

Article

A Comparison of Internet Protocol (IPv6) Security Guidelines

Steffen Hermann and Benjamin Fabian *

Institute of Information Systems, Humboldt-Universität zu Berlin, Spandauer Str. 1, 10178 Berlin, Germany; E-Mail: steffen_amerika@web.de

* Author to whom correspondence should be addressed; E-Mail: bfabian@wiwi.hu-berlin.de; Tel.: +49-30-2093-5662.

Received: 5 November 2013; in revised form: 10 December 2013 / Accepted: 12 December 2013 / Published: 10 January 2014

Abstract: The next generation of the Internet Protocol (IPv6) is currently about to be introduced in many organizations. However, its security features are still a very novel area of expertise for many practitioners. This study evaluates guidelines for secure deployment of IPv6, published by the U.S. NIST and the German federal agency BSI, for topicality, completeness and depth. The later two are scores defined in this paper and are based on the Requests for Comments relevant for IPv6 that were categorized, weighted and ranked for importance using an expert survey. Both guides turn out to be of practical value, but have a specific focus and are directed towards different audiences. Moreover, recommendations for possible improvements are presented. Our results could also support strategic management decisions on security priorities as well as for the choice of security guidelines for IPv6 roll-outs.

Keywords: Internet; IPv6; deployment; security

1. Introduction

1.1. Motivation

Concerns about the depletion of IPv4 address space have existed ever since it was noticed that a possible address shortage might occur. As a result, a new version of the Internet Protocol (Version 6, IPv6) was specified in 1995 [1]. As of today, however, only few Internet Service Providers (ISPs) or other IT organizations have moved to the new protocol, even though the pool of available IPv4 addresses at the

Internet Assigned Numbers Authority (IANA) was exhausted in 2011, which indicates that now is the time to gain knowledge, gather experience, and prepare for deployment of IPv6-ready infrastructures [2]. The main features of IPv6 are introduced in this paper and can be found in Section 2.

While the IPv6 standard has matured, in particular during the last decade, a lot of research has been invested into finding possible IPv6 security issues and solutions. Two official organizations from the U.S. (National Institute of Standards and Technology, NIST) and Germany (Bundesamt für Sicherheit in der Informationstechnik, BSI) have published guidelines for a secure IPv6 deployment. However, topicality of content and coverage of important IPv6 topics are crucial to make such guides useful for practitioners. As more organizations need to deploy IPv6 infrastructures, an evaluation of these guidelines is necessary in order to assess the quality of their advice and to make sure they provide the right information for a secure deployment, with up to date methods and techniques.

The current article aims to close this gap by providing a methodology for evaluating and comparing these two guidelines. This methodology can be adapted by individual organizations for prioritizing their individual knowledge needs and for selecting an appropriate guideline (or sections of it) accordingly. Moreover, we present the results of a small-sized global survey of IPv6 experts and their aggregated importance weightings of topic categories for a secure IPv6 deployment. Partly based on these weights, we conducted a first iteration of our methodology and present the results of our comparative evaluation of the guidelines.

1.2. Method Overview

In this article, at first a review of recent IPv6-related research papers and online resources is conducted. The Internet Engineering Task Force (IETF) regularly publishes Requests for Comments (RFCs) that cover most (if not all) IPv6 standards, related protocols, specifications, security issues, best practices as well as other information about IPv6, even including methods that are still in an experimental stage. RFCs related to IPv6 were filtered and categorized into five main categories, each with multiple subcategories. The complete list can be found in Appendix A. Based on these RFCs, the scores *completeness* and *depth* were derived. Content completeness is a score indicating the breadth of RFC coverage within the guides. Content depth is based on completeness and indicates to what extent the content of relevant RFCs is covered. A detailed explanation of these scores can be found in Section 3. Since not all topics are equally relevant for a secure deployment guide, they need to be weighted and ranked. For this purpose an expert survey was carried out. This procedure can be reused and generalized to a universal use case of a group of people introducing IPv6 into an organization.

Weights for categories were calculated using the method of Analytic Hierarchy Process (AHP) discussed in Section 3.3. Subcategories were rated for importance using a scale, and results were aggregated and ranked. The weights were applied to the completeness values of the guides. Finally, the list of relevant RFCs, completeness and depth, the weights, and importance ratings were used to evaluate the guides. Individual evaluations can be found in Sections 4 and 5; a guideline comparison in Section 6. Based on these results, recommendations for usage of the guidelines and possible improvements are discussed in Section 7. Limitations and future work is presented in Section 8.

1.3. Related Research

IPv6 has existed for almost two decades and a lot of technical research has been conducted in this area. However, in the area of managing and supporting the secure introduction of IPv6 into existing networks, literature is very scarce. Currently, we are not aware of a deep and systematic comparison of the important guidelines that support practitioners during this process. Concerning general literature, most relevant information on IPv6 can be found in the RFCs published by IETF, see the list in Appendix A, which is updating and extending an older list published by NIST [3]. Those RFCs also cover important research in the field of IPv6, including experimental methods and protocols. The RFCs were also used as a starting point of our work, extended to a large extent during the literature review. To the best of our knowledge, no evaluation of security guidelines for the deployment of IPv6 has been conducted before that was based on relevant RFCs published by the IETF.

Concerning other general literature, Silvia Hagen gives a comprehensive overview of the IPv6 in her books [4,5] as do older reference works such as [6,7]. High level introductions to IPv6 security are given by [8–12]. More detailed discussions on IPv6 security include [10,13,14], as well as books such as [15,16]. Another very detailed introduction to IPv6 security in German is [17]. Reference [18] gives a comparison of IPv4 with IPv6 security and threats. Reference [19] focuses on network auto configuration and related security issues. A survey of secure protocols for Mobile IPv6 is presented by [20]. Moving-target defense based on IPv6 is the topic of [21]. Reference [22] present the result of a survey (with 11 usable responses) on security issues during transition to IPv6 as well as some limited practical security tests on production networks. In comparison to this paper, the number of respondents in our paper is larger and the result more detailed.

With respect to security, our current paper does not aim at providing a concise survey of IPv6 security issues and details of recent exploits. Such a work would be an important complement to our article. Instead, we focus on the management aspects of secure IPv6 deployment and the question to what extent the relevant RFCs are reflected in the two most prominent guidelines for practitioners.

2. Introduction to IPv6

IPv6 is the successor of IPv4 and will replace it in the long run as the main protocol of the network layer. IPv6 is aimed at providing end-to-end communication between network interfaces even when the number of Internet participants and corresponding demand for address space keep on increasing massively, for example caused by the growing demand for Internet-enabled mobile devices. Security, Quality of Service (QoS), and reduced load for routers are further goals of IPv6 [5]. IPv6 is not downward compatible, therefore a simple switch of protocols is not possible. This is also due to various old network devices that are optimized for the use with IPv4 and hence do not support new version. The development of the next generation Internet protocol began in 1993 when people realized that the address space would not suffice forever. IPv6 was first published in 1995 in the RFC 1883 [1], which was deprecated in 1998 by RFC 2460 [23].

IPv6 quadruples the address length of IPv4 to 128 bit. This extension leads to an exponentially growth of the address-space size to $2^{128} \approx 340$ undecillion. This would in theory correspond to 6.65×10^{23} addresses per square meter of the earth. Such a tremendous amount of addresses makes it possible to

give a unique address to every device connected to the Internet for a practically indefinite amount of time and enables a true end-to-end communication among them. The effectively available address space is certainly smaller than theoretically possible, since large blocks are reserved for special purposes such as multicast, or for purposes yet unknown. The smallest allocation possible is furthermore a /64 prefix. This leaves 64 bit to be assigned to network devices. While this will also lead to a lot of waste of addresses, this decision was made to improve manageability and routability of networks [23].

Moreover, there are also further standards published around IPv6 that, for example, define interoperability with other protocols or compatibility with IPv4. Basically, IPv6 serves the same purpose as IPv4 does, namely the packet-oriented connection of host systems. The following are the main features introduced with IPv6: a simplified IP header structure, Extension Headers, Stateless Address Autoconfiguration (RFC 4862) [24], IP Security Extensions (IPsec), Mobile IPv6 (MIPv6), QoS, route aggregation, and Path Maximum Transmission Unit (PMTU) Discovery.

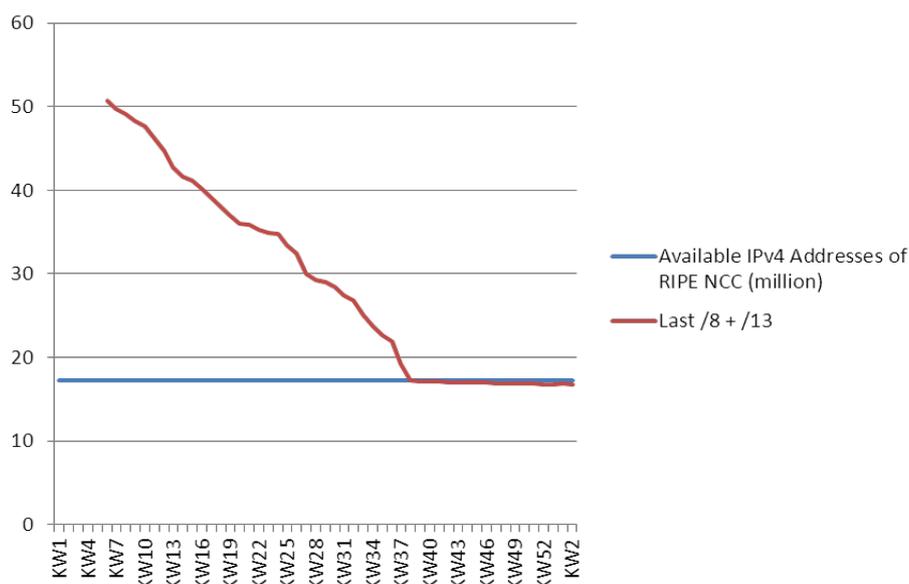
Although IPv6 has already been specified in 1995, IPv4 is still the most popular protocol in networks of all sizes including the Internet as has been shown by several studies. With CAIDA, kc claffy investigated the global IPv6 peering of AS's in 2010. Only 307 thousand paths to networks were sufficient to cover 99% of all routed prefixes for IPv6, while 170 million paths were used for IPv4, covering 96% of all routed IPv4 prefixes [25]. According to Dell Inc., there were only 44 ISPs worldwide who offered native IPv6 connectivity in 2010 [26].

Why does it take so long for IPv6 to replace IPv4? It is true that the IPv4 address space is very small and would have been exhausted for a long time if the principle of end-to-end connectivity had been upheld. However, techniques such as Network Address Translation (NAT) were developed that are virtually extending the address space, making it possible to use a single address for multiple sites by utilizing formerly unused transport layer ports [27]. Moreover, some of the features introduced with IPv6, such as IPsec [28] and QoS, were made available for IPv4 as well. Another problem is the unclear business case for IPv6 [29]. So far, there are only very few applications leveraging the features of IPv6, and there is barely any noticeable advantage for end customers. Hence, it is difficult for ISPs to sell IPv6 as a feature to customers and charge for it. Until now, most ISPs have postponed the migration of IPv6 to the point of time when it will be indispensable because IPv4 addresses will not be available anymore.

