as they can be found in the public administrations’ networks, while the rightmost column names the related table sheets.

Device		Table sheet
End system		
	Workstation, Desktop	End system, node, if need be: Management
	Notebook, Tablet	End system, node, packet filter, if need be: Management
	Server (Application)	End system, node, management
Router		
	SOHO router	Router, node, packet filter, DNS- / DHCP-Server
	Perimeter router Edge router Border router	Router, node, management
	infrastructure router	Router, nod, management, if need be: DNS- / DHCP-Server
(Layer2-) switch		Enterprise Switch, management
Security device		
	Packet filter	Packet filter, node, management, if applicable: Router
	Application layer gateway (ALG), Proxy	Application layer gateway, node, management, if applicable: Router
	Crypto box VPN gateway	VPN crypto-gateway, node, packet filter, management, if applicable: Router
(Network-)infrastructure		
	DNS server DHCP server RADIUS server tunnel broker	End system, node, infrastructure server, management

Table 1: Relation between Device Classes and Matrix Table Sheets

3.4.1.2 Functional Categories

All features listed in the table sheet for a device class are grouped into a hierarchy. Most of the time this hierarchy will be: “category” referred RFC document belonging to this category, and “selected feature” from inside this referred RFC document. Figure 2 in this document shows an example of this approach for structuring.

Each sheet starts with generic requirements that are relevant for several classes; followed by the features referring to the core functionality of the class.

The following list describes the generic functional categories:

- Base requirements: These features are needed for a successful IPv6 communication. Amongst them are the support for the IPv6 protocol itself, ICMPv6, Neighbor Discovery and functions for detecting the maximum packet size (MTU discovery).
- Addressing: IPv6 address semantics, formatting, and address configuration features belong in this category.
- DNS resolver: this category covers all the differences between client-side DNS related to either IPv4 or IPv6
- Transition mechanisms: this category covers all technologies that serve the migration from IPv4 towards IPv6 support
- NAT: the category describes mechanisms that implement features in an IPv6 environment that are realized in IPv4 using network address translation (NAT)
- IPsec: this category covers the security-related features
- Multicast: the category describes the support of multicast functionality
- Quality of Service (QoS): the category covers all functions that are needed to support different levels of network transmission quality
- Mobility: the category covers the functions needed for Mobile IPv6
- Network and system management: This category describes the management-related protocols for use with IPv6, as far as they are not yet contained within the top-level device class “management” already

A similar categorization is used by [UCR08_2].

The latter of each sheet can contain a list of requirements specific to a device class (for example router, end system, packet filter).

3.4.1.3 Description of the Table Columns

While the concrete row structure may differ between sheets of the profile matrix, the structure of the used columns is uniform across the sheets, cf. table 2.

Column	Contents
Category **Category** **Category**	possibly multiple stages of functional categories (cf. section 3.4.1.5)
RFC	number of relevant RFC document
Titel	title of relevant RFC document
Feature, function	name of the concrete function
Project recommendation	recommendation level of this feature for use in the public administration
Comment	associated remarks (if any)
ripe-554 (successor to ripe-501)	recommendations of the respective profile document

Table 2: Description of Table Columns

The latter columns are filled to a different level, sometimes more, sometimes less, because not all referred external profile documents contain statements to each feature we list in our profile matrix. In some occurrences our profile matrix contains suggestions on how a certain profile document relates to this device class or to this category.

Due to the different structure of the diverse profile documents it was not possible to find one common terminology for the specification of requirement levels. If in doubt, the reader should consult the original document of the corresponding profile.

3.4.1.4 Requirement Levels

More or less each existing profile uses its own terminology for requirement levels specification. Our profile matrix uses the terms "must", "recommended", "optional", and "for information"; cf. the following table.

Term	Description
mandatory	The noted feature has to be realized in this form, based on technical and/or administrative reasons, because the desired behaviour cannot be implemented otherwise, without this feature.
recommended	The realization of this feature is deemed useful. Depending on the concrete use case and other requirements a device from this device class may omit the implementation of this feature.
optional	The given feature is optional.
not recommended	The feature should not be used.
prohibited	The feature must not be used.
for information	further information, for example overview documents

Table 3: Definition of Requirement Levels

RFC documents that only have an informational character do not receive a recommendation in our profile other than „for information”, as they do not contain concrete, implementable

specifications or features, but only describe additional requirements to an implementation or realization of a feature.

Conditional Requirements

In the profile matrix document, as well as in other, referred profiles, some features are only required when certain conditions are true. In these cases the condition is clearly stated in the requirement level column of the feature's table row.

In case that conditions relate to the whole set of features inside a functional category, then the condition is stated in the matrix already on the category level. For example, the use of SNMP is recommended. This means SNMP-related requirements are to be fulfilled only in case that SNMP is actually used.

The following sections describe, where needed, selected recommendations, showing background information to motivate our selected recommendation level. We suggest to the reader to read these description alongside the respective table sheet.
The existence of additional features in a device – i.e. the features that are implemented but not used – is not always beneficial. Their existence could result in an increased configuration overhead, or could pose an unwanted security risk/hole. Procured new devices should therefore not contain an unnecessarily huge feature set, and it should be known (and documented on installation) what other functions a device may realize (e.g. "router XYZ: Can also work as a packet filter – not used").

3.4.1.5 How to Read the Profile Matrix

The following paragraphs document some examples on how to read our profile matrix document. For a better comprehension we have included here some excerpts (snippets) from the actual profile matrix document. These snippets can be easily found in the profile matrix document. The following examples show some aspects of its use:

Cate-gory	Cate-gory	Cate-gory	RFC	Title	Feature, function	Project recommendation	Comment
Communication of the IPv6 node							
	Basic requirements						
		Basic					
			RFC 2460	Internet Protocol, Version 6 (IPv6) Specification		mandatory	
					Flow Label Field not used and ignored (unless RFC 6437 is implemented)	mandatory	

Figure 2: Profile example #1 – Feature / Function and Requirement Level

In this example the last line gives additional detail information, related to the specific feature. Each used feature or function which is referred in our profile matrix, will have assigned a recommendation level. If single features from an RFC are explicitly listed in our profile matrix, then (in rare) cases they may show a requirement level that differs from the one given in the

RFC itself. Also, our document sometimes assigns requirement levels to a feature which did not show any requirement level in the RFC document at all.

Cate-gory	Cate-gory	Cate-gory	RFC	Title	Feature, fun ction	Project recommendation	Comment
Device functionality							
	Management and configuration					mandatory	
					Access to management / configuration via IPv6 and IPv4	recommended	
					Support of deactivation of an IP variant (IPv4 / IPv6) not used for management / configuration	recommended	if a separate management / configurations interface will be used

Figure 3: Profile example #2 – Feature / Function without a Related RFC

The second example shows requirements from within the profile matrix which were not specified by an RFC document initially. This is usually the case in our document when the requirements are of a more abstract level, and represent a requirement not represented by a single RFC document. In this example we show the requirement to have devices configurable (remotely) via IPv4 as well as IPv6. The comment field gives additional information, here, under which conditions this specific recommendation is relevant.

		SEND, if usage planned				recommended	only few inplementations available
			RFC 3971	Secure Neighbor Discovery (SEND)		mandatory	
			RFC 3972	Cryptographically Generated Addresses (CGAs)		mandatory	

Figure 4: Profile example #3 – Condition „if use is planned”

In some cases a condition is specified, related to a complete function category or subcategory in the matrix. The IPv6 feature SEcure Neighbor Discovery (SEND) for example is not necessarily needed for normal IPv6 operation, therefore some RFCs do only need to be addressed, when SEND is to be used in a practical setup. This always depends on the concrete use case. In practice, for example, not many networked systems require support for mobile IP. If they do, however, then a plethora of features become mandatory, as they are conditional on the use of mobile IP.

The usage of certain other function categories is explicitly recommended, especially for security purposes. If you decide to support the function category, then the listed RFCs are mandatory, because the used function category should conform to the relevant standards.

This means: In the first step, you make a decision for the whole function category and in the second step the whole category is ignored if usage is not planned or the requirement levels of the RFCs and functions in the whole category are treated like unconditional table entries. In our example: If you decide to use SEND, then RFC 3971 and RFC 3972 are mandatory.

			RFC 4864	Local Network Protection for IPv6		for information	compilation of corresponding RFCs and native IPv6 features

Figure 5: Profile example #4 – Row without requirement level specification

The fourth example shows that a row in our profile can also omit the recommendation level – if it is of informational level only. In these cases the profile indicated that would be very helpful to know about the RFC, especially, when it is also referred by other profile documents as well. In such a case then comment field usually explains the contents of the referred RFC, and possibly, why it is only for information.

An RFC may contain requirement levels for single features, even if it does not specify a requirement level for its contents in their entirety. This is often the case when an RFC is informational, yet contains some features give a requirement level, or extend older features, which already had a requirement level. In this case our profile also gives that requirement level, instead of “for information”.

		IKEv1, if usage planned		recommended	for interoperability with nodes which are not IKEv2-capable
	RFC 2409 (obsolete!)	IKE version 1 (IKEv1)		mandatory	for interoperability with nodes which are not IKEv2-capable
			During SA establishment, discarding of further answers after reception of the first cryptographically correct answer	mandatory	

Figure 6: Profile Example #5 – Notion of obsoleted RFC

Some RFCs in our profiles are marked as “obsolete”, such as in the figure above. There are two cases where this applies:

- if a newer RFC updates an existing, older RFC in its entirety, adding clarifications and/or corrections
- in the description of (additional) new protocol features and/or functions, which are incompatible with parts of an existing RFC standard

In the latter case where the newer RFC obsoletes ("overwrites") only parts of the older RFC we also list the older RFC and features (and requirement levels) of it within the profile matrix. The same is true for new RFCs which are not yet in wide-spread practical use, or if the features of the older RFC must be supported, because they are in practical use still. In the above profile example #5 the older protocol (here: IKE version 1) plays an independent role (compared to IKE version 2), therefore it is listed in the profile matrix still. Even older features can still have the requirement level “mandatory”, in case they are relevant for certain use cases. In such a case the use cases are clearly indicated in the comments field. Generally, however, an implementer/manufacturer of a device has to follow the newer RFCs; including their documented corrections (“verified errata”).

3.4.2 Node

Nodes are the most general devices of an IP network. In contrary to routers and hosts, they are

not reflected by dedicated physical equipment but is an abstract component implementing the basic communication functions in real devices. The advantage of this approach is that common features of different device types involved in a given communication can be described at a single place. This simplifies the presentation and the assurance of interoperability between different device types.

The specific requirements for nodes can be classified into the following:

- the communication of the IPv6 node,
- the network or system management, and
- the link-specific requirements.

3.4.2.1 Communication of the IPv6 Node

This section covers all features required to participate in the communication in an IPv6 network.

Basic Requirements

The basis for the communication is the IPv6 basic specification in RFC 2460. If no functionality based on the Flow Label in the IP Header is used, this field shall not be used (set to ZERO) and ignored. Otherwise, the handling of the field conforming to RFC 6437 (“IPv6 Flow Label Specification”) shall be implemented.

Following RFC 5722 (“Handling of Overlapping IP Fragments”), the use of overlapping IP fragments is forbidden for security reasons.

RFC 6540 (“IPv6 Support Required for All IP-Capable Nodes”) describes the problem that the term IP implied IPv4 in older RFCs and that primarily new RFCs have been created for IPv6. Therefore, it is sometimes unclear which IP version(s) have to be supported. This RFC recommends as “Best Practice” that

- new IP implementations shall implement IPv6 mandatorily,
- updates of existing IP implementations should IPv6,
- concerning functionality and quality, the IPv6 support shall be equivalent or better compared to the IPv4 support, and
- the coexistence of IPv4 and IPv6 (dual-stack operation) should be supported and IPv4 shall not be necessary for proper operation of new or updated implementations.

For security reasons, some ICMPv6 features have to be configurable, to avoid the disclosure of the local network infrastructure and to prevent denial-of-service attacks.

The Implementation and the use of the Neighbor Discovery Protocol (NDP) are mandatory. For the protection against malicious neighbours, some usage requirements are tightened.

RFC 5942 (“IPv6 Subnet Model”) contains some clarifications concerning the IPv6 subnet model in conjunction with the use of NDP. It is informational.

Secure Neighbor Discovery (SEND) is a mechanism to protect the automatic network management of IPv6. Its support is recommended, but only few implementations are available up to now.

The topic “Transfer” covers basic communication features of nodes in IPv6 networks that are related to data transmission or the coordination of devices.

- Path MTU Discovery is a relevant basis for the functioning of IPv6 communication as a fragmentation by routers is not envisaged. Thus, nodes shall support Path MTU Discovery. Nodes should support the processing of packets with at least 1500 octets to enable high-performance communication. If a node receives “Packet Too Big” ICMP messages in return to unfragmented, minimum-size packets of <= 1280 octets (as specified in RFC 2460) it shall insert a Fragment Header in those packets as specified in RFC 2460 and RFC 1981. Received single-fragment messages shall be handled conforming to RFC 6946 (“Processing of IPv6 "Atomic" Fragments”).

- IPv6 jumbograms are packets up to a theoretic size of 4 GB which might be used by special applications to transport large amounts of data in the future. It has to be noted that the customary transport protocols (i.e. TCP, UDP) do not support such big data units. Thus, special protocols are required above IPv6. Today, customary Layer 2 transmission mechanisms do not support such packet sizes, too.

- The Router Advertisement (RA) messages of the Neighbor Discovery Protocol (NDP) contain an 8-bit field for flags. RFC 5175 (“IPv6 Router Advertisement Flags Option”) defines an extension enabling further flags for future applications.

- The IP Router Alert Option conforming to RFC 2711 is based on a hob-by-hop header that informs routers along the path about the necessity to process the packets carrying it. This function can enable a more efficient handling of the packets related to certain protocols (e.g. RSVP) by routers.

Header Compression

The term “Header Compression” covers different methods to compress the transmitted

headers of typical Internet protocols like IP (IPv4 or IPv6), UDP, and TCP etc. as short as possible. Generally, redundant data is not transmitted, i.e. data known to the communication partner(s) is omitted. A typical example is the omission of the message length as it can be derived from the message borders of the underlying layer.

Header compression always requires the use of compatible compression components at all communication partners. In many cases, header compression leads to a higher processing effort at the communication partners. Additionally, some errors can no longer be detected when header compression is applied. E.g., the loss of a segment of a fragmented message cannot be detected if the overall message length is not transmitted.

Header compression is optional for general scenarios of public administrations as it is only useful under specific conditions like a very small transmission rate.

If header compression is used, the availability of corresponding components typically influences the method applied. For very low-performance systems, the complexity of the method can be determinant.

The most modern and efficient header compression method is Robust Header Compression (ROHC, RFC 5795 and others). This method is formally structured into a framework specification and different profiles.

If the use of ROHC is planned, the framework specification RFC 5795 (”The RObust Header Compression (ROHC) Framework”) and the profiles for TCP/IP (RFC 4996) and for RTP, UDP, IP ESP and UDP-Lite (RFC 5225) shall be implemented.

If the old profiles for RTP, UDP, ESP and uncompressed messages) are implemented conforming to RFC 3095, the implementation of RFC 4815 (“Corrections and Clarifications to RFC 3095”) is mandatory. RFC 3843 (“ROHC Profile for IP”) and RFC 4362 (“ROHC: A Link-Layer Assisted Profile for IP/UDP/RTP”) are optional.

For the use above PPP, an adapted variant of ROHC is specified in RFC 3241 (“ROHC over PPP“).

Two older but still fully functional header compression methods are specified in RFC 2507 (“IP Header Compression“) for point-to-point links and RFC 2508 (“Compressing IP/UDP/RTP Headers for Low-Speed Serial Links“).

Payload compression

Besides applying header compression, payload compression can be performed optionally, i.e. a lossless compression of the user data in messages. (An analogous example is the zipping to optimise the use of data storage.)

For this purpose, the framework specification RFC 3173 – IP Payload Compression Protocol (IPComp), enabling the use of different concrete compression algorithms, is available.

For payload compression, the same conditions and consequences apply as for header compression (low transmission rate, increased processing effort).

Addressing

The "General" section covers relevant RFCs with focus on IPv6 addressing and address-types. The use of IPv4-mapped addresses is not recommended. The inherent ambiguity of these addresses induces security risks.

The use of site-local addresses is no longer allowed; unique-local addresses (ULAs) provide a similar concept.

All nodes shall support manual/static address configuration as a basic mechanism. (Hosts and certain categories of routers need to support additional address configuration means as well.)

All nodes shall implement RFC 4862 ("IPv6 Stateless Address Autoconfiguration") (for exceptions concerning security devices see the corresponding profile sheets). It shall be possible to switch off and to configure the use of stateless address autoconfiguration. It has to be noted that RFC 4862 covers multiple classes of functions: on one hand a mechanism for the automatic address configuration of hosts and on the other hand important basic functions for the operation of IPv6 networks that are independent from automatic address configuration. Two of these functions are to be emphasized here: Link-local address configuration and duplicate address detection. The automatic generation of link-local addresses is a prerequisite for the automatic configuration of networks. Duplicate address detection (DAD) is a mandatory function to preserve the functioning of the network. Under certain operational conditions, e.g. when using mobile IP, optimistic DAD conforming to RFC 4429 can be used optionally.

Where DHCPv6 is available, the use of automatic address configuration conforming to RFC 4862 is not recommended. When automatic address configuration is used, stateless DHCPv6 may optionally be used in addition to distribute information about infrastructure servers (like DNS or NTP servers).

DNS Resolver

Largely, the DNS system is not IPv6-specific. It is contained in the profile due to extensions for the use in conjunction with IPv6 and due to the fundamental relevance of the functions. It has to be noted that not all nodes have to contain a DNS resolver. As this is the exception, DNS is mandatory.

The implementation of the router advertisement (RA) option for the configuration of the DNS

server conforming to RFC 6106 is recommended to largely enable future autoconfiguration via RA.

Under corresponding conditions, the implementation of DNSSEC is recommended, as DNS is a critical infrastructure for the operation of IP networks that should be protected.

Transition Mechanisms

Different transition mechanisms towards IPv6 (also called migration) are described in RFC 4213 ("Basic Transition Mechanisms for IPv6 Hosts and Routers").

Teredo should only be used under well-founded, extraordinary conditions.

NAT Succession

The development of the Internet and the usage has shown early that the number of IPv4 addresses will not be sufficient. Mainly, this led to two developments: the IPv6 protocol with a much larger address space and network address translation (NAT) as a bridging technology. While the implementation of IPv6 went slowly, it was identified that the NAT mechanism can be used to handle several other network problems. Relevant practically used functions of NAT are the hiding of the (addresses of) the local network infrastructure for security reasons and the persistence of the internal IP addresses even in the case of changing the Internet provider or when multi-homing is used. However, NAT violates the end-to-end principle guiding the design of the IP protocols. This principle means that a communication relationship is controlled by the peer hosts and transparently supported by the IP network. Especially, an IP network can largely operate stateless. I.e., for the correct operation of the network, routers need not to store information about a data flow from IP packet to IP packet or to change IP packets (except for forwarding related header fields). This does not cover the use of proxies or Application Layer gateways that have to evaluate the protocol data.