As Regional Internet Registries (RIRs) such as the Réseaux IP Européens Network Coordination Centre (RIPE NCC) hand out the last available addresses, new policies are applied for their allocation. In particular provider-independent PI addresses, which are needed for organizations that require multihoming or prefer their network to be independent from their ISP, are harder to acquire [30]. There are also some initiatives taking place that encourage testing and implementing IPv6. In 2011, the "IPv6 Day" aimed for an initial large-scale test of IPv6, followed by the "IPv6 Launch" one year later. In 2012, websites like Google, Facebook or Yahoo! did not only test IPv6, but made their websites permanently available via IPv6. More than 70% of the participants are still reachable via IPv6 as of October 2012 [31]. According to surveys among ISPs and other network related organizations conducted by the Number Resource Organization (NRO), more than 70% of the participants have some kind of IPv6 presence internally or on the Internet. Only 7% do not plan to deploy IPv6 yet. Most of the participants report only very low traffic via IPv6 so far [32]. This shows that most network companies already have some kind of IPv6 in use and are gaining experience in handling it.

Today almost all address blocks of the five RIRs are allocated. The RIPE NCC keeps statistics on the current available address space that is updated on a weekly basis. An excerpt from February 2012 to January 2013 is shown in Figure 1. The flat (blue) line represents the last/8 block of IPv4 addresses allocatable by RIPE NCC and a/13 block reserved for unforeseeable events. The red line shows the amount of IPv4 addresses left. As can be seen, the available amount of addresses shrunk very fast until it hit the last/8 block some time around the 38th week of 2012. Since then, new restricted allocation policies have come into force. The maximum allocatable address size from this last/8 block are/22 blocks. Applicants for these address blocks must already have been given an allocation of IPv6 address space. Furthermore, applicants have to prove the need for more IPv4 addresses [33]. As the graph shows, these policies slowed down the depletion to a great extent. Now, the amount of available IPv4 addresses declines very slowly. In the foreseeable future this pool will subside. While some IPv4 addresses will always be available, larger address blocks will only be allocated from the IPv6 pool. Large companies who received very large address blocks at the beginning of the Internet will have enough space to support their networks for a long time, but new companies who never had the chance to get an IPv4 allocation will have to use IPv6 to build up their network.

Figure 1. Depletion of Internet Protocol (IPv4) from February 2012 to January 2013.



In the following, we will give a brief overview on selected aspects of IPv6 that are important topics for the secure deployment guidelines.

2.1. ICMPv6

The Internet Control Message Protocol Version 6 (ICMPv6) is an important element of IPv6, and at least parts of ICMPv6 have to be used in every network based on IPv6. Similar to the ICMP of IPv4, it handles error messages and can help with network diagnoses through echo requests (ping) and other familiar features. The protocol itself is documented in RFC 4443 [34]. ICMPv6 is the foundation of

some new protocols specially designed for the use with IPv6. These protocols are: Neighbor Discovery, Path MTU, Autoconfiguration and Multicast Listener Discovery (MLD).

Neighbor Discovery (ND) is one of the most important new protocols based on ICMPv6 and serves many functions. It enables each node to find all other reachable nodes within its link and to learn their MAC and link addresses, which replaces the Address Resolution Protocol (ARP). Together with Stateless Address Autoconfiguration it enables devices to receive a network prefix and other configuration information from a router in order to automatically configure the IPv6 address; moreover, a Duplicate Address Detection (DAD) can be performed to ensure uniqueness within the link (or within the scope of the prefix if the link was given its own subnet). Other uses are to check which neighbors are still available and detect changes of link-layer addresses. ND is specified by the IETF in RFC 4861 [35].

As mentioned above, IPv6 does not only feature *stateful* autoconfiguration via DHCPv6 (Dynamic Host Configuration Protocol), but also *stateless* autoconfiguration using ICMPv6 messages and DAD, specified in RFC 4862 [24]. When an interface becomes enabled, it automatically defines its link-local address by combining the fixed link-local prefix *fe80::0* with a unique interface identifier, which could be an Extended Unique Identifier (EUI-64) address as in RFC 4291 [36]. If the router of the link announces a global unicast prefix, nodes can also configure a global unicast address which is routable on the Internet [24].

Path MTU (PMTU) describes the biggest possible packet size that can be sent via a particular path through a network. The smallest MTU of IPv6 is 1280 byte. This enables the link layer to perform an encapsulation without exceeding the 1500 byte limit of Ethernet. A recommendation is to implement PMTU discovery on every node. The reason for this is that with IPv6 only the source and destination are able to fragment and defragment the packet (exceptions apply if tunneling is used). Every time a packet reaches a node which cannot handle its size, the packet does not get fragmented further; instead an ICMPv6 message “Packet too big” is triggered and sent back to the source. By using PMTU discovery on every node, the PMTU can be established in advance and thus prevent unnecessary traffic. Fragmentation can furthermore be avoided to a large extent by only sending packets of the size of the PMTU if possible. A complete specification of the PMTU discovery can be found in RFC 1981 [37].

2.2. DNS

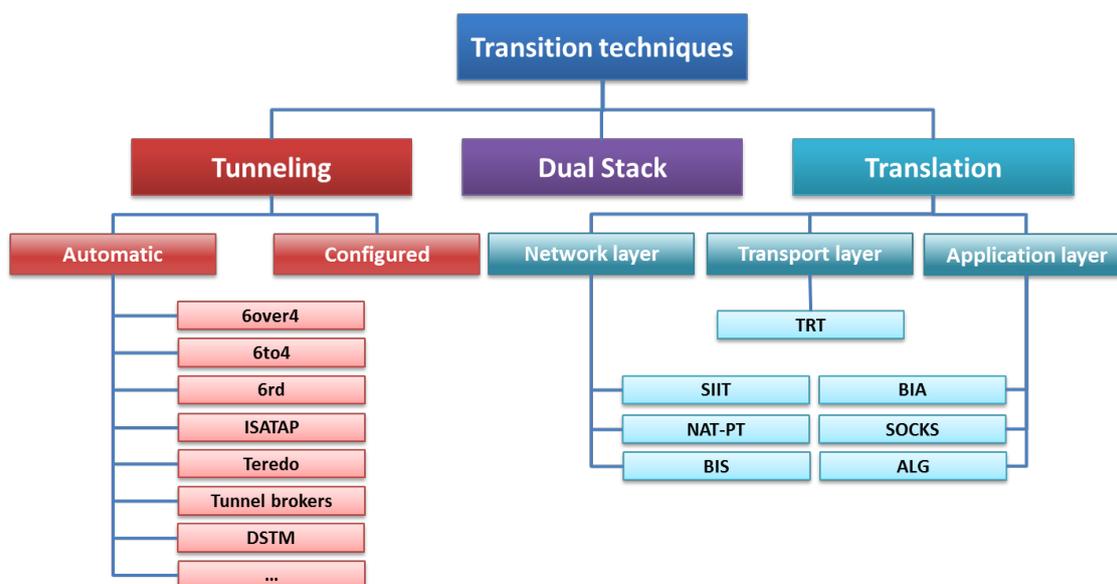
The Domain Name System (DNS) has not changed much for IPv6. In general, it works similar for IPv6 as it does for IPv4. It is possible to query for both IPv4 and IPv6 addresses disregarding the type of the network. The resource record for IPv6 is called AAAA record (Quad A). Each AAAA record can only store one IPv6 address so that some hosts could have multiple AAAA records. In an answer all of these addresses would have to be included. For reverse lookup, a new domain *ip6.arpa* was defined.

Some older applications might have problems handling 128 bit addresses when expecting a 32 bit address. Since multiple addresses could be returned, services must be able to handle this. Another issue could arise if fragmentation of the answer is needed, since fragmentation of IPv6 might not be allowed in some networks. Other security implications are basically the same as with IPv4. There are no new IPv6 specific protection mechanisms because Transaction Signatures TSIG [38] and DNS Security Extensions DNSSEC [39–43] are also applied in the context of IPv4 [3].

2.3. Transition Methods

Transition methods support gradually moving from IPv4 to IPv6 without major interruptions of services and networks. It is expected that most networks will have to support both IPv4 and IPv6 in parallel for a long time because of legacy equipment and the dependency on others to completely switch to the new protocol. Transition methods can be categorized into tunneling and translation methods. Figure 2 shows a hierarchical representation of the transition methods.

Figure 2. Transition methods.



2.3.1. Coexistence of IPv4 and IPv6

Dual stacking is probably the easiest way to establish a transition without too many outages. In some cases, however, this might not be possible. Incompatible hardware may be too expensive to replace, so some parts of the network have to stay with IPv4 (at least for a while). Furthermore, dual stacking adds complexity and increases administration workload. This situation leads to a need for further transition or translation mechanics.

6to4 and Teredo—described in Section 2.3.3.—are mechanics used for tunneling. IPv4-compatible addresses are deprecated because none of the specified transition methods use it anymore. The use of IPv4-mapped IPv6 addresses is discussed in RFC 4038 [44]. The address structure is $::FFFF/96 + \text{IPv4 address}$ (e.g., $::FFFF:123.45.67.89$). Basically, mapped addresses are used in dual stack networks that are still in transition where a IPv4 only node would like to access an IPv6-only application. However, the use of IPv4-mapped addresses is disabled by default in many systems because of security concerns.

Possibilities to translate IPv4 to IPv6 were enhanced in RFC 6052. The structure is shown in Figure 3. While formerly/96 prefixes were used like $::/96$ or $::FFFF/96$, the new standard allows network specific prefixes in various lengths. The length depends on the allocated network prefix. If a unique/96 prefix is used, the IPv4 address does not have to be globally unique. The resulting IPv6 address must be unique if it is supposed to be a global unicast address. If the network does not have its own network prefix, a special prefix can be used. This prefix is called Well-Known prefix and has the form $64:ff9b:/96$.

Figure 3. IPv4 embedded IPv6 address formats [45].