Numerous discussions have taken place about the pros and cons of NAT. They are not to be repeated here. It is relevant to know that the end-to-end principle is one of the basics of the design of IP protocols (and therefore an assumption protocol and application developers rely on) and that, on the other hand, NAT is used as a simple solution to perform network tasks. In some situations, both together can result in problems.

Using IPv6, there is no longer a need to use NAT. RFC 4864 ("Local Network Protection for IPv6") [RFC4864] describes several IPv6 mechanisms and how they can be used to perform network tasks. It shows the relationship between the goal, the corresponding NAT feature when IPv4 is used, and the native IPv6 mechanism.

After long discussions, RFC 6296 ("IPv6-to-IPv6 Network Prefix Translation") [RFC6296]

specifying a mechanism similar to NAT is now available. However, its use is not recommended. The usual network tasks can be performed with other IPv6 mechanisms. E.g., the persistence of the IP addresses is ensured via the addressing scheme of the public administration. The internal address and network structure is not visible due to the Application Layer gateway, proxy or reverse proxy usually used.

IPsec Protocol Family

The support of IPsec is recommended to protect the communication. Its predominant use is the establishment of tunnels between networks or sub-networks.

The current, recommended version of IPsec ("IPsec v3") is defined in RFC 4301 ("Security Architecture for the Internet Protocol") [RFC4301].

An IPsec security association (SA) simultaneously coupling IPv4 and IPv6 sub-networks is forbidden. IPv4 and IPv6 connections shall always use a dedicated session key in dedicated SAs. This does not preclude the transport if IPv4 in IPv6 or IPv6 in IPv4 in IPsec tunnel mode. This operation mode is recommended explicitly.

The use of IPsec in its actual version implies the use of IKEv2. For special scenarios, the use of IKEv1 is possible, especially when interoperability with nodes not yet being IKEv2-enabled is required.

Optionally, the use of IPsec-v2 is possible.

Concerning the support of cryptographic algorithms, the profile only provides a summary of the available standards. The technical guideline ("Technische Richtlinie") TR-02102 of the BSI [TR02102] ("Kryptographische Verfahren: Empfehlungen und Schlüssellängen") or the NIST Special Publication (SP) 800-133, *Recommendation for Cryptographic Key Generation* [NIST_KGEN] from December 21, 2012 can be used for the concrete selection and configuration. It shall be ensured that the latest version of these guidelines is used.

Multicast

In the profile, multicast is considered in its role as a necessary, basic mechanism of the IPv6 network management. This view currently does not cover the use of multicast for application purposes, e.g. for multimedia applications.

For the support of multicast listener discovery (MLD), implementation of one of the specifications RFC 3810, RFC 5790 or RFC 2710 is necessary and therefore mandatory. Preferentially, MLDv2 (RFC 3810) should be implemented, which enhances the functionality of MLDv1 by source-specific multicast. Lightweight MLDv2 (RFC 5790) is a simplified subset of MLDv2 without the 'exclude' functionality (blocking of packets from undesirable source

addresses). When MLDv1 (RFC 2710) is used, RFC 3590 (“Source Address Selection for MLD“) is mandatory and all nodes using the link shall use the MLDv1 mode.

Quality of Service (QoS)

Several methods are used to support quality of service. Typically, their use is limited to an administration, single administrational areas or to the interface to a specific Internet provider due to mutual agreements. DiffServ is the only noteworthy method used, especially due to functions that are backwards-compatible to the TOS field functions defined in IPv4.

3.4.2.2 Network / System Management

Generally, the support of network management using SNMP is recommended for all nodes. The operation of the network management system via IPv4 or IPv6 is independent from using IPv6 for the normal operation of the node. I.e. even if the normal communication of the node uses IPv6, management data can, in principle, be queried via an IPv4-based network management interface. For newly acquired devices, the use of SNMP via IPv6 shall be supported. Under normal conditions, only passive use of the network management system is envisaged, i.e. the reading access to management data, e.g. to present the network status. For security reasons, the setting of values via network management is allowed only when necessary.

In the node profile, the implementation of some specific, standardised MIBs is recommended. Generally, one should take care that the manufacturer-specific extensions of the MIBs are adapted and available for the use in conjunction with IPv6, too.

3.4.2.3 Link-Specific Requirements

In general, the network access of a node can take place via the following mechanisms

- direct use of data transmission protocols
- use of virtual links and tunnels
- use of complex access networks like mobile communications networks

In this section of the node profile, typical network access technologies from the LAN and WAN area are listed as references. This list is not necessarily complete. In general, a node will only implement the technologies it will really use.

More link-specific requirements are given in the router section.

3.4.3 Router

Routers are key components of any network infrastructure. A router is a routing and relaying device coupling nodes and complete networks at IP level. It performs routing decisions based on IP level data, primarily on the destination IP address.

The specific requirements concerning routers are categorised as follows:

- the communication of the router,
- the routing and relaying functions,
- the functions for network and system management, and
- the link-specific requirements

3.4.3.1 Communication of the Router

The communication of the router covers all functions that have to be implemented by a router to participate in IPv6 communication and the functions necessary for the management and the protection of this communication.

Basic Requirements

The response behaviour of routers concerning the transmission of ICMP error messages shall be configurable. Too many such messages can overload the network and the transmitting router.

Rate limitation for such messages is one configuration alternative. Rate limitation can be scaled up to the (temporary) blocking of ICMP error message transmission. Non-configurable response behaviour would be a risk for proper network and router operation as attackers could force the transmission of too many ICMP error messages.

On all links, it should be possible to transmit the MTU value in router advertisement messages. This prevents a more complex determination.

To detect misbehaviour of other routers, being intentional or resulting from errors, it should be possible to log inconsistent router advertisement messages. Inconsistencies are, e.g., contradictory messages from one or more routers or messages in contradiction to the knowledge of the detecting router.

All routers should support jumbograms. This can enhance the future-proofness of these central components.

Addressing

The use of 127-bit prefixes on point-to-point links (conforming to RFC 6164) limits the opportunity for attacks via hidden channels and is therefore mandatory. This function corresponds to the 31-bit prefixes commonly used on point-to-point IPv4 links.

SOHO routers shall support automatic configuration as the configuration is typically performed by the Internet service provider. For this purpose, it can be necessary that a SOHO router is able to act as a DHCPv6 client conforming to RFC 3315 (“Dynamic Host Configuration Protocol for IPv6 (DHCPv6)“). Otherwise, this address configuration method is not recommended. A CE router getting its prefix via DHCP shall implement RFC 3633 (“IPv6 Prefix Options for DHCPv6“).

It is recommended not to use privacy extensions for router address configuration conforming to RFC 4941 (“SLAAC Privacy Extensions“). Routers need a permanently valid address for proper usability.

DNS

SOHO routers shall be able to distribute DNS configuration data using router advertisements conforming to RFC 6106 (“IPv6 Router Advertisement Options for DNS Configuration“).

Transition Mechanisms

CE routers shall implement generic router encapsulation (GRE) as specified in RFC 2784 and the corresponding specific encapsulation in IPv6 packets conforming to RFC 2473 (“Generic Packet Tunnelling and IPv6“). Conforming to RFC 4891 (“Using IPsec to Secure IPv6-in-IPv4 tunnels“), this is also valid for IPsec in transport mode for IPv4 tunnels transporting IPv6 packets if no VPN crypto-gateway is used in addition. In this context, the key and numbering extensions to GRE conforming to RFC 2890 (“Key and Sequence Number Extensions to GRE“) should be available, too.

IPsec Protocol Family

The recommendations for nodes apply to routers as well.

Multicast

If the use of protocol independent multicast (PIM) in conjunction with source-specific multicast (SSM) is planned, PIM – Sparse Mode (PIM-SM) conforming to RFC 4601 (“PIM – Sparse Mode (PIM-SM)“) should be implemented. If the use of PIM without SSM is planned, PIM-SM or PIM – Dense Mode (PIM-DM conforming to RFC 3973 (“PIM – Dense Mode (PIM-DM)“) can be selected. The support of rendezvous point addresses in multicast addresses (for PIM-SM any-source multicast conforming to RFC 3956 (“Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address”) is optional.

Quality of Service (QoS)

The recommendations for nodes apply to routers as well.

Home Agent for Mobile IP

If it is planned to use the router as a home agent for mobile IP, some requirements are resulting:

- The home agent function conforming to RFC 6275 (“Mobility Support in IPv6“) as well as RFC 3776 (“Using IPsec to Protect Mobile IPv6 Signalling between Mobile Nodes and Home Agents“) and RFC 4877 (“Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture“) shall be implemented.
- It is recommended to implement RFC 4282 (“The Network Access Identifier“), RFC 4283 (“Mobile Node Identifier option for MIPv6“) and RFC 5555 (“Mobile IPv6 Support for Dual Stack Hosts and Routers“) additionally.

It is not defined finally and uniformly if network access identifiers or other service-provider-independent identifiers for mobile hosts are used in the context of pubic administrations. Nevertheless, a home agent should be prepared correspondingly. The use of service-provider-independent identifiers can be advantageous from the point of security.

For still a long time, mobile hosts will face native IPv6 or IPv4 depending on the local situation. Therefore, the corresponding home agent should provide uniform and complete support for both protocol versions.

Mobile Router

Mobile routers shall implement RFC 3963 (“Network Mobility (NEMO) Basic Support“).

3.4.3.2 Router Functions

The router functions primarily include the different routing protocols available for different local situations and supporting different roles of routers (access router or network-internal router).

Basic Requirements

In a network where it is planned to use DHCP across consecutive links, each router shall implement the DHCPv6 relay function conforming to RFC 3315. Otherwise, DHCP messages cannot reach their destination.

Routing Protocols

Several routing protocols exist. They can be used alternatively or, depending on the role of the router, simultaneously.

The following applies to routers at administrative borders, so-called exterior routers or CE routers (customer edge routers):

- They shall implement the Border Gateway Protocol 4 (BGP-4, RFC 4271) and the specifications in RFC 1772 (“Application of the Border Gateway Protocol in the Internet“), RFC 4760 (“Multiprotocol Extensions for BGP-4“) and RFC 2545 (“Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing“). RFC 4760 and RFC 2545 specify the necessary protocol extensions for the support of IPv6 as RFC 4271 and RFC 1772 were originally developed for a pre IPv4 environment.

- RFC 5492 (“Capabilities Advertisement with BGP-4“) should be implemented to enable the exchange of information about their capabilities between routers and the corresponding optimization of the procedures between them.

- It is recommended to implement RFC 2918 (“Route Refresh Capability for BGP-4“). It enables the querying of routing data previously announced by neighboring systems.

- It is recommended to implement RFC 1997 (“BGP Communities Attribute“) to enable efficient use of BGP-4 and corresponding routing tables. This makes it possible to distribute routing data corresponding to administrative requirements. It is also recommended to implement RFC 5701 (“IPv6 Address Specific BGP Extended Community Attribute“). This RFC specifies a number of community identifiers and their classification. This enables a more fine-grained differentiation of communities and simplifies filtering (based on the class).

The potential advantage of supporting virtual private networks (VPNs) based on BGP and MPLS in and by public administrations has not yet been determined. Especially, a corresponding solution had to be compared to other solutions in terms of security aspects.

As internal routing protocols within an administrative domain, several alternatives are available: Routing Information Protocol Next Generation (RIPng, RFC 2080), Open Shortest Path First (OSPF, RFC 5340 in combination with RFC 2328) and IS-IS (RFC 5308 in combination with RFC 1195, RFC 5305 and ISO/IEC 10589:2002). The selection is at the discretion of the operator of the domain and technically independent of the methods used in other – including neighbouring – domains.

- RIPng:

RFC 2080 (“RIPng for IPv6“) completely specifies RIPng for IPv6 environments.

- OSPF:

RFC 5340 (“OSPF for IPv6“) specifies the extensions / changes to OSPF version 2 (for IPv4, RFC 2328) required for IPv6 environments.

To prevent the processing of routing messages originating from unauthorised systems, the messages shall at least be protected by authentication data conforming to RFC 4552 (“Authentication / Confidentiality for OSPFv3“). RFC 4552 implies the availability of IPsec.

- IS-IS:

RFC 5308 (“Routing IPv6 with IS-IS“) specifies the extensions to RFC 1195 (“Use of OSI IS-IS for Routing in TCP/IP and Dual Environments“) in conjunction with RFC 5305 (“IS-IS Extensions for Traffic Engineering“) required to support IS-IS in IPv6 environments.

RFC 1195 only contains extensions / changes to ISO/IEC 10589:2002 („Intermediate System to Intermediate System intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service (ISO 8473)“) which therefore shall be implemented, too.

Virtual Router Redundancy Protocol (VRRP)

Under certain conditions, routers in a physical broadcast LAN, e.g. an Ethernet- or WLAN-based network, can automatically take over the duties of failed routers.

RFC 5798 („Virtual Router Redundancy Protocol (VRRP) version 3 for IPv4 and IPv6“) specifies a protocol for the configuration and the execution of the take-over without involvement of the hosts concerned.

As the method conforming to RFC 5798 reacts much faster than neighbour and router discovery methods, as it requires less communication effort and as it does not involve the hosts concerned, its availability is advantageous.

3.4.3.3 Network / System Management

The management functions especially enable remote querying of data collected about the communication by the router.

SNMP

If the use of SNMPv3 conforming to RFC 3410 (“Simple Network Management Protocol version 3“) and the numerically following RFCs is planned, routers shall implement RFC 3414 (“SNMP User based Security Model“). The querying and especially the setting of router parameters are

critical functions in terms of security and shall therefore be protected against unauthorised use.

The format of management data – especially when SNMP is used – is specified in management information bases (MIBs). Routers supporting SNMP shall implement RFC 4293 (“Management Information Base for the Internet Protocol (IP)“) and RFC 4292 (“IP Forwarding Table MIB“), too.

If the use of IP tunnelling is planned, corresponding routers shall implement RFC 4087 (”IP Tunnel MIB“). If it is planned to use a given router as a mobile IP home agent or – less often – as a mobile node or as a correspondent node (communication partner of a mobile node), the router shall implement RFC 4295 (“Mobile IPv6 Management Information Base“).

The implementation of RFC 3289 (“Management Information Base for the Differentiated Services Architecture“) is optional.

If a given router is used as an RMON agent (remote network monitoring agent), then the router shall implement RFC 3919 (“Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi-Protocol Label Switching (MPLS)“).

IPFIX / NetFlow

If it is planned to use IPFIX / NetFlow, templates with IPv6 information elements (IEs) shall be provided.

3.4.3.4 Link-Specific Requirements

The link-specific requirements describe which standards, recommendations (e.g. of the ITU) are valid for the different link types. Special emphasis was put on access network links, as a broad variety exists there.

No recommendations are given concerning the link-specific requirements. On one hand – concerning virtual links – these requirements are highly dependent on the specific situation and the use of the network where the router concerned is used. On the other hand – concerning access networks – the operators of the access networks enforce the requirements.

More link-specific requirements are given in the profile sheet “Node”.

Virtual Links

Virtual links in a router can:

- enable IPv6 communication via a (partially) IPv4-only infrastructure (e.g. an IPv4 access network), e.g. conforming to RFC 4213 (“Basic Transition Mechanisms for IPv6 Hosts and

Routers“) or RFC 5969 (“Pv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification“),

- support different Layer 3 protocols on top of an IPv6 infrastructure as specified in RFC 2473 (“Generic Packet Tunnelling in IPv6 Specification“), and

- increase the efficiency of message forwarding, e.g. using the method specified in RFC 3031 (“Multiprotocol Label Switching Architecture“), where routing is not performed for each packet individually but packets are allocated to pre-configured routes.

3.4.4 Host

Hosts are the endpoints of the communication. A large number of device classes can be distinguished: PCs as fixed workplaces in a public administration, mobile access via notebooks, internal servers for infrastructure services or servers to provide user and government applications.

The profile of the host is based on the profile of the node. Therefore, many parts contain references to requirements for nodes.

3.4.4.1 Communication of the Host

The communication of the host covers all functions that are necessary to participate in an IPv6 network.

Basic Requirements

For security reasons, it shall be configurable that a host does not react on redirect messages of the neighbour discovery protocol (NDP).

Path MTU discovery, a necessary mechanism to participate in IPv6 communication, may be implemented via higher layer protocols as specified in RFC 4821.

Addressing

It should be possible to determine the source address via a configurable rule table.

Besides static / manual address configuration, as required for each node, hosts shall implement automatic address configuration, too. The mechanisms are SLAAC or DHCPv6.

Hosts shall implement privacy extensions conforming to RFC 4941.

For sufficiently large networks, the use of DHCPv6 is recommended. When DHCPv6 is used, the host shall implement the DHCP client function. For security reasons, hosts shall ignore DHCP

options not specified for the type of a given message.

DNS

If the use of DHCP is planned, the DHCPv6 option to configure the DNS server shall be implemented.

Mobile IPv6

The support of mobile IP in the profile sheet “Host” addresses two device classes, which are distinguished in the following subsections:

- hosts communicating with mobile hosts
- mobile hosts

Non-mobile host prepared to communicate with mobile hosts

The communication between a non-mobile and a mobile host can be optimised if the non-mobile host implements the route optimization mechanism specified in chapter 8.2 of RFC 6275 (“Mobility Support in IPv6”).

In this case, the mobile host may – if no security concerns exist – accept that the communication takes place between the two hosts directly, without using the home agent of the mobile host as a forwarder. For this purpose, the non-mobile host gets informed about the actual direct IÜPv6 address (care-of address) of the mobile host.

The implementation of the route optimization mechanism is recommended.

Mobile Host

Mobile IP is available for the communication with mobile devices. It is specified in RFC 6275 (“Mobility Support in IPv6”). A conforming mobile host shall implement the functions specified in chapter 8.5 of this RFC.

Mobile hosts should support the route optimization mechanism described above, too. It can only be used if it is implemented by all hosts and home agents (see chapter 4.3) involved in a given communication.

The home agent functions specified in RFC 6275 are not used in a host. Thus, an implementation is superfluous.

For the management of the communication with mobile hosts, these must be able to exchange data with their home agent (a component on a router of the home network) in a trustable –

and, if required, a privacy-protecting – way. For this purpose, the implementation of RFC 3776 (“Using IPsec to Protect Mobile IPv6 Signalling Between Mobile Nodes and Home Agents”) and of RFC 4877 (“Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture”) is mandatory.

As mobile hosts are often used in networks of different operators, they should implement RFC 4283 (“Mobile Node Identifier option for MIPv6“) and RFC 4282 („The Network Access Identifier”). This enables an identification of device or user independent from the home IP address of the host, e.g. for accounting purposes.

Originally, mobile IP was specified for the support of IPv6 only. However, it can be used for IPv4 with minor extensions. Therefore, it is advantageous to use a common protocol specification of both IP variants. The necessary extensions are specified in RFC 5555 (“Mobile IPv6 Support for Dual Stack Hosts and Routers”) and should be implemented by mobile dual-stack hosts.