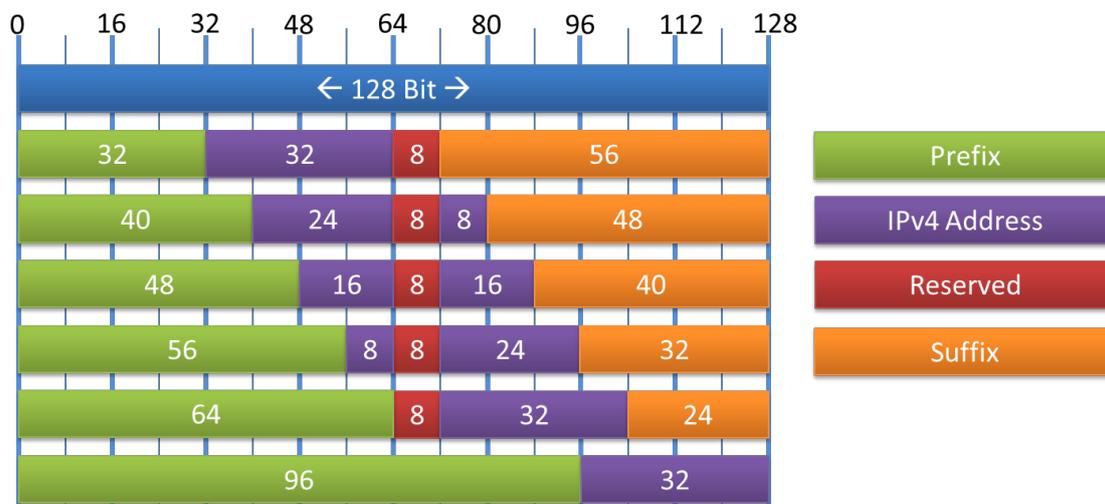


Figure 3 shows six specified possibilities to create an IPv4-embedded IPv6 address. Depending on the length of the prefix (green) the structure changes. If the prefix is 96 bit long, the IPv4 address (purple) is just added after the prefix to reach a length of 128 bit. If the prefix is shorter than 96 bit, the IPv4 address is interrupted by an octet of zeros (red). This octet is always placed at the positions 64 through 71. The rest of the address is reserved for a suffix (orange) which is not used yet and has to be set to all zeros. This suffix could be used in the future for additional functions, so IPv4-embedded IPv6 addresses might have to be changed. Many address blocks of the IPv6 address space are still to be assigned to a particular purpose. Overall this accounts for 86% of the available address space. This space is reserved for future developments, which is why IPv6 is—and will continue to be—very flexible for a long time.

2.3.2. Dual Stack

Dual IP layer or Dual Stack is defined in RFC 4213 ([46], p.1) as a “technique for providing complete support for both Internet protocols—IPv4 and IPv6—in hosts and routers.” At least in part, dual stacking will occur in any transition from IPv4 to IPv6. It is further expected that dual-stacked networks will exist for a long time also after IPv4 depletion. A complete dual stack is probably the best way to avoid security issues involved with IPv4-IPv6 interaction. On the other hand, it does increase administration workload by adding complexity and literally doubling the configuration overhead. Most other transition techniques of the categories tunneling and translation require some kind of dual stacking.

2.3.3. Tunnel

Tunnels for IPv6 were primarily developed to be able to cross IPv4-only sections of a network during transition. Several tunneling techniques have been specified in the last years. This section gives an overview of the currently most prominent tunneling techniques. Since tunnels add complexity and transparency to the network, they are considered temporary tools for IPv6 deployment. If possible, tunnels should be avoided and disabled as soon as they are not needed anymore [3,47]. Generally, there are two types of tunnels: Tunnels which have to be manually configured and automatic tunnels. From

a security point of view, automatic tunneling is questionable and should always be turned off if it is not used [47].

Configured tunnels have to be set up and managed manually by an administrator and are specified in RFC 4213 [46]. For tunneling IPv6 through an IPv4 network the protocol 41 is used and has to be enabled on the route. In case that IPv4 packets are tunneled through an IPv6 network, Generic Routing Encapsulation GRE or Multiprotocol Label Switching MPLS can be used. Configured tunnels do not scale as well as automatic tunnels because administrators have to set up and shut down tunnels manually every time when changes are necessary.

All the following tunnels are automatic tunnels. 6to4 is specified in RFC 3056 [48]. This technique is used for global reachability and tunneling through the IPv4 Internet. Since the publicly available prefix 2002::/16 is used, a globally unique IPv4 prefix is needed. Networks that want to connect to each other need to have access to the same IPv4 network and set up a 6to4 relay router at the border of both sites. 6to4 is in use in productive systems. The technique, however, has some security implications and should only be used if the ISP does not provide IPv6 prefixes. Among the security threats are source spoofing and Denial of Service (DoS) attacks.

6over4 is specified in RFC 2529 [49]. It depends on IPv4 multicast as virtual link layer and thus is intended for use within a site rather than for connecting an IPv6 node with the rest of the Internet. IPv4 multicast must be enabled in the entire network. IPv6 interfaces are assigned a unicast address with a valid 64 bit prefix and a 32 bit IPv4 address as suffix. Additionally, they are assigned a link-local address. So far, this method is not widely used. 6rd (IPv6 rapid deployment) is similar to 6to4 but does not use the publicly available prefix. It requires a globally routable IPv6 prefix. This technique is specified in RFC 5969 [50]. It is primarily meant for use by ISPs as a fast deployment of IPv6 to their customers. The IPv6 address is constructed by the network prefix in concatenation with a prefix-reduced customer IPv4 address. The calculation of the prefix is automated and conform with automatic reset of IPv4 addresses because it recalculates the prefix every time.

Teredo was developed by Microsoft and later approved by the IETF in RFC 4380 [51]. It is meant to solve the problem of tunneling IPv6 through NATs or multiple layers of NATs by using the User Datagram Protocol (UDP) instead of IP protocol 41. It can be used as “technology of last resort” [3] for deployment of IPv6 hosts behind NAT. Teredo provides automatic tunneling and uses addresses of the following type: 2001:0000::/32 + Teredo Server IPv4 address (globally unique) + Flags + Port + Client IPv4 address. However, Teredo has many security issues. It requires UDP port 3544 to be open, and rogue Teredo servers could be used for man-in-the-middle attacks. DoS and distributed DoS could also be issues [51].

Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is used for connecting isolated IPv6 hosts within a site network. ISATAP is specified in RFC 5214 [52]. This technique is meant for an early stage IPv6 transition, when small IPv6 islands exist. It is supported by almost all operating systems which feature IPv6. Hosts using ISATAP must be dual stacked while the connecting network can be entirely IPv4, with each ISATAP host connected to at least one ISATAP router. The use of ISATAP is recommended to be stopped as soon as IPv6 connectivity is established in the network. Operating systems, which have automatic tunneling enabled by default, should be configured to have it turned off if ISATAP is not needed.

Tunnel brokers deploy dual stack tunnel servers with access to the Internet. Clients can connect to tunnel brokers that establish a tunnel in return. The tunnel broker is responsible for the complete management including DNS, authentication, and access control. The main use of tunnel brokers is for experimental reasons or single individuals not having native support by their ISP yet. Configurations vary depending on the tunnel broker. Information about tunnel brokers can be found in RFC 3053 [53]. There are two more “tunnel techniques” still in development. One is Dual Stack Transition Mechanism (DSTM) that is a transition mechanic using 6over4 for IPv6 dominant networks [54]. The second is the Bi-Directional Mapping System (BDMS) which tries to avoid tunneling but focuses on translation mechanisms [55]. Both have not made it to a standard track by now and are considered experimental.

2.3.4. Translation

Translation mechanisms try to translate IPv6 packets into IPv4 packets and vice versa. This can be done on different layers as shown in Figure 2. Translation techniques are discouraged as transition approach because they can impede hierarchical routing and do not take advantage of the new header and extended address space [3]. The most important techniques are explained in the following.

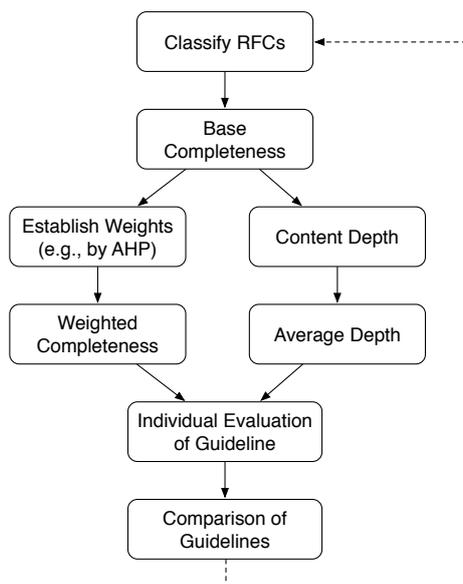
Stateless IP/ICMP Translation (SIIT) is used on the network layer and defined in RFC 6145 [56]. It makes use of IPv4-converted and IPv4-translatable addresses, which are a subset of IPv4-embedded addresses explained in Section 2.3.1. While still called stateless, this technique offers a stateless and a stateful mode, compliant with the rules defined in RFC 6052 [45]. SIIT can handle ICMP as well as IP packets in both directions. For ICMP only the vital messages such as echo are translated, most others are dropped. Generally, only information that is 1:1 translatable is in fact translated. Other information, such as option fields, are ignored or can cause the packets to be silently dropped. While not introducing new security issues, SIIT is not able—and not supposed—to translate all traffic. Network Address Translation-Protocol Translation (NAT-PT) is the combination of SIIT (old specification) and IPv4 NAT. It is specified in RFC 2766 [57] and is still valid but moved to historic status by RFC 4966 [58]. NAT-PT should not be used because it is vulnerable for DOS attacks, does not support DNSSEC, and IPsec cannot be translated. Furthermore, it hinders the complete deployment of IPv6 and IPv6 applications. NAT-PT is replaced by SIIT as in RFC 6145.

Transport Relay Translation (TRT) aims to solve the translation problem on the transport layer and defines a method for Transmission Control Protocol (TCP) and UDP traffic. TRT is a stateful translation technique and uses DNS mapping between AAAA and A records and is defined in RFC 3142 [59]. It is vulnerable to DoS attacks and does not support IPsec. ALT techniques were developed to handle legacy applications that use IPv4 but cannot be upgraded to IPv6 or be replaced. Most of them present an artificial pool of IPv4 addresses to the application and then translate requests [3].

3. Methodology and Criteria for a Comparative Evaluation of the Guidelines

The current section presents the methodology and evaluation criteria for the comparative evaluation of the guidelines for secure IPv6 deployment. Figure 4 shows the most important steps of our methodology, which are described in more detail in the following.

Figure 4. Base methodology.



3.1. Content Completeness

The score for content *completeness* describes to what extent IPv6-relevant topics are covered in the guides. This score is based on the set of RFCs relevant for IPv6 published by the IETF. As almost all changes and new developments regarding IPv6 are documented within the RFCs, they are a good basis for the score. There might be other topics and information not yet published as RFC, but during the review it was found that RFCs are very comprehensive. A list of RFCs relevant for IPv6 was compiled for this article and can be found in Appendix A.

The base completeness score for a guideline with respect to a single RFC has two values: 0 and 1. A value of 0 indicates that the RFC is not covered at all. It is neither mentioned nor is its content covered in any way. A value of 1 means the RFC is at least referenced in some way. The level of detail does not matter for completeness. In order to calculate completeness of content subcategories, the base completeness values for the RFCs associated with it are summed up and divided by the number of relevant RFCs of the subcategory. The result is a relative value between 0 and 1. The closer the value is to 1, the more relevant RFCs have been covered. A value of 1 means 100% of possible RFCs were covered. The same is done for the main categories and, finally, the complete guide.

For *weighted completeness*, a ranking of main categories according to their priority for practitioners was conducted. The normalized weights were derived by interviews and the AHP method (Section 3.3.1.) and are multiplied with the respective category scores and the results are added up. Again, the highest achievable value is 1, indicating that all RFCs are covered. In this case the weights have no impact. The weights only matter if the completeness without weights is less than 1.

3.2. Content Depth

Content *depth* is a second score that is based on completeness. Content depth describes how detailed RFCs are covered and explained in a guideline. Depth is divided into six categories. Each category corresponds to a numerical value between 0 and 1, assigned as shown in Figure 5.

Figure 5. Content depth—Categories and values.