3.4.4.2 Application Support

On hosts, not only the direct network functions are relevant for the functioning in an IPv6 environment. Additionally, certain mechanisms of the applications have to support IPv6. Input masks for IP addresses, especially of web browsers, are an example as well as the size of internal data fields to store these addresses. In this section of the host profile, a several RFCs are listed that specify APIs for which IPv6 support is necessary. These RFCs shall be implemented if corresponding functions are used by applications running on a given host, e.g. via the access to software libraries.

An application shall take into account the mentioned RFCs for the selection and use of multicast addresses if the application uses multicast communication.

3.4.4.3 Network / System Management

The .network and System management is described by the node profile. It is recommended, especially for servers, to implement the MIB conforming to RFC 2790. It makes it possible to query the actual performance data of the host. It has to be noted that this MIB is not IPv6-specific.

3.4.5 Security Components

This section covers several components:

- packet filters
- application layer gateways

- VPN crypto-gateways
- intrusion detection / prevention systems (IDS, IPS)

In the following, only recommendations and ratings concerning the specific functionality of the component concerned are given. Components additionally providing other functions (e.g. as a host or router), shall comply with the requirements for these functions, too.

The specific functionality of security components is scarcely specified by RFCs or other standards (up to now). Therefore, both the corresponding profile sheets and this description are considerably different from the basic network components (hosts and routers).

The functionality of IPv6 packet filters and application layer gateways is determined by local functions in the corresponding security components. The functionality of VPN crypto-gateways is determined by bilateral, partially proprietary protocols between peer gateways. Therefore, the corresponding profile sheets primarily describe necessary or recommended (observable) capabilities of such components. Less emphasis is put on the concrete implementation of these capabilities.

It has to be noted that certain functions are deliberately not implemented by security components as many functions can increase the vulnerability for attacks. In a real environment, it has to be ensured that the device used is well adapted to the usage scenario. Therefore, intended deviations from the profiles are possible for security components.

Intrusion detection / prevention systems are not covered here due to the large number of different approaches.

3.4.5.1 General Requirements for Security Components

Security components are transit systems, i.e. they forward incoming data packets if these are qualified as secure or after they have been changed correspondingly.

All transit systems have to support the following function categories:

- general
- communication of the transit system
- network / system management
- support of the transit traffic
- self-protection while performing the specific protection functions

Due to security requirements, deviations between the requirements described in the profile and real functions of security devices are possible. Clarify the details with the manufacturer concerned. Due to its checklist nature, the profile can support this clarification.

Generally, the functions and the performance of a security component should at least be in accordance with those of a (existent) corresponding IPv4 component.

When an IPv4 network is migrated, it is recommended to analyse first, which of the functions of the IPv4 security components should be available in the IPv6 environment, too, to reach at least equivalent functionality between IPv6 and IPv4 use.

This analysis is especially important as most of the concrete security functions are not specified in RFCs or standards and implemented in different detail using manufacturer-specific mechanisms.

Here, the functions of the security components are classified as follows: general communication functions, support of the transit traffic, supported network / system management functions and the specific protection functions.

A security component has to provide communication functions to be able to participate in IPv6 communication. The requirements are largely equivalent to those for IPv6 nodes as described in section 3.4.2.1.

As long as trustable neighbour discovery (e.g. using SEND) is not available, security devices should ignore incoming router advertisements. A misrouting of the data traffic, especially when it happens near to central components like security devices, can have a dramatic influence on the performance and the security of the network.

For point-to-point links, the implementation of RFC 6164 (“Using 127-Bit IPv6 Prefixes on Inter-Router Links”) is mandatory to prevent hidden channels.

The implementation of RFC 4862 (“IPv6 Stateless Address Autoconfiguration”) is not mandatory, but the following functions should be implemented:

- on-demand deactivation of address autoconfiguration
- on-demand permanent setting of the managed address configuration flag and the other stateful configuration flag in IPv6 messages
- configuration of the link-local addresses using SLAAC
- multiple address detection using SLAAC
- on-demand deactivation of multiple address detection using SLAAC for

multicast interfaces

It is not recommended to configure addresses other than link-local ones using SLAAC.

The support of the transit traffic covers the functions additionally required to forward compliant user and control data by the security component. These are:

- the recommended implementation of jumbogram support,
- the support of neighbour discovery by other nodes via router advertisements and router solicitation and
- the forwarding of DHCP messages.
- The mechanisms to support quality of service applied in the network concerned should be implemented. Quality of service can only be provided if it is supported by all components on a given data path.

In the area of network / system management, a monitoring of the network components is recommended. Typically, SNMP is used for this purpose. Details concerning the SNMPv3 RFCs are given in section 3.4.2.2 and the corresponding profile sheet. For security reasons, it may be necessary to use an SNMP proxy. This enables to configure read-only access to the configuration data and to block the changing of configuration data via writing access.

The general management and configuration requirements valid for all IPv6 devices are detailed in section 3.4.7.

Security devices shall provide administration functions and be protected against unauthorised access. Authorisation and authentication are mandatory for the access to configuration function. If unauthorised access is suspected, the components shall log corresponding events and send alarms.

A security device shall protect itself against compromising its functioning when applying its specific protection functions. Security components are prominent attack targets themselves. A successful attack can influence whole sub-networks.

Typical attacks target a malfunction, a performance reduction or a total breakdown in the case of overload.

Self-protection addresses the protection of the resources for packet processing against attacks. Nevertheless, it shall be ensured that packets cannot circumvent their analysis applying such attacks. In a resource-critical situation, security components should drop packets that cannot be analysed sufficiently.

A security component shall implement protection against fragmentation attacks. This is important both in IPv43 and in IPv6 networks. It has to be noted that security components must reassemble packets for detailed analysis even though reassembly is envisaged in hosts only.

General self-protection requirements (valid for both IPv4 and IPv6) are:

- The intended protection quality shall be reached even under heavy load conditions. If necessary, the component shall create an alarm and block the communication completely.
- The configuration of a security component should be protected against manipulation. A typical mechanism is to keep a signed copy of the configuration data – possibly on a separate component – and the regular comparison of the configuration with this copy.

3.4.5.2 IPv6 Packet Filter

A packet filter controls the connection between networks and protects a network against attacks from outside. It cannot protect against internal attacks. It can only protect on the layer(s) where it is applied (depth of analysis). A Network Layer packet filter cannot protect against Application Layer attacks.

In general, it has to be noted that the use of packet filters is one of a large number of security measures. Packet filters should be combined in a useful way with other measures (e.g. intrusion detection systems) to establish several lines of defence.

Packet filter functions are categorized as follows:

- general
- communication of the packet filter
- support of the transit traffic
- network / system management
- packet filter functionality (protection functionality) consisting of
    - self-protection of the packet filter device
    - packet analysis

The requirements related to the different categories are given in the profile sheet “Packet Filter” and are explained below, if necessary.

The requirements of the categories ”general”, communication of the packet filter, support of the transit traffic and network / system management are those which are valid for security components in general (see section 3.4.5.1).

In practice, many devices with a packet filter component works as a router, too. In this case, the requirements for IPv6 routers given in profile sheet “Router” and in section 3.4.3 shall also be fulfilled.

The core packet filter functionality – the protection of the internal edge components against attacks from outside and the protection of internal data against unauthorized diffusion to the outside – includes the protection of the resources of the packet filter against attacks and the analysis of incoming IP control data.

In a dual-stack environment, a packet filter analyses both, IPv6 and IPv4 packets, or a single protocol version only. In the latter case, it shall be ensured that all packets of the unsupported IP version are dropped.

Besides the general self-protection functions of security components, a packet filter shall be prepared against attacks with long chains of extension headers. Attacks using options in hop-by-hop extension headers should be detected and handled, too. These attacks are iPv6-specific.

Packet Analysis

Concerning the analysis of incoming user and control data, we distinguish the following categories:

- functions for all packets
- fragmented packets
- jumbograms
- encapsulated packets
- packets containing extension headers
- ICMP packets

Concerning the functions for all packets, the following particularities shall be taken into account:

- Blocking of packets based on port numbers, protocol type, and IP addresses (mandatory): It shall be possible to configure the blocking of arbitrary protocols, source and destination port numbers and source and destination IP addresses and of

arbitrary combinations thereof. This functionality is required for both IPv4 and IPv6 packet filters. Special emphasis has to be put on the fact that all IP address types shall be supported.

- Asymmetrical blocking (mandatory): It shall be possible to limit the blocking based on specific IP header contents to one transmission direction (outgoing or incoming). This functionality is required for both IPv4 and IPv6 packet filters.

- IP header analysis (mandatory): As the IPv6 header is different from the IPv4 header, this function shall for be implemented for IPv6 specifically and it shall support all mandatory, recommended and optional header fields.

- Handling of IPsec traffic (mandatory): Depending on the requirements of the operator, a packet filter shall be able to block IPsec connections completely or to selectively block IPsec traffic based on certain IP header contents.

- Stateful packet inspection (mandatory): This functionality is required for both IPv4 and IPv6 packet filters. However, specific functions shall be implemented for IPv6 packets, e.g. for the rate limitation of ICMPv6 packets.

- Detection of malformed packets (mandatory): This is necessary in IPv6 packets, too. As IPv4 and IPv6 packets are different, specific functions are required for IPv6 packets.

- Detection of small packets (< 1280 octets) (recommended): especially many small fragments of large messages may be an indication for a denial of service attack. This kind of attack is possible in IPv4 networks, too. However, specific functions are required for IPv6 as the packet, fragment and message sizes, and the fragmentation strategy are different between IPv4 and IPv6.

- Detection of known attacks (recommended): This recommendation is unspecific and therefore not justiciable, but it is a placeholder for concrete known attacks that can be named by potential customers or by a provider.

- Detection of port scans (recommended): Typically, port scanning is a pre-stage of a dedicated attack. However, it can be a denial of service attack, too. This functionality is useful for both IPv4 and IPv6 packet filters.

- Detection of host scans (recommended): In general, host scanning is a pre-stage of a dedicated attack. However, it can be a denial of service attack, too. This functionality is useful for both IPv4 and IPv6 packet filters. However, different attacker behaviour may be expected as for IPv6 the address space is larger and other address types and

well-known addresses exist.

- Port-to-application mapping (optional): The rule-based change of the port typically used for an application by a packet filter can prevent attacks and/or enable access of different user groups to different functional subsets of an applications. This functionality is useful for both IPv4 and IPv6 packet filters.

It shall not be possible that fragmentation or the use of extension headers circumvents the analysis of a packet by the packet filter. All packet filters shall implement functions to analyse such packets.

When handling fragmented packets, the following particularities shall be taken into account:

- Logging of the number of fragmented packets per source IP address for the detection of possible denial-of-service attacks.
- Reassembly of fragmented packets (recommended): In contrary to RFC 2460, reserving reassembly for hosts, a packet filter should reassemble packets for in-depth analysis. Compliant packets can be forwarded after the analysis without a new fragmentation if the fragments are stored for this purpose.

When handling tunneled packets, the following particularities have to be taken into account:

- Detection, analysis and blocking functions for tunnelled packets (mandatory): In extension to the functionality for native packets, it shall be possible to block certain kinds of encapsulation completely.
- Stateful packet inspection (mandatory): This functionality shall be available for encapsulated packets, too.
- Detection of IPv6-inIPv6 encapsulation (mandatory): IPv6-inIPv6 encapsulation may be an attempt to prevent analysis of packets.

When handling packets with extension headers, the following particularities have to be taken into account:

- Detection and interpretation of extension headers (mandatory): Possible sub-functions are:
  - Detection of unusual header order (mandatory)
  - Detection of unusual header repetition (mandatory)
  - Detection of the extensive use of options in hop-by-hop headers (mandatory)

- Detection of invalid options (mandatory)
- Detection of padding octets that are not zero-filled (mandatory).

When handling ICM;Pv6 packets, the following has to be taken into account:

- Filtering of ICMPv6 packets conforming to RFC 4890 (mandatory): ICMPv6 packets may not be blocked generally as some of them contain essential messages (e.g. message-too-big messages).

3.4.5.3 Application Layer Gateways

An Application Layer gateway has the task to monitor the communication necessary for one or more specific applications and to change or block this communication if necessary. For this purpose, transport connections are terminated by the Application Layer gateway. The Application Layer gateway performs internal routing and relaying of the application messages between incoming and outgoing transport connections.

Formally, an Application Layer gateway could act independently from the IP version used. Practically, dependencies exist to the used IP version via the availability of different and/or additional functions.

The Application Layer gateway functions are categorized as follows:

- general
- communication of the Application Layer gateway
- support of the transit traffic
- network / system management
- filter / protection functions consisting of
  - self-protection of the Application Layer gateway device
  - packet analysis

The requirements for the individual categories are given in the profile sheet “Application Layer Gateway” and detailed below, if necessary.

To a large extent, the requirements of the categories ”general”, communication of the Application Layer gateway, support of the transit traffic and network / system management are those which are valid for security components in general (see section 4.5.1).

Additionally, an Application Layer gateway should be able to perform Packetization Layer Path MTU Discovery conforming to RFC 4821 (the determination of the maximum packet size by evaluating application-related traffic).

For the non-transparent, authenticated access from external networks, the SOCKS5 protocol [RFC 1928] is available. Its provisioning – including secure configuration facilities – by Application Layer gateways is recommended.

In practice, many devices with an Application Layer gateway component work as a router, too. In this case, the requirements for IPv6 routers given in profile sheet "Router" and in section 4.3 shall also be fulfilled. Besides that, combinations between Application Layer gateways and packet filters exist. In this case, the requirements of the profile sheet "Packet Filter" and of section 4.5.2 shall be fulfilled additionally.

The core Application Layer gateway functionality – the protection of the internal edge components against attacks from outside and the protection of internal data against unauthorized diffusion to the outside – includes the protection of the resources of the Application Layer gateway against attacks, the analysis of incoming user and control data and, if necessary, the changing of this data.

Packet Analysis

The evaluation of incoming user and control data is further categorized as follows:

- functions for all messages
- typical applications
- Concerning the functions for all messages, the following particularities have to be taken into account:
- In general, both user and control data of the protocols and layers concerned shall be handled.
- It shall be possible to block (i.e. discard) messages of undesirable protocols completely.
- Configurable blocking or changing of port numbers and addresses as far as these are explicitly exchanged with the IP layer (mandatory)
- Asymmetrical blocking (mandatory): It shall be possible to limit the blocking based on application protocol type, individual protocol functions, port numbers and/ or addresses to one direction of initiation (from internal to external or from external to

internal). For example, HTTP request could be limited to the outgoing direction, corresponding answers to the incoming direction.

- Configurable blocking or changing of options of the lower layers, as far as these are explicitly exchanged with the IP layer (mandatory)
- Detection of non-conforming messages (mandatory): For the supported protocols, a complete analysis of the messages shall be possible.
- Analysis / blocking of fragmented messages (mandatory): It shall not be possible that fragmentation circumvents the analysis of a message by the Application Layer gateway. Application Layer gateways shall b able to detect and to handle fragmentation above the IP layer.
- Reassembly of fragmented messages (recommended): An Application Layer gateway should reassemble application-related messages for in-depth analysis. Compliant messages can be forwarded after the analysis without a new fragmentation if the fragments are stored for this purpose.
- Analysis and blocking functions for encrypted messages (mandatory): It shall be possible to analyze and/or discard encrypted messages.
- Analysis and blocking functions for tunneled messages (mandatory): It shall be possible to block certain kinds of encapsulation completely.
- Detection and handling of known attacks (recommended): This recommendation is unspecific, but it is a placeholder for concrete known attacks that can be named by potential customers or by a provider.
- An Application Layer gateway shall be able to handle all typical applications of a given public administration in an appropriate way and corresponding to the latest state concerning typical message fields and message sequences.
- Generally, typical applications are webserver communication (HTTP), e mail, file transfer (in e-mail messages, via FTP) and applications for network and system management.
- Taking into account the increasing use of voice-over-IP, Application Layer gateways should implement corresponding support even if no use of voice-over-IP is planned yet.

3.4.5.4 VPN Crypto-Gateway

A VPN crypto-gateway provides protected virtual links via insecure, especially public, networks. It works application-independent.

The VPN crypto-gateway functions are categorized as follows:

- general
- communication of the VPN crypto-gateway
- support of the transit traffic
- network / system management
- VPN crypto-gateway functionality consisting of
    - self-protection of the VPN crypto-gateway device
    - VPN crypto-gateway tunnelling variants

The requirements for the individual categories are given in the profile sheet “VPN Crypto-Gateway” and detailed below, if necessary.

To a large extent, the requirements of the categories ”general”, communication of the VPN crypto-gateway, support of the transit traffic and network / system management are those which are valid for security components in general (see section 3.4.5.1).

If it is planned to use a given VPN crypto-gateway directly at a redundant interface controlled via VRRP, the VPN crypto-gateway shall implement RFC 5798 („Virtual Router Redundancy Protocol (VRRP) version 3 for IPv4 and IPv6“).

The same is valid for the implementation of the IPv6 variant of the hot router standby protocol (HSRP) for corresponding interfaces. There exists no RFC for this protocol variant.

Besides the general self-protection functions for security components, a VPN crypto-gateway shall be prepared against attacks with long chains of extension headers. Attacks using options in hop-by-hop extension headers should be detected and handled, too. These attacks are iPv6-specific.

A VPN crypto-gateway shall support all possible combinations of IP versions for the operation of the virtual link on one hand and for the transported data traffic on the other hand. Especially if a dual-stack gateway is to be expected at the remote side, simultaneous IPv6- and iIPv4-based links shall be possible.

3.4.6 Infrastructure Servers

This profile sheet covers different functional network components that are typically required for proper network operation. These components can be realised as individual server devices. In this case, they are based on the host profile. Alternatively, they can be integrated in a router device. The requirements for an infrastructure server are only relevant if the use of the corresponding IPv6 functionality is planned.

3.4.6.1 DHCP Server

The capabilities of a DHCPv6 server are specified in RFC 3315 (“Dynamic Host Configuration Protocol for IPv6 (DHCPv6)“). Via several DHCPv6 options, the addresses of different (further) infrastructure servers can be configured on the DHCPv6 clients. Due to their central importance for the proper operation of a network, the implementation of the DHCPv6 options for DNS and NTP servers on clients is deemed mandatory. The support of further DHCPv6 options is recommended if and when implementations are available.

3.4.6.2 DNS Server

Due to the relevance of DNS, the profile contains recommendations for the operation of a DNS server even though it is – largely – not IPv6-specific.

The use of a recursive DNS resolver is mandatory. Typically, it will access the DNS server of the provider.

3.4.6.3 RADIUS Server

If a RADIUS server [RFC2865] is used for AAA (authentication, authorization and accounting) when accessing IPv6 networks (e.g. for WLAN authentication), it shall be able to handle IPv6 addresses and address parts. The necessary RADIUS attributes are specified in RFC 3162 (“RADIUS and IPv6”). The RADIUS protocol itself is located above UDP and thus independent from the IP version.

3.4.6.4 Tunnel Broker

A tunnel broker enables the automatic establishment of a tunnel to attach a sub-network or a client to an existing IPv6 infrastructure. This efficiently supports the migration phase towards IPv6 where access to a native IPv6 or dual-stack network is not yet provided by Internet service provider at all possible locations.

3.4.7 Management and Configuration

Most of the IPv6-enabled devices used in a public administration have configurable communication parameters and one or more interfaces (local user interfaces, webservers, dedicated applications for remote access) to perform this configuration and to query static device characteristics, configuration values and logged data.