Missing	0
Very low	0.2
Low	0.4
Medium	0.6
High	0.8
Very high	1

RFCs are also called items in the following. An item is considered *missing* if it is not covered at all by the guide. It is neither named, nor is any other information regarding the item given. Missing items also decrease the completeness and might, but not have to, be recommended to be included in a future version of the guides. The next category, *very low*, is not assigned to any RFC in the current evaluation. It does exist for depth values that are aggregated for subcategories and categories. The numerical value is 0.2 for this category. An item is categorized *low* for depth if it is only named or referenced in an appropriate context. A very short description may also exist. The numerical value is 0.4.

An item falls into the *medium* category if it fulfills the criteria for *low*. Additionally, the item is described in detail and an example is given if appropriate. The numerical value of this category is 0.6. *High* depth is assigned to items that satisfy the requirements for *medium* and, in addition, provide an example solution for the item, which is useful in practice. The numerical value is 0.8. Every item which fulfills the requirements for *high* and exceeds these is categorized as *very high* regarding its depth. The numerical value is 1.

Depth scores for subcategories, categories, and the complete guide are aggregated by adding up the numerical values and dividing them by the respective number of relevant RFCs. They can be very low if many of the underlying RFCs are missing. Thus, a value of 0.4 for a category can mean different things: It could be that there are many missing RFCs, but some were covered with very high content depth. It might also be that all RFCs were covered with a depth of low. Both cases could lead to the same result.

In order to get a better insight while comparing the guidelines, it is also necessary to look at completeness and depth in combination by adding up the depth values for the RFCs of a category, and then dividing by the count of only the covered (not of all the relevant) RFCs. The result of this calculation gives the *average depth* of covered RFCs, which is later used for a better comparison of the two guides because they differ substantially in completeness.

3.3. Survey Evaluation

Not all RFCs are equally important for a secure deployment. This causes the need for an objective consensus method of weighting the RFCs, either globally aggregated or specifically tailored to any given

organization. In order to exemplify such a weighting process, we adopted the AHP method in order to conduct a first attempt of a global weighting. For this, a survey was created and published in expert forums and expert groups in social networks (see Appendix B).

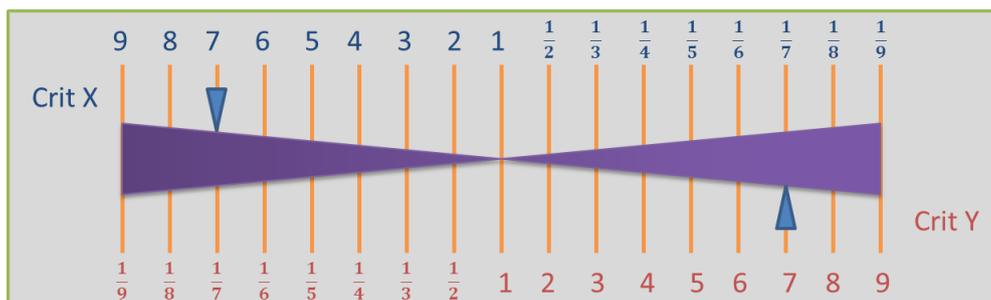
3.3.1. AHP and Weight Calculation

Analytic Hierarchy Process (AHP) is a method for systematic decision support between alternatives [60]. It turns abstract priorities of a decision maker into quantitative weights and thus helps to make objective decisions. One of the advantages of the process is that it can be used by a single decision maker but is also suitable for group decisions as well. A disadvantage is that criteria and possible features should be well known. Furthermore, priorities can still be biased and subjective. Nevertheless, the quality of a decision is tremendously increasing compared to a free decision without any supporting process. The decision making process is composed of the following steps, as described by [60]:

1. Define the problem and determine the kind of knowledge sought.
2. Structure the decision hierarchy from the top with the goal of the decision, then the objectives from a broad perspective, through the intermediate levels (criteria on which subsequent elements depend) to the lowest level (which usually is a set of the alternatives).
3. Construct a set of pairwise comparison matrices. Each element in an upper level is compared with the elements in the level immediately below it.
4. Use the priorities obtained from the comparisons to weight the priorities in the level immediately below. Do this for every element. Then for each element in the level below add its weighted values and obtain its overall or global priority. Continue this process of weighing and adding until the final priorities of the alternatives in the bottom level are obtained.

The pairwise comparison is based on a two sided scale. Each criterion is compared to every other criterion. Two criteria are compared by putting them on the opposite sites of the scale. The original scale features nine levels of intensity of importance. The center of the scale represents level 1 that represents equal importance for both criteria. The other eight levels extend to both sides towards the two criteria. Figure 6 shows a graphical example of such scale for better understanding. If a criterion x is assigned with one of the nine values when compared to criterion y, then y receives the reciprocal value when compared to x [60].

Figure 6. Graphical example scale for category comparison.



The results are entered into a matrix. If only one decision maker is performing the process, it is suitable to directly fill in the matrix without using a graphical scale. If the answers are collected using a survey, a graphical scale is more appropriate because participants do not need to understand the complete process and a matrix might be too demanding. From this matrix the weights (priorities) for criteria (alternatives) can be derived. This is conducted by normalizing the matrix, adding up each row and dividing them by their totals. This method has been proven to be close to actual statistical results [60]. In order to fill in the matrix, answers of the participants are aggregated by averaging. Since only half of the matrix can be filled directly via the answers, the corresponding fields are completed with the reciprocal values. Table 1 is established through this process. Table 2 shows the matching of short names used in the tables for the criteria. Criteria are from here on also called categories or main categories.

Table 1. Aggregated (average) comparison matrix (n = 34).

	C1	C2	C3	C4	C5
C1	1	1.55	0.77	0.95	1.11
C2	0.65	1	1.27	1.21	1.51
C3	1.30	0.79	1	1.55	1.60
C4	1.05	0.83	0.64	1	1.77
C5	0.90	0.66	0.62	0.57	1

Table 2. Categories.

Category Name	Short Name
DHCPv6 and Autoconfiguration	C1
IPv6 Specification and Address format	C2
Routing and DNS	C3
Transition Methods	C4
IPsec and ICMPv6	C5

For simplicity the scale is reduced to five intensity levels. In general the scale is kept as suggested by Saaty. Only a small number of categories are chosen to keep the number of necessary comparisons as small as possible, since the number of comparisons grows exponentially with the number of categories. There are also subcategories for each category. AHP was not used on the subcategories. The process for the subcategories is explained in Section 3.3.2. The categories and subcategories are based on the IPv6 topics which are covered by the RFCs of IETF and are possible content for a secure deployment guide.

After the comparison matrix is filled with average ratings, the matrix is normalized by dividing each field with the sum of the respective row resulting in Table 3.

Now for each row the weights can be calculated. Table 4 shows the weights for the main categories calculated using the AHP method.

Table 3. Normalized comparison rating matrix (n = 34).

	C1	C2	C3	C4	C5
C1	0.20	0.32	0.18	0.18	0.16
C2	0.13	0.21	0.29	0.23	0.22
C3	0.26	0.16	0.23	0.29	0.23
C4	0.21	0.17	0.15	0.19	0.25
C5	0.18	0.14	0.14	0.11	0.14

Table 4. Category weights (n = 34).

Category	Weight
DHCPv6 and Autoconfiguration	0.21
IPv6 Specification and Address format	0.22
Routing and DNS	0.24
Transition Methods	0.20
IPsec and ICMPv6	0.14

As the results show, most of the weights are very close. Only *IPsec* received a low weight of 14%. *Routing and DNS* is viewed as most important with 24%. The *IPv6 Specification and Address format* is ranked second with 22%, closely followed by *DHCP and Autoconfiguration* (21%) and *Transition Methods* (20%). *IPsec* might be rated lower than the other categories because it is implicitly contained in IPv6 and is activated by default when implementing IPv6. Another reason might be that *IPsec* is already used with IPv4 and most cryptographic methods are already known from the IPv4 world. *ICMPv6* does not seem to be as important as other categories, even though the numbering of the messages has changed and new mechanisms such as ND and PMTU have been introduced.

Routing and DNS are also known from IPv4, but are more difficult due to the increased length of the addresses. Routing tables are feared to dramatically increase, and it is important to know how to use the routing protocols with the new Internet protocol version. DNS works very similar with IPv6 as with IPv4, but needs to be handled carefully. In particular, reverse DNS can easily lead to faults due to human failure when entering reverse addresses manually.

IPv6 Specification and Address format are also important for a secure deployment of IPv6. Since IPv6 addresses are longer and represented in a very different way than with IPv4, practitioners need to become comfortable with the new addresses. The new scope concept for addresses is also an important feature. IPv6 also specifies a new streamlined header and extension header concept, which makes IPv6 more flexible but also more complex. For this reason, probably, this category has been rated this high. *DHCPv6 and Autoconfiguration* and *Transition Methods* are also important to be aware of as the results show.

3.3.2. Importance Ratings for Subcategories

The second part of the survey was aimed to establish ratings for the subcategories. Pairwise comparisons were not reasonable for all categories, since this would have tremendously increased the

survey time. Thus participants were asked to rate the importance of the subcategories for a secure deployment guide of IPv6 using a scale from 1 to 10 where 10 represents the highest value, while 1 is the lowest rating. Averages were calculated from the results, and the outcomes were ranked for each category as well as overall (see Table 5).

Table 5. Rating results for subcategories (n = 27).

IPv6 Specification and Address Format			
IPv6 Main Header Format	6.03	3	13
Extension Header Format	6.07	2	12
Address Format & Textual Representation	5.72	5	20
Address Types and Scopes	6.69	1	2
Mobile IPv6	5.76	4	19
IPsec and ICMPv6			
Cryptographic Mechanisms	5.69	4	21
IKEv2	5.66	5	23
Path Maximum Transmission Unit(PMTU)	6.0	3	17
Neighbor Discovery	6.59	1	5
ICMPv6 Specification and Header Format	6.03	2	13
DHCPv6 and Autoconfiguration			
DHCPv6	6.66	1	3
Stateless Autoconfiguration	6.28	2	10
Routing and DNS			
DNSSEC	5.69	4	21
DNS Security Issues	6.62	1	4
DNS for IPv6 Specification	6.03	2	13
Routing Protocols (BGP, RIPng, OSPv3)	6.03	2	13
Protocol Independent Multicast(PIM)	4.62	6	25
Multihoming	5.0	5	24
Transition Methods			
Tunneling Methods	6.38	2	8
Translation Methods	6.21	3	11
Dual Stacking	7.38	1	1
IDS/IPS/Firewalling			
DPI	6.0	4	17
EH Support	6.48	2	7
ICMPv6 Handling	6.56	1	6
Ingress/Egress Filtering	6.33	3	9

In the category *IPv6 Specification and Address Format* all subcategories are rated above five on average. Most important is the category *Address Types and Scopes*, followed by *Extension Header Format* and *IPv6 Main Header Format*. *Address Format & Textual Representation* and *Mobile IPv6* are of minor importance in this category but also overall. *Address Types and Scopes* even came in second in the overall ranking and thus is the second most important subcategory of IPv6.

The subcategories of *IPsec and ICMPv6* were also all rated above five. ND is most important in this category, followed by the *ICMPv6 Specification and Header Format* and PMTU. *Cryptographic Mechanisms*, and as one of these *IKEv2*, are least important in this category and also overall. ND became fifth in the overall ranking and thus has high, but not a leading importance overall.

DHCPv6 and Autoconfiguration is a category with only two subcategories. One is the *DHCPv6 Specification*, which ranked above the second *Stateless Autoconfiguration*. Both got into the top ten in the overall ranking and thus are important IPv6 topics, with the *DHCPv6 specification* even coming in third place.

DNS Security Issues is the most important subcategory in the category *Routing and DNS* and became fourth in the overall ranking. Within this category, *Routing Protocols* and *DNS for IPv6 Specification* became second, followed by *DNSSEC*. *PIM* and *Multihoming* are of minor importance within the category as well as overall.

All three subcategories of *Transition Methods* got rated above six, and *Dual Stacking* was even rated above seven and thus received not only the first rank within the category but also overall. *Dual stacking* will be necessary for a long time as IPv4 and IPv6 have to be used in parallel due to compatibility. *Tunneling methods* got in second within the category and eighth overall. These, together with *Translation methods* that became eleventh overall, are important mechanics for connecting isles of IPv6 (or in future of IPv4) with the rest of the net when dual stacking is not possible. The last category is *IDS/IPS/Firewalling*. This category was not included in the comparisons because it is not a primary IPv6 topic, and relevant content is spread over many RFCs and is, thus, covered within the other categories. IPv6 poses only minor changes to this category and is only a small part, as this theme extends over all layers of the network, from physical layer to application layer.

As the results show, there are three very important topics, which all got into the the top ten of the overall ranking. These are *ICMPv6 Handling* at the sixth rank, *EH Support* at the seventh and *Ingress/Egress Filtering* at the ninth position. *Deep Packet Inspection* is more related to the application layer and thus got rated lower, but still received six points. *EH Support* means the ability of the security devices to handle extension headers of IPv6 and detect any corresponding malicious use. *ICMPv6 Handling* is the ability to handle ICMPv6 messages as described in RFC 4890 [61], while *Ingress-/Egress Filtering* includes the rules for outgoing and incoming traffic using IPv6 addresses.

All of these ratings and weights are utilized in the comparative evaluation of the secure deployment guides.

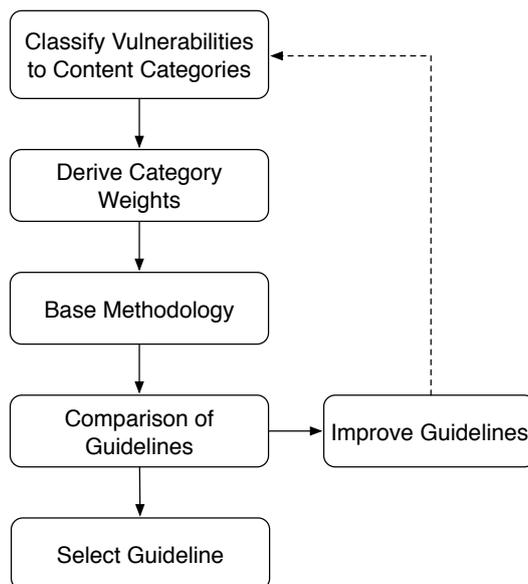
3.4. Extended Methodology Covering IPv6 Vulnerabilities

In a future evolution of our approach, current and newly discovered IPv6 vulnerabilities can be considered in the evaluation (and improvement) process of the guidelines. One possible extended methodology would work as follows (see Figure 7).

Discovered IPv6 vulnerabilities are classified according to the same categorization process as the RFCs in the base methodology. A possible starting point would be one or multiple information portals on vulnerabilities, such as the *Common Vulnerabilities and Exposures* (CVE) site [62]. Another source could be news on attacks on cryptographic protocols or infrastructures such as those apparently

conducted by the *National Security Agency* (NSA) or national agencies of other countries. Many new vulnerabilities, however, are specific to a particular vendor or operating system; these can be ignored in the methodology if the organization at hand is not using corresponding systems. The remaining vulnerabilities can be used as an evaluation criterion for weighting the categories of the IPv6 security guidelines during another execution of the base methodology, resulting in a weighted comparison of the guidelines and criteria for selecting one of them.

Figure 7. Extended methodology.



If the goal of running an instance of the extended methodology is to improve the guidelines themselves, vulnerabilities that could affect multiple implementations of a protocol of the IPv6 suite should be considered. Moreover, a statistical analysis of the frequency of the vulnerabilities discovered so far could lead to an appropriate weighting of categories for the guideline improvement process.

4. NIST Guidelines for the Secure Deployment of IPv6

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. Its mission is to promote U.S. innovation and industrial competitiveness by advancing measurement methods, standards, and technology in ways that enhance economic security and improve quality of life. NIST has laboratories for many different areas of science but mostly physical science as chemistry, physics, biology, and others. Among them is the Information Technology Laboratory and one of its divisions, the Computer Security Division [63]. It provides standards and technology to protect information systems against threats to confidentiality, integrity, and availability of information and services. Thus, the division publishes their own standards and works together with other standardization organizations such as the IETF. Beside standards, NIST and the Computer Security Division also publish security guidelines for different areas, e.g., cryptographic algorithms, and also provide evaluations and best practices for the use of standards [64].

In 2010 NIST published the “Guidelines for the Secure Deployment of IPv6” [3]. The document is meant to give a comprehensive overview about IPv6 and point out possible threats regarding the different

areas and technologies that are influenced by IPv6. Special focus is given to the security risks that might appear during deployment and transition to IPv6, since this is a critical evolution step for any network. It also provides a suggestion for a deployment strategy with a rough outline of recommended steps for the transition. The full document is 212 pages long and available for free download [3]. It does not require the reader to know IPv6, but knowledge about IPv4 and other networking protocols is necessary to a certain extent.

The NIST guide is structured in the following way. After a short introduction, the second chapter introduces IPv6, its history, major features, and a comprehensive comparison of threats for IPv4 and IPv6. The third chapter is focused on general IPv6 concepts. These include IPv6 addresses, addressing and allocation as well as the IPv6 header, extension header, ICMPv6, and DNS. The fourth chapter covers advanced IPv6 features in more detail. These include multicast, QoS, Multihoming, DHCPv6, and Mobile IPv6. The fifth chapter continues with security mechanisms such as privacy addresses, cryptographically generated addresses, IPsec in IPv6, and secure stateless address autoconfiguration. The final chapter focuses on the deployment of IPv6 and describes transition mechanisms, secure addressing schemes, and recommends steps and actions for the preparation of a deployment.

4.1. Content Completeness and Depth of the NIST Guide

For the evaluation of content completeness and depth, the NIST guide was checked for coverage of the RFCs listed in Appendix A. The main categories remain the same as in the survey. Additionally, the weights derived by AHP using the results from the survey from Section 3.3.1. of the Appendix were applied to derive the weighted completeness that for each main category multiplies its result by its weight and then adds them all up. For weighted completeness only the end result of the guide counts while (basic) completeness is shown for every subcategory, category and the whole guide.

Depth is calculated as explained in Section 3.1. This depth score is aggregated for every subcategory, category, and for the overall guide. The following list shows the legend for Table 6 and explains the columns: A = Count of covered RFCs, B = Count of relevant RFCs, C = Completeness, D = Weight (gray rows)/Importance Rating (white rows), E = Weighted Completeness (A*D), F = Depth. Category rows are shaded gray and show their subcategories below them (white rows). Values for subcategories are aggregated to the main categories. Totals are shown in the last line of the table.

Overall: As the totals of the last line of the table show, the NIST guide covers 174 of the 213 RFCs selected for evaluation. This results in a completeness of 0.82 or 82%. This result does not change much when applying the weights. The weighted completeness is 0.81 or 81%, which is only 0.01 less than completeness without weights. Thus, overall the NIST guide covers many of the existing RFCs regarding IPv6 and seems to be closely aligned to the preferences derived by the opinion of the survey participants. The overall depth is only 0.43 which translates to a little above *low* when translating it into a depth category.

Table 6. NIST Content Completeness and Depth. Columns: A = Count of covered RFCs; B = Count of relevant RFCs; C = Completeness; D = Weight/Importance Rating; E = Weighted Completeness (A * D); F = Depth.

Category	A	B	C	D	E	F
Specification & Address Format	50	57	0.88	0.22	0.19	0.52
Specification	4	4	1.00	6.17		0.75
Address Features	18	19	0.95	6.69		0.64
Header	9	13	0.69	6.05		0.34
Mobile IPv6	19	21	0.90	5.76		0.49
IPsec & ICMPv6	59	69	0.86	0.14	0.12	0.40
ICMPv6 Specification	5	6	0.83	6.03		0.67
Neighbor Discovery	7	11	0.64	6.59		0.36
Path MTU Discovery	1	1	1.00	6.00		0.60
Multicast Listener Discovery	4	5	0.80			0.32
IPsec	10	13	0.77	6.93		0.37
IKEv2	13	13	1.00	5.66		0.40
Cryptographic Methods	19	20	0.95	5.69		0.38
DHCPv6, Autoconfiguration	12	14	0.86	0.21	0.18	0.40
Stateless Autoconfiguration	2	2	1.00	6.66		0.70
DHCPv6	10	12	0.83	6.28		0.35
Routing & DNS	29	40	0.73	0.24	0.17	0.37
DNS Specification	1	3	0.33	6.03		0.33
Security Issues	8	9	0.89	6.62		0.49
DNSSEC	5	9	0.56	5.69		0.27
Multihoming	6	7	0.86	5.00		0.43
Routing Protocols	4	5	0.80	6.03		0.36
PIM	5	7	0.71	4.62		0.29
Transition Methods	24	33	0.73	0.20	0.15	0.41
Dual Stack	4	4	1.00	7.38		0.60
Tunneling	12	16	0.75	6.38		0.45
Translation	8	13	0.62	6.21		0.29
Totals	174	213	0.82		0.81	0.43

Specification and Address Format: The category *Specification and Address format* has 57 relevant RFCs, of which 50 are covered in the guide by NIST. This leads to a completeness of 0.88 and thus almost 90%. The missing points come from subcategory *Header* (4), *Mobile IPv6* (2) and *Address format* (1). The completeness of this category is very high and shows that the guide at least mentions many of the relevant RFCs. The depth is at 0.52 which translates to between low and medium with a tendency to medium. When looking into the subcategories, this value results from a low depth of the subcategories *Header* (0.34) and *Mobile IPv6* (0.49) while the other two subcategories achieved higher depth values. From the point of view of the importance ratings, *Header* and *Mobile IPv6* also got lower scores, therefore a less deep coverage must not be automatically considered as negative. In general,

the category *Specification and Address format* is well covered, which also aligns with the importance of its subcategories.