In the following, only interfaces for remote access are addressed. The requirements / recommendations are independent of the kind of interface used, i.e. if a separate physical management and configuration interface is provided or if the corresponding communication takes place “in-band” (via a common interface used for other applications, too).

Configuration settings and relevant, locally logged events shall be available after a power outage. Otherwise, a complete tracking of configuration operations would not be possible.

All devices should be equipped with at least one management and configuration interface for remote access. The opportunity to configure and query all devices in an administrative domain from a central point does not only increase the comfort and the efficiency of these operations. Coincidentally, the risk to miss updates and critical events is reduced. This is especially important if devices may be not physically accessible (e.g.in locked rooms).

In principle, a management / configuration interface should be accessible via both IPv4 and IPv6. If the use of one of these protocols is (temporarily) not possible or undesirable, it should be possible to block the protocol concerned.

Static, configurable and logged data shall be protected against unauthorized access (including local access). For remote access, appropriate authentication and authorization mechanisms shall be implemented.

It should be possible to enable access to logging data and alarms via IPv4 and IPv6 (like to the configuration). It should be possible to disable one of the protocol versions when it is (temporarily) not used for practical operation.

If a management and configuration interface uses IPsec and IPv6 transmission in an IPv4 tunnel, it shall be possible to protect this IPv6 transmission using IPsec. At the terminal, it is possibly not visible that a tunnel is part of the communication path. A later omission of the tunnel (due to seamless IPv6 availability) shall not require changes at the terminal.

3.4.8 Enterprise Switch

Even though (layer 2) switches forward data below the IP layer, they should be able to detect and handle certain IPv6 packets. Two aspects have to be distinguished:

- It should be possible to block the forwarding of packets that can be classified on the ingress side as being critical or that should not be forwarded for functional reasons. Corresponding requirements are given in the section “Data monitoring and filtering” of the profile sheet “Enterprise Switch”.

- Some IPv6 mechanisms are dependent on the availability of certain functions on all forwarding devices on the data path. These functions should be implemented even if the use of the dependent, higher layer functions is not yet planned. In the corresponding profile sheet “Enterprise Switch”, such requirements are given in the sections “Quality of Service (QoS)” and “Multicast”.

If the management and configuration interface of the switch shall support IPv6 communication, the corresponding profile sheets, e.g. “Node”, are valid.

4. CONCLUSIONS

As the development around IPv6 is still quite dynamic, and many new RFCs related to IPv6 are still published each year, also the recommendations will develop in future revisions of the profile documents. These upcoming standards, plus practical experiences of network equipment vendors and users mandate updating of the documents in the future. Differences in profiles existing in EU context should be discussed and removed in the updates, or the detailed explanation of the reason should be given. We propose to use both the RIPE and the German profiles depending of the intended purpose. The proposed solution does not exclude the development of further profiles in other EU countries, as far as the profiles remain consistent to each other.

5. REFERENCES

[Cho09]	Choudhary, A.R., "In-depth analysis of IPv6 security posture", *5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, CollaborateCom 2009*, 11-14 Nov. 2009, doi: 10.4108/ICST.COLLABORATECOM2009.8393
[IPv6_Migration]	BVA, „IPv6 Migrationsleitfaden für die öffentliche Verwaltung“, online verfügbar unter http://www.ipv6.bva.bund.de
[IPv6Ready]	IPv6 Ready Logo Program, https://www.ipv6ready.org/
[NIST_119]	NIST, “Guidelines for the Secure Deployment of IPv6“, December 2010.
[NIST_KGEN]	NIST Special Publication (SP) 800-133, Recommendation for Cryptographic Key Generation, http://dx.doi.org/10.6028/NIST.SP.800-133
[NIST_USGv6]	NIST, „A Profile for IPv6 in the U.S. Government – Version 1.0“, NIST Special Publication 500-267, July 2008, http://www-x.antd.nist.gov/usgv6/docs/usgv6-v1.pdf
[RFC2460]	Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998, http://www.rfc-editor.org/rfc/rfc2460.txt
[RFC4294]	Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, April 2006, http://www.rfc-editor.org/rfc/rfc4294.txt
[RFC4864]	Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, Mai 2007, http://www.rfc-editor.org/rfc/rfc4864.txt
[RFC6071]	Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011, http://www.rfc-editor.org/rfc/rfc6071.txt
[RFC6204]	Singh, H., Beebee, W., Donley, C., Stark, B., and O. Troan, Ed., "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011, http://www.rfc-editor.org/rfc/rfc6204.txt
[RFC6434]	Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011, http://www.rfc-editor.org/rfc/rfc6434.txt
[ripe-501]	Jan Žorž, Sander Steffann, „Requirements For IPv6 in ICT Equipment“, RIPE NCC, ripe-501, Nov 2010, http://www.ripe.net/ripe/docs/ripe-501
[ripe-554]	Merike Käo, Jan Žorž, Sander Steffann, „Requirements for IPv6 in ICT Equipment“, RIPE NCC, ripe-554, http://www.ripe.net/ripe/docs/current-ripe-documents/ripe-554

[TR02102]	BSI, „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Technische Richtlinie TR-02102, Version 1.0, 20.06.2008, online verfügbar unter https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
[UCR08_2]	Department of Defense, "Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)", December 2010 Changes to UCR 2008, Change 2, Section 5.3.5, IPv6 Requirements, online verfügbar unter http://www.disa.mil/Services/NetworkServices/UCCO/~/media/Files/DISA/Services/UCCO/UCR2008-Change-2/07UCR08Chg2Section535.pdf
[UCR08_3]	Department of Defense, "Unified Capabilities Requirements 2008, Change 3 (UCR 2008, Change 3)", September 2011, online verfügbar unter http://www.disa.mil/Services/Network-Services/UCCO/~/media/Files/DISA/Services/UCCO/UCR2008-Change-3/01_UCR08_Chg3_Sections_1-4.pdf

6. REFERRED RFCS

RFC1195	Callon, R., "Use of OSI IS-IS for routing in TCP/IP and dual environments", RFC 1195, December 1990.
RFC1772	Rekhter, Y. and P. Gross, "Application of the Border Gateway Protocol in the Internet", RFC 1772, March 1995.
RFC1928	Leech, M., Ganis, M., Lee, Y., Kuris, R., Koblas, D., and L. Jones, "SOCKS Protocol Version 5", RFC 1928, March 1996.
RFC1981	McCann, J., Deering, S., and J. Mogul, "Path MTU Discovery for IP version 6", RFC 1981, August 1996.
RFC1997	Chandra, R., Traina, P., and T. Li, "BGP Communities Attribute", RFC 1997, August 1996.
RFC2080	Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.
RFC2205	Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", RFC 2205, September 1997.
RFC2207	Berger, L. and T. O'Malley, "RSVP Extensions for IPSEC Data Flows", RFC 2207, September 1997.
RFC2210	Wroclawski, J., "The Use of RSVP with IETF Integrated Services", RFC 2210, September 1997.
RFC2281	Li, T., Cole, B., Morton, P., and D. Li, "Cisco Hot Standby Router Protocol (HSRP)", RFC 2281, March 1998.
RFC2328	Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.
RFC2401	Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.
RFC2402	Kent, S. and R. Atkinson, "IP Authentication Header", RFC 2402, November 1998.
RFC2404	Madson, C. and R. Glenn, "The Use of HMAC-SHA-1-96 within ESP and AH", RFC 2404, November 1998.
RFC2406	Kent, S. and R. Atkinson, "IP Encapsulating Security Payload (ESP)", RFC 2406, November 1998.
RFC2407	Piper, D., "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, November 1998.
RFC2408	Maughan, D., Schertler, M., Schneider, M., and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)", RFC 2408, November 1998.
RFC2409	Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)", RFC 2409, November 1998.
RFC2410	Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.

RFC2451	Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.
RFC2460	Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
RFC2464	Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.
RFC2467	Crawford, M., "Transmission of IPv6 Packets over FDDI Networks", RFC 2467, December 1998.
RFC2473	Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.
RFC2474	Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.
RFC2475	Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
RFC2491	Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, January 1999.
RFC2492	Armitage, G., Schulter, P., and M. Jork, "IPv6 over ATM Networks", RFC 2492, January 1999.
RFC2507	Degermark, M., Nordgren, B., and S. Pink, "IP Header Compression", RFC 2507, February 1999.
RFC2508	Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", RFC 2508, February 1999.
RFC2516	Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.
RFC2526	Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, March 1999.
RFC2545	Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, March 1999.
RFC2553	Gilligan, R., Thomson, S., Bound, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 2553, March 1999.
RFC2597	Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.
RFC2637	Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.
RFC2671	Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.
RFC2675	Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.

RFC2710	Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
RFC2711	Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.
RFC2746	Terzis, A., Krawczyk, J., Wroclawski, J., and L. Zhang, "RSVP Operation Over IP Tunnels", RFC 2746, January 2000.
RFC2747	Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.
RFC2750	Herzog, S., "RSVP Extensions for Policy Control", RFC 2750, January 2000.
RFC2766	Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
RFC2784	Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.
RFC2790	Waldbusser, S. and P. Grillo, "Host Resources MIB", RFC 2790, March 2000.
RFC2872	Bernet, Y. and R. Pabbati, "Application and Sub Application Identity Policy Element for Use with RSVP", RFC 2872, June 2000.
RFC2890	Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.
RFC2894	Crawford, M., "Router Renumbering for IPv6", RFC 2894, August 2000.
RFC2918	Chen, E., "Route Refresh Capability for BGP-4", RFC 2918, September 2000.
RFC2961	Berger, L., Gan, D., Swallow, G., Pan, P., Tommasi, F., and S. Molendini, "RSVP Refresh Overhead Reduction Extensions", RFC 2961, April 2001.
RFC2983	Black, D., "Differentiated Services and Tunnels", RFC 2983, October 2000.
RFC2996	Bernet, Y., "Format of the RSVP DCLASS Object", RFC 2996, November 2000.
RFC3031	Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.
RFC3053	Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.
RFC3095	Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.
RFC3140	Black, D., Brim, S., Carpenter, B., and F. Le Faucheur, "Per Hop Behavior Identification Codes", RFC 3140, June 2001.