IPsec and ICMPv6: IPsec and ICMPv6 are also well covered by the NIST guide. 59 out of 69 relevant RFCs are mentioned, which results in a completeness of 0.86 or 86%. Except for the subcategories *Path MTU Discovery* and *IKEv2*, all other of the seven subcategories miss some points. The lowest scores pertain to *Neighbor Discovery* (4 missing) and *IPsec* (3 missing). Again, 0.86 is a very good result and shows that very many of the relevant RFCs are at least mentioned. The depth of this category is at 0.4 (low). Many of the subcategories have a very low depth. Only *Path MTU Discovery* and *ICMPv6 Specification* achieved a depth of 0.6 or higher. Other subcategories should have been covered in more detail as they received high importance ratings in the survey. These are in particular *Neighbor Discovery* and *IPsec*. *Neighbor Discovery* has an importance rating of 6.59 but only has a depth of 0.36 and thus is not described sufficiently. *IPsec* is rated even higher for importance (6.93) and also achieves only a depth of 0.37 (less than low). As one of the most important topics, this clearly shows a deficit and should be considered for improvement. The other subcategory scores for depth are well aligned to the importance rating they achieved. In general, this category is covered to a large extent in the NIST guide, but focus for detailed coverage should be shifted to the more important topics.

DHCP and Autoconfiguration: This smaller category with only 14 relevant RFCs is covered well by the NIST guide. 12 out of 14 RFCs are at least mentioned in the guide. The two missing points are coming from the subcategory *DHCPv6*. The resulting completeness is 0.86 or 86% and thus a good result. Depth of this category is only 0.4. This results from a very low depth of the subcategory *DHCPv6* (0.35) and a high depth of *Stateless Autoconfiguration* (0.70). The depth of *DHCPv6* is too low in relation to its importance rating of 6.28 and should be given more attention. Generally, the coverage of this category is good with room for a few improvements in depth.

Routing and DNS: With a coverage of 29 of 40 possible relevant RFCs and a completeness of 0.73 (73%) *Routing and DNS* is one of the less covered categories. Nevertheless, 73% is a good result, but could be better considering the highest weight of all five categories. None of the subcategories is completely covered, with *DNSSEC* missing 4 RFCs and, thus, the most of all. Depth of the category is 0.37. This indicates that the highest weighted category is not described well. Going into detail, this results from an overall low depth within the category. None of the subcategories achieved a depth above 0.5. Especially *Security Issues*, *Routing Protocols* and *DNS Specification* should be described in a more extensive way, as they received relative high importance ratings. The other subcategories were not rated very high for importance and thus do not necessarily need to be covered more. In general, this category should be covered more to increase depth and completeness for a better alignment to its importance.

Transition Methods: 24 out of 33 relevant RFCs are covered in this category in the NIST guide. Thus the completeness is 0.73 or 73%. Regarding the weighting of the category, this is a good result. Points are missing in the subcategories *Tunneling* (4) and *Translation* (5) while *Dual Stack* is completely

covered. The depth of Transition Methods is at 0.41 translating into a little above low. Looking at the subcategories, the depth of *Translation* is too low relative to its importance rating of 6.21. The same holds for *Tunneling*: even though its depth is 0.45 it could be higher. This is partially due to newer versions of RFCs, which are not yet included in the guide. Last but not least, *Dual Stack* achieves a depth of 0.6. This relative high value could also be higher since this topic is rated highest for importance and thus should receive detailed coverage. Generally, this category should be covered in more detail respecting its importance rating.

The NIST guide features a high coverage of the relevant RFCs and thus received a high completeness. The depth of coverage is aligned to the importance in many, but not all cases. There are some outdated RFCs that should be replaced by their newer versions and corresponding content should be checked for correctness.

4.2. Topicality of the NIST Guide

The secure deployment guide by NIST was published in 2010. Most but not all of the presented information is up to date. Generally RFCs with the numbers 6000 and up are not covered in the guide as most of these were published after the NIST guide. Five of the covered RFCs have newer versions: RFC 3177 is replaced by RFC 6177, RFC 3484 by RFC 6724, RFC 3697 by RFC 6437, RFC 3775 by RFC 6275, and RFC 4869 by RFC 6379.

When completeness and depth were evaluated, the content and the extent of the changes in the RFCs were taken into consideration. Thus some of the relevant topics are regarded as covered if the content of the guide is still valid and when changes only had a minor impact. Some covered topics are outdated. The NIST guide presents some methods and techniques that are already moved to historic or obsolete or whose use is discouraged by the IETF, for example, NAT-PT. The NIST guide includes recommendations for the notation of IPv6 addresses to reduce human failure and increase readability while keeping unambiguity; however, these are not fully correct anymore. Last but not least, the NIST guide still mentions IPsec as mandatory part of IPv6. While this holds true for some sub-protocols, the IPv6 specification now only recommends the use of IPsec as the wording was changed from *MUST* to *SHOULD* use.

5. BSI Secure Networking Guide

The BSI, founded in 1991, is a German federal office responsible for solving security issues and giving recommendations on the secure use of information technology. One of their biggest assets is the “IT-Grundschutz-Katalog” (basic IT protection catalog). The catalog is about 4000 pages long and provides recommendations for enterprises to keep their IT secure. Moreover, it is possible for companies to achieve a “BSI Grundschutz” certificate if an enterprise implements the necessary controls and measures. The catalog is divided into three main sections. The first, “Bausteine” (building blocks), describes all elements of IT which might exist within an enterprise. The second, “Gefährdungskataloge” (risks catalogs), contains a list of various security risks for IT and describes the problems that can occur. The last catalog, “Maßnahmenkatalog” (measure catalog), lists measures that have to be taken in order

to prevent or avoid security risks. Each one of the IT building blocks is associated with one or more security risks, and these again are associated with appropriate measures to avoid them.

The last version of the IT-Grundschutz-Katalog was released in 2008. It gets updated with smaller additional parts if necessary. The latest version, however, does not cover IPv6 yet. IPv6 is named, if at all, only as a side note and considered as not relevant enough at that point of time. The only recommendation regarding IPv6 is that new network devices should be checked for IPv6 compliance and that IPv6 addresses are four times as long as IPv4. However, other documents for secure use of IPv6 have been published by the BSI. Among them is the guide for a secure deployment of IPv6.

The BSI published this updated secure networking guide “Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)” in July 2012 [65]. Before this, there existed an older version of the same guide that did not cover IPv6 at all. There was another small addition for IPv6 which only covered basic information. The new guide version two incorporates IPv6 from the beginning to end [65]. It is labeled as “Studie” (study) and provides a comprehensive overview of networking technology and protocols. The general structure of the BSI guide is the following.

First, it introduces computer networks with basic networking protocols and components, which are needed to set up a Local Area Network (LAN). Second, it provides a complete chapter introducing IPv6 basics (new in this version). This chapter covers basically all relevant technologies of IPv6 without going into much detail. The guide continues with introducing ways to connect to the Internet and explains basic security technologies, such as packet filters and concepts such as Demilitarized Zone DMZ. The next chapter covers a basic infrastructure for requirements that the BSI calls “normaler Schutzbedarf” (common protection requirements). This chapter recommends an architecture for network segmentation, address planning, and a structure for the implementation of a security gateway to connect to the Internet and use and deliver Internet services. Chapter 6 describes by what criteria security components should be selected, the standards according to which they should be configured, and how they can be securely operated. The last chapter, which accounts for one third of the document, covers potential security hazards and provides recommendations to mitigate them, or at least to reduce the probability of network outages. It does not only feature solutions for the common protection requirements, but also for higher protection requirements. Also worth mentioning is the appendix where several variations of the basic infrastructure are shown and a recommendation for an addressing concept with IPv6 is given.

5.1. Content Completeness and Depth of the BSI Guide

This section presents and evaluates the results of the assessment of the BSI guide for completeness and depth. The table follows the same scheme as in Section 4.1. The columns are: A = Count of covered RFCs, B = Count of relevant RFCs, C = Completeness, D = Weight (gray rows)/Importance Rating (white rows), E = Weighted Completeness (A*D), F = Depth. Category rows are shaded gray, with their subcategories below them (white rows). Values for subcategories are aggregated to the main categories. Totals are shown in the last line of the table (see Table 7).

Table 7. BSI Content Completeness and Depth. Columns: A = Count of covered RFCs; B = Count of relevant RFCs; C = Completeness; D = Weight/Importance Rating; E = Weighted Completeness (A * D); F = Depth.

Category	A	B	C	D	E	F
Specification & Address Format	27	57	0.47	0.22	0.10	0.28
Specification	3	4	0.75	6.17		0.40
Address Features	14	19	0.74	6.69		0.55
Header	7	13	0.54	6.05		0.22
Mobile IPv6	3	21	0.14	5.76		0.06
IPsec & ICMPv6	14	69	0.20	0.14	0.03	0.11
ICMPv6 Specification	4	6	0.67	6.03		0.40
Neighbor Discovery	5	11	0.45	6.59		0.29
Path MTU Discovery	1	1	1.00	6.00		0.40
Multicast Listener Discovery	2	5	0.40			0.16
IPsec	2	13	0.15	6.93		0.08
IKEv2	0	13	0.00	5.66		0.00
Cryptographic Methods	0	20	0.00	5.69		0.00
DHCPv6 & Autoconfiguration	4	14	0.29	0.21	0.06	0.16
Stateless Autoconfiguration	2	2	1.00	6.66		0.60
DHCPv6	2	12	0.17	6.28		0.08
Routing & DNS	10	40	0.25	0.24	0.06	0.11
DNS Specification	1	3	0.33	6.03		0.27
Security issues	1	9	0.11	6.62		0.04
DNSSEC	0	9	0.00	5.69		0.00
Multihoming	1	7	0.14	5.00		0.06
Routing Protocols	5	5	1.00	6.03		0.40
PIM	2	7	0.29	4.62		0.11
Transition Methods	11	33	0.33	0.20	0.07	0.16
Dual Stack	2	4	0.50	7.38		0.25
Tunneling	6	16	0.38	6.38		0.18
Translation	3	13	0.23	6.21		0.11
Totals	66	213	0.31		0.32	0.17

Overall: The BSI guide is not focused on details and also does not contain every aspect of IPv6. This can be seen when looking at the overall results. Only 66 out of the 213 relevant RFCs are covered in the guide, resulting in a completeness of 0.31 (31%). The weighted completeness increases this by 0.01 (1%) to 0.32 (32%). This means that the BSI guide, in general, takes the individual importance of the categories in consideration. Since the weights are quite evenly spread, their impact is only small. The depth is only 0.17. This is also due to the low coverage since missing RFCs receive a depth of 0 and thus have a huge negative impact on the overall depth. Nevertheless, this low value shows that the BSI guide does not explain all details of the included topics.

Specification and Address format: Twenty-seven out of the 57 relevant RFCs are covered in the BSI guide which results in a completeness of 0.47 (47%) in this category. In particular, *Mobile IPv6* is responsible for such a low value because only 3 of the possible 21 RFCs are at least mentioned. Without this subcategory, this result would be increased to 0.66. Also the other subcategories are missing some aspects, e.g., *Address Features* and *Header*. Depth is at 0.28. This value also got negatively affected by *Mobile IPv6* to a large extent. On the other hand, *Mobile IPv6* is rated relatively low for importance in our survey and thus the low attention might be justifiable. The other subcategories are relatively well described concerning depth and respective importance, even though *Header* should receive more coverage. The two subcategories *IPv6 Specification* and *Address Features* are ranked as the highest for importance within this category and are covered well.

IPsec and ICMPv6: This category received the lowest weighting of all categories and also achieves the lowest completeness value for the BSI guide. Out of 69 relevant RFCs only 14 are covered which results in 0.20 (20%) completeness. This is because the BSI guide is completely ignoring *Cryptographic Methods* and *IKEv2*. It also ignores IPsec to a large extent, only mentioning it as a side note. Without these three subcategories, the completeness would be above 50%. Still, there are also many RFCs missing in the other subcategories, except for *Path MTU Discovery* which only consists of one RFC. Completeness for the category is 0.11. Again this would be higher without the before mentioned categories. *Neighbor Discovery* only got a completeness of 0.29, which could be seen as negative but is a good result when taking into account that six out of eleven RFCs are not even covered. IPsec, as one of the most important topics, is barely covered. Its depth is also very low at 0.08. This shows that even the covered RFCs have not much detail. In general, completeness and depth of this category are very low and should be increased. At least IPsec should be given more room and explanation.

DHCPv6 and Autoconfiguration: The smallest of the five categories involves only 14 relevant RFCs. The BSI guide, however, only covers 4 of them. This results in a completeness of 0.29 or 29%. There are only two subcategories. *Stateless Autoconfiguration* has two RFCs, which are both covered in the BSI guide. The second subcategory *DHCPv6*, with the bigger part of 12 RFCs, is only represented with two of them, resulting in a completeness of 0.17, and thus lowering the completeness of the whole category. This also has an effect on depth. The main category only got a depth score of 0.16. While *Stateless Autoconfiguration* has a medium grade of 0.6, *DHCPv6* is as low as 0.08 which, basically, means this topic is barely mentioned. At least the main RFC about DHCPv6 is covered with a depth of medium (0.6). When looking at the importance rating, *Stateless Autoconfiguration* is well aligned, *DHCPv6* needs more coverage because an importance rating of 6.28 does not align with such a low depth and completeness.

Routing and DNS: The category with the highest weighting *Routing and DNS* is not well covered in the BSI guide. Only 10 out of 40 relevant RFCs are presented. This results in a completeness of 0.25 (25%). Except for the subcategory *Routing Protocols* that has all of its relevant RFCs at least mentioned and briefly explained (5 out of 5), all other subcategories have at most a completeness of 0.33. *DNSSEC* is not even mentioned at all, *Multihoming* is barely addressed and even *Security Issues* regarding DNS

receive almost no coverage (1 out of 9). Depth of the category is only 0.11 which is due to the many missing RFCs. Generally, only one of the three RFCs (RFC 3596—DNS extension for IPv6) received a high score for depth (0.8). Only because of this, the depth of the DNS Specification achieved 0.27, which is still less than “low”. The other subcategories have even lower depth scores. *Security issues* should be covered more profoundly since its importance rating is the highest of the category. A depth of only 0.04 on this topic is not acceptable for a secure deployment guide. *Routing Protocols* are well represented and depth is aligned with their importance. The same holds for Protocol Independent Multicast (*PIM*), which has the lowest importance rating of all subcategories and thus does not need to receive more attention. *DNSSEC* and *Multihoming* clearly are not dealt with sufficiently. While their importance rating is not the highest, giving a note about their existence or possible issues seems necessary.

In general, this category is underrepresented in the BSI guide, given its high importance as shown by the results of the survey. More focus has to be put on *Security Issues*. The other subcategories could also receive at least a bit more attention. Thus, this category has a lot room for improvement and should be looked at at the next revision of the guide.

Transition Methods: This category contains 11 out of 33 relevant RFCs. This results in a completeness of 0.33 (33%). *Dual Stack* is covered by 2 out of 4 (completeness = 0.5), *Tunneling* is covered by 6 out of 16 (completeness = 0.38), and *Translation* is covered by only 3 out of 13 (completeness = 0.23). Thus, translation techniques and tunnels are not represented to a high extent. This might be due to the fact that the guide discourages the use of these kind of transition methods. Nevertheless, these are necessary for many deployments and should be covered. Its depth score shows a similar picture. For the whole category, depth is at 0.16 (very low). Generally, all three subcategories have low depth values due to missing RFCs. Depth of *Dual Stack* is the highest with 0.25. Given that its completeness is 50%, depth is still not high enough since the survey revealed that this topic is actually the most important for a secure deployment of IPv6. The other two, while not as important, did only achieve a depth value of 0.18 (Tunneling) and 0.11 (Translation). As mentioned before, these two need a deeper coverage even though the guide mostly discourages their use if possible. Overall this is one of the categories where the BSI guide has huge potential for improvement. Completeness and depth show that this category is underrepresented when comparing the importance rating of the subcategories with the score values.

As mentioned in Section 5 the BSI guide is generally more focused on giving advice for practical implementation with focus on providing examples for various scenarios. The BSI guide only covers what it considers as necessary to know leaving out a lot of details. This was also proven by the scores depth and completeness. Nevertheless, it was shown that when compared to the importance rankings established by the survey, the guide does not focus enough on some areas and there is a lot room for improvement.

5.2. Topicality of the BSI Guide

The secure deployment guide by the BSI was published in the middle of 2012. As of the time of writing this paper, the presented information was up to date and all referenced sources and RFCs were referenced in their current version.

6. Comparison of the BSI and NIST Guides

This section compares the two guides to each other, using the depth and completeness scores. The guides differ a lot from each other, thus it is not surprising that the values of scores are very different as well. Table 8 shows the results of both guides in comparison using following columns: A = BSI completeness, B = NIST completeness, C = Completeness difference (B–A), D = BSI depth, E = NIST depth, F = Depth difference (E–D). Columns C and F show the difference between the two guides for completeness (C) and depth (F). The difference is calculated by subtracting the value of the score of the BSI guide from the value of the NIST guide. Thus a positive value in these columns stands for a higher value for NIST, and a negative value represents a higher value of the BSI guide.

Table 8. Comparison of BSI and NIST. Columns: A = BSI completeness; B = NIST completeness; C = Completeness difference (B–A); D = BSI depth; E = NIST depth; F = Depth difference (E–D).

(Sub)category	A	B	C	D	E	F
Specification & Address Format	0.47	0.88	0.40	0.28	0.52	0.24
IPv6 Specification	0.75	1.00	0.25	0.40	0.75	0.35
Address Features	0.74	0.95	0.21	0.55	0.64	0.09
Header	0.54	0.69	0.15	0.22	0.34	0.12
Mobile IPv6	0.14	0.90	0.76	0.06	0.49	0.43
IPsec & ICMPv6	0.20	0.86	0.65	0.11	0.40	0.29
ICMPv6 Specification	0.67	0.83	0.17	0.40	0.67	0.27
Neighbor Discovery	0.45	0.64	0.18	0.29	0.36	0.07
Path MTU Discovery	1.00	1.00	0.00	0.40	0.60	0.20
Multicast Listener Discovery	0.40	0.80	0.40	0.16	0.32	0.16
IPsec	0.15	0.77	0.62	0.08	0.37	0.29
IKEv2	0.00	1.00	1.00	0.00	0.40	0.40
Cryptographic Methods	0.00	0.95	0.95	0.00	0.38	0.38
DHCPv6 & Autoconfiguration	0.29	0.86	0.57	0.16	0.40	0.24
Stateless Autoconfiguration	1.00	1.00	0.00	0.60	0.70	0.10
DHCPv6	0.17	0.83	0.67	0.08	0.35	0.27
Routing & DNS	0.25	0.73	0.48	0.11	0.37	0.26
DNS Specification	0.33	0.33	0.00	0.27	0.33	0.07
Security issues	0.11	0.89	0.78	0.04	0.49	0.44
DNSSEC	0.00	0.56	0.56	0.00	0.27	0.27
Multihoming	0.14	0.86	0.71	0.06	0.43	0.37
Routing Protocols	1.00	0.80	-0.20	0.40	0.36	-0.04
PIM	0.29	0.71	0.43	0.11	0.29	0.18
Transition Methods	0.33	0.73	0.39	0.16	0.41	0.25
Dual Stack	0.50	1.00	0.50	0.25	0.60	0.35
Tunneling	0.38	0.75	0.38	0.18	0.45	0.28
Translation	0.23	0.62	0.38	0.11	0.29	0.18
Totals	0.31	0.82	0.51	0.17	0.43	0.26

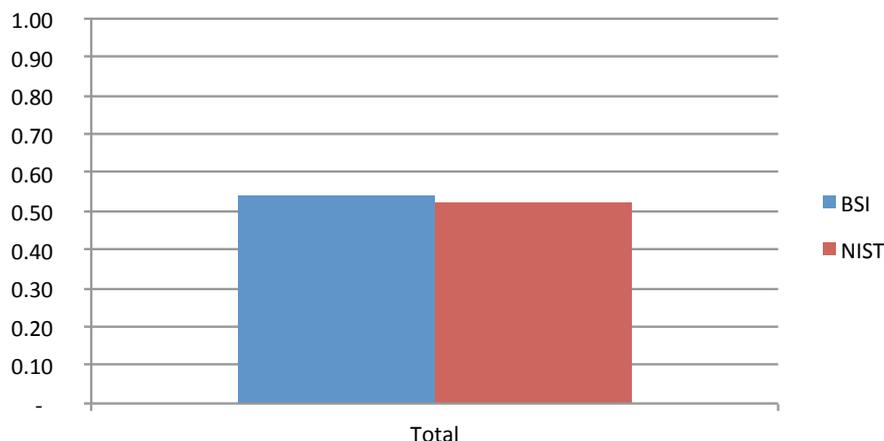
On average the completeness of the NIST guide is 0.41 higher than the completeness of the BSI guide. When looking at the totals, the difference is even higher. 0.51 is the total difference in completeness

based on the total counts of relevant RFCs and covered RFCs. This means that the NIST guide covers 41% more RFCs on average and even 51% in total. There is only one occurrence of a negative value (BSI > NIST). This is the subcategory *Routing Protocols*. Here the BSI guide covers all of the relevant RFCs, while the NIST guide covers 80% (4 out of 5). Both guides have equal completeness values in three subcategories. Both completely covered the subcategories *Path MTU Discovery* and *Stateless Autoconfiguration*. They also have the same value (0.33) in the subcategory *DNS Specification* where both covered the main RFC for DNS for IPV6, but ignored the other two relevant RFCs. In all other subcategories and all main categories, the NIST guide is superior to the BSI guide in terms of completeness.

The content depth score of the NIST guide is on average 0.22 higher than the depth of the BSI guide and 0.26 higher in the total results. These results imply that the NIST guide is on average and in total at least one level better concerning depth with respect to the levels definitions of Section 3.2 (missing, very low, low, medium, high, very high). In total, depth of the BSI guide is very low at 0.17 and the NIST guide is a little above medium, with a value of 0.43. This shows that the NIST guide is generally much more detailed and provides more explanations and examples. There is only one subcategory where the BSI guide exceeds the NIST guide in depth which is *Routing Protocols*. However, the BSI value is only 0.04 higher and thus both are still close together. There are in total three subcategories where both are less than 0.1 apart from each other and another three within 0.12 difference. On the other hand, there are also six subcategories where both guides differ more than 0.3 points in depth. This group is lead by *DNS Security Issues*, with a difference of 0.44 in depth and followed by *IKEv2*, with a 0.4 points difference.