RFC3146	Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", RFC 3146, October 2001.
RFC3162	Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.
RFC3168	Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.
RFC3173	Shacham, A., Monsour, B., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 3173, September 2001.
RFC3175	Baker, F., Iturralde, C., Le Faucheur, F., and B. Davie, "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175, September 2001.
RFC3181	Herzog, S., "Signaled Preemption Priority Policy Element", RFC 3181, October 2001.
RFC3182	Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S., and R. Hess, "Identity Representation for RSVP", RFC 3182, October 2001.
RFC3226	Gudmundsson, O., "DNSSEC and IPv6 A6 aware server/resolver message size requirements", RFC 3226, December 2001.
RFC3241	Bormann, C., "Robust Header Compression (ROHC) over PPP", RFC 3241, April 2002.
RFC3246	Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.
RFC3247	Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, "Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)", RFC 3247, March 2002.
RFC3260	Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, April 2002.
RFC3289	Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.
RFC3306	Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, August 2002.
RFC3307	Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", RFC 3307, August 2002.
RFC3315	Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
RFC3319	Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, July 2003.
RFC3392	Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", RFC 3392, November 2002.

RFC3410	Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.
RFC3411	Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.
RFC3412	Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.
RFC3413	Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.
RFC3414	Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.
RFC3415	Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.
RFC3416	Presuhn, R., Ed., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.
RFC3418	Presuhn, R., Ed., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.
RFC3484	Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.
RFC3493	Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.
RFC3513	Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.
RFC3526	Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.
RFC3542	Stevens, W., Thomas, M., Nordmark, E., and T. Jinmei, "Advanced Sockets Application Program Interface (API) for IPv6", RFC 3542, May 2003.
RFC3566	Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.
RFC3572	Ogura, T., Maruyama, M., and T. Yoshida, "Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)", RFC 3572, July 2003.
RFC3590	Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, September 2003.

RFC3596	Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.
RFC3602	Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.
RFC3633	Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
RFC3646	Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.
RFC3678	Thaler, D., Fenner, B., and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", RFC 3678, January 2004.
RFC3686	Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.
RFC3736	Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.
RFC3775	Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
RFC3776	Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.
RFC3810	Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
RFC3843	Jonsson, L-E. and G. Pelletier, "RObust Header Compression (ROHC): A Compression Profile for IP", RFC 3843, June 2004.
RFC3879	Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, September 2004.
RFC3898	Kalusivalingam, V., "Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3898, October 2004.
RFC3919	Stephan, E. and J. Palet, "Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)", RFC 3919, October 2004.
RFC3948	Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.
RFC3956	Savola, P. and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, November 2004.
RFC3963	Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
RFC3971	Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.
RFC3972	Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

RFC3973	Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.
RFC3986	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
RFC4007	Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, March 2005.
RFC4022	Raghunarayan, R., Ed., "Management Information Base for the Transmission Control Protocol (TCP)", RFC 4022, March 2005.
RFC4033	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.
RFC4034	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.
RFC4035	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.
RFC4038	Shin, M-K., Ed., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "Application Aspects of IPv6 Transition", RFC 4038, March 2005.
RFC4075	Kalusivalingam, V., "Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6", RFC 4075, May 2005.
RFC4087	Thaler, D., "IP Tunnel MIB", RFC 4087, June 2005.
RFC4106	Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.
RFC4109	Hoffman, P., "Algorithms for Internet Key Exchange version 1 (IKEv1)", RFC 4109, May 2005.
RFC4113	Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)", RFC 4113, June 2005.
RFC4191	Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.
RFC4193	Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.
RFC4213	Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
RFC4241	Shirasaki, Y., Miyakawa, S., Yamasaki, T., and A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service", RFC 4241, December 2005.
RFC4271	Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.
RFC4282	Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.

RFC4283	Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.
RFC4291	Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
RFC4292	Haberman, B., "IP Forwarding Table MIB", RFC 4292, April 2006.
RFC4293	Routhier, S., Ed., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.
RFC4294	Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, April 2006.
RFC4295	Keeni, G., Koide, K., Nagami, K., and S. Gundavelli, "Mobile IPv6 Management Information Base", RFC 4295, April 2006.
RFC4301	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
RFC4302	Kent, S., "IP Authentication Header", RFC 4302, December 2005.
RFC4303	Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
RFC4306	Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
RFC4307	Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.
RFC4308	Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, December 2005.
RFC4309	Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.
RFC4311	Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, November 2005.
RFC4338	DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", RFC 4338, January 2006.
RFC4360	Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.
RFC4362	Jonsson, L-E., Pelletier, G., and K. Sandlund, "RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP", RFC 4362, January 2006.
RFC4364	Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.
RFC4380	Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.
RFC4429	Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, April 2006.

RFC4434	Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, February 2006.
RFC4443	Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.
RFC4489	Park, J-S., Shin, M-K., and H-J. Kim, "A Method for Generating Link-Scoped IPv6 Multicast Addresses", RFC 4489, April 2006.
RFC4495	Polk, J. and S. Dhesikan, "A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow", RFC 4495, May 2006.
RFC4541	Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.
RFC4543	McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.
RFC4552	Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.
RFC4577	Rosen, E., Psenak, P., and P. Pillay-Esnault, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4577, June 2006.
RFC4581	Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format", RFC 4581, October 2006.
RFC4584	Chakrabarti, S. and E. Nordmark, "Extension to Sockets API for Mobile IPv6", RFC 4584, July 2006.
RFC4594	Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.
RFC4601	Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
RFC4604	Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.
RFC4607	Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
RFC4609	Savola, P., Lehtonen, R., and D. Meyer, "Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements", RFC 4609, October 2006.
RFC4659	De Clercq, J., Ooms, D., Carugi, M., and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN", RFC 4659, September 2006.

RFC4684	Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, November 2006.
RFC4718	Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", RFC 4718, October 2006.
RFC4760	Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.
RFC4807	Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", RFC 4807, March 2007.
RFC4809	Bonatti, C., Ed., Turner, S., Ed., and G. Lebovitz, Ed., "Requirements for an IPsec Certificate Management Profile", RFC 4809, February 2007.
RFC4815	Jonsson, L-E., Sandlund, K., Pelletier, G., and P. Kremer, "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095", RFC 4815, February 2007.
RFC4821	Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.
RFC4835	Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.
RFC4861	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
RFC4862	Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
RFC4864	Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.
RFC4868	Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.
RFC4869	Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, May 2007.
RFC4877	Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.
RFC4884	Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, April 2007.
RFC4890	Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.
RFC4891	Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.
RFC4941	Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

RFC4944	Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.
RFC4945	Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", RFC 4945, August 2007.
RFC4966	Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.
RFC4982	Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, July 2007.
RFC4995	Jonsson, L-E., Pelletier, G., and K. Sandlund, "The RObust Header Compression (ROHC) Framework", RFC 4995, July 2007.
RFC4996	Pelletier, G., Sandlund, K., Jonsson, L-E., and M. West, "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)", RFC 4996, July 2007.
RFC5006	Jeong, J., Ed., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007.
RFC5014	Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.
RFC5072	Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.
RFC5095	Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.
RFC5114	Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.
RFC5120	Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, February 2008.
RFC5121	Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.
RFC5155	Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.
RFC5175	Haberman, B., Ed., and R. Hinden, "IPv6 Router Advertisement Flags Option", RFC 5175, March 2008.
RFC5225	Pelletier, G. and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite", RFC 5225, April 2008.
RFC5304	Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, October 2008.

RFC5305	Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.
RFC5308	Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, October 2008.
RFC5310	Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.
RFC5340	Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.
RFC5453	Krishnan, S., "Reserved IPv6 Interface Identifiers", RFC 5453, February 2009.
RFC5492	Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, February 2009.
RFC5555	Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.
RFC5701	Rekhter, Y., "IPv6 Address Specific BGP Extended Community Attribute", RFC 5701, November 2009.
RFC5722	Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.
RFC5790	Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, February 2010.
RFC5795	Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, March 2010.
RFC5798	Nadas, S., Ed., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, March 2010.
RFC5838	Lindem, A., Ed., Mirtorabi, S., Roy, A., Barnes, M., and R. Aggarwal, "Support of Address Families in OSPFv3", RFC 5838, April 2010.
RFC5908	Gayraud, R. and B. Lourdelet, "Network Time Protocol (NTP) Server Option for DHCPv6", RFC 5908, June 2010.
RFC5942	Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, July 2010.
RFC5969	Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.
RFC5996	Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.
RFC6040	Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, November 2010.
RFC6071	Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011.
RFC6106	Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

RFC6141	Camarillo, G., Ed., Holmberg, C., and Y. Gao, "Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP)", RFC 6141, March 2011.
RFC6144	Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.
RFC6164	Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", RFC 6164, April 2011.
RFC6204	Singh, H., Beebee, W., Donley, C., Stark, B., and O. Troan, Ed., "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011.
RFC6275	Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.
RFC6296	Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.
RFC6379	Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 6379, October 2011.
RFC6380	Burgin, K. and M. Peck, "Suite B Profile for Internet Protocol Security (IPsec)", RFC 6380, October 2011.
RFC6398	Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, October 2011.
RFC6434	Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.
RFC6437	Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, November 2011.
RFC6540	George, W., Donley, C., Liljenstolpe, C., and L. Howard, "IPv6 Support Required for All IP-Capable Nodes", BCP 177, RFC 6540, April 2012.
RFC6945	Gont, F. „Processing of IPv6 "Atomic" Fragments", RFC6946, May 2013.