Figure 8 shows the average depth of covered RFCs for both guides, which is the ratio of aggregated depth scores to the number of actually covered RFCs. From this perspective it becomes clear that both guides have on average a low to medium depth for covered RFCs. Interestingly, the depth of RFCs that are covered is slightly higher in the BSI guide than it is in the NIST guide. This is because the NIST guide often only mentions relevant RFCs without going into detail while the BSI guide only covers RFCs that it also explains at least to some extent.

Figure 8. Average depth of covered RFCs in total.

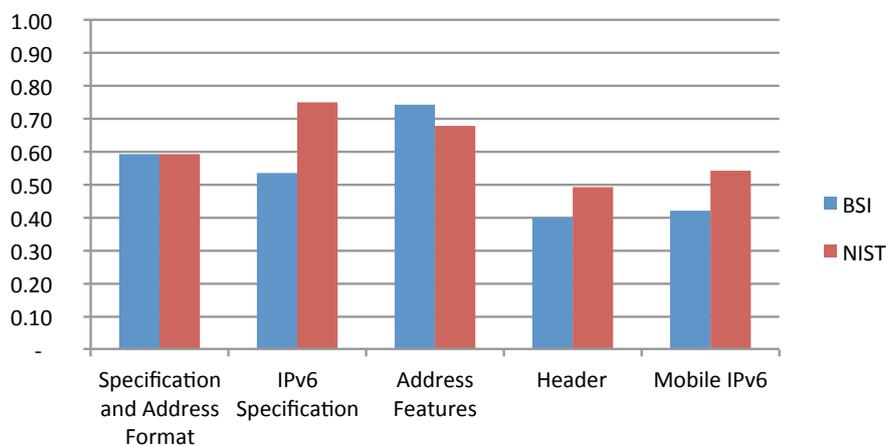


There are some subcategories where differences become particularly evident. Within the category *Specification and Address Format*, the subcategory *Mobile IPv6* stands out the most. This subcategory

is barely covered by the BSI guide (0.14), but received a lot more coverage from the NIST guide (0.9). Nevertheless, both guides did not cover this subcategory much in terms of depth. The NIST guide achieved a depth of 0.42. This is 0.23 higher than the value of the BSI guide. The BSI guide does not yet consider *Mobile IPv6* as an important topic for an initial deployment of IPV6. The NIST guide, however, does provide more coverage of the topic as shown by the completeness and depth values. The coverage by the BSI guide can be considered too low when looking at the importance rating of 5.76. While this value is not high, it still indicates the need for at least medium coverage in a secure deployment guide.

The *IPv6 Specification* is explained well by both guides (BSI = 0.75 vs. NIST = 1.0), but is discussed in much more detail by the NIST guide (BSI = 0.4 vs. NIST = 0.75). In respect to the importance ranking of 6.17 the results are still good for both guides. The other two subcategories are relatively close together in terms of completeness as well as depth. Figure 9 shows the average depth in this category. Both guides provide on average medium depth for the RFCs they cover (around 0.6). *IPv6 Specification* is explained in much more detail by the NIST guide. *Address Features* are important for both guides. The BSI guide on average is even more detailed in describing the RFCs it covers than the NIST guide. The figure also shows that the BSI guide does not deal with the subcategories *Header* and *Mobile IPv6*, while the NIST guide at least has almost medium coverage for *Mobile IPv6*.

Figure 9. Average depth of IPv6 specification and address format.

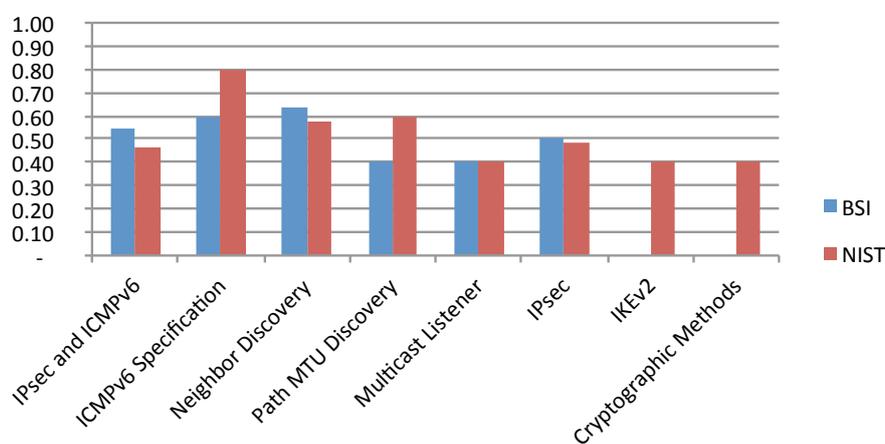


The difference between the BSI and NIST guides is surprisingly large in the category *IPsec and ICMPv6*. While the NIST guide covers 86% of all relevant RFCs, the BSI guide merely covers 20%. This also shows in the depth score, with a difference of 0.29 points in depth in favor of the NIST guide. There are two subcategories that have a huge impact on the outcome of the results for the main category. Those two are *IKEv2* and *Cryptographic Methods*. On the BSI side, both subcategories were completely ignored. The BSI guide does not contain any cryptographic methods at all, even though they play an important role in IPsec. Though on the one hand the NIST guide covers almost every RFC in these two subcategories, on the other hand it provides only low depth of coverage. Thus most relevant topics are only named or are briefly explained. From an importance point of view, the way the NIST guide handles these topics seems to be sufficient. The BSI guide, in contrast, should increase coverage at least for *IKEv2*. Even though IPsec is not a mandatory part of IPv6 anymore, the BSI guide should generally improve coverage of IPsec as its use is highly recommended.

ICMPv6 is well covered by both guides for most parts. Again, coverage by the NIST guide is more complete and deeper over all subcategories. *Multicast Listener Discovery* is handled more profoundly by the NIST guide as indicated by a difference in completeness of 0.4 points. This could be an important security mechanism in the future as use of multicast might increase. As for now, more coverage should not be necessary.

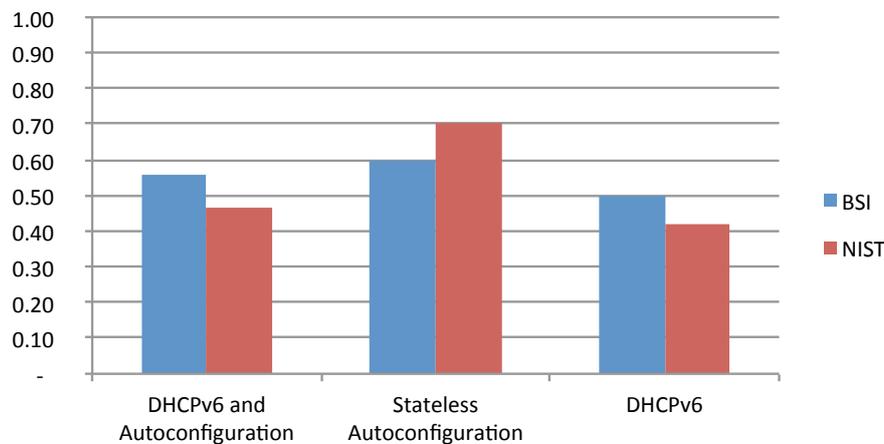
Figure 10 shows the depth of RFCs covered in this category. From this point of view the BSI guide is more detailed than the NIST guide. Nevertheless, the figure shows that the NIST guide is very detailed in presenting the *ICMPv6 Specification* and also more detailed for PMTU than the BSI guide. The NIST guide discusses IKEv2 and Cryptographic Methods but only with low detail. In all other subcategories, the two guides are close together when only looking at covered RFCs.

Figure 10. Average depth of IPsec and ICMPv6.



Both guides also differ to a large extent in the category *DHCPv6 and Autoconfiguration*. The difference lies at 0.57 points in completeness and 0.24 points in depth. Most of this is, however, due to the lack of coverage of DHCPv6 in the BSI guide. As DHCP has not changed much to support IPv6, the BSI guide barely mentions it. The NIST guide, however, contains a lot more of the relevant RFCs for reference, but does not cover DHCPv6 in detail either. *Stateless Autoconfiguration*, one of the new important features of IPv6, is completely covered by both guides. From a depth point of view, the NIST guide is slightly more detailed including examples for stateless autoconfiguration. All in all both guides sufficiently handle this topic.

Figure 11 shows the average depth of covered RFCs for this category. From this perspective the BSI guide is on average more detailed than the NIST guide. On the one hand *Stateless Autoconfiguration* is explained in more detail by the NIST guide, and on the other hand the BSI guide does better for *DHCPv6* on average. This shows that the BSI guide does not cover many RFCs regarding DHCPv6, but the ones that are, are covered well. Both guides provide more detailed descriptions for *Stateless Autoconfiguration* than for *DHCPv6*.

Figure 11. Average depth of DHCPv6 and autoconfiguration.

Routing and DNS is overall 0.48 completeness points better covered by the NIST guide than the BSI guide. Additionally, depth of both guides is very low. On the one hand the BSI guide is down to 0.11 points in depth, on the other hand the NIST guide also has a low rating of 0.37. As this category received the highest weighting and thus highest importance, it should have been discussed more by both guides and in particular the BSI guide.

Both guides are equal in the coverage of *DNS Specification*, containing 1 out of 3 relevant RFCs, although the NIST guide has a better depth, featuring more detail in explaining the specification. This is a shortcoming of the BSI guide. *DNS for IPv6* is another example for the BSI guides focusing only on basics. Except for the specification, there is not much more coverage of other DNS-relevant topics. *Security issues* and *DNSSEC* are barely mentioned by the BSI guide as shown by the completeness values of 0.11 and 0. The NIST guide, however, contains almost all security issues (0.89) and also in detail as the depth value of 0.49 indicates. *DNSSEC* is covered by the NIST guide, however, only 56% of it and most of it is only mentioned.

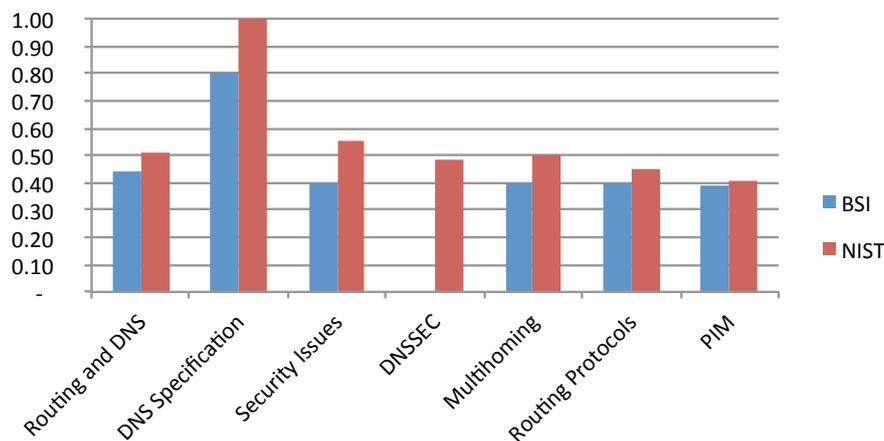
Multihoming was also very superficially explained in the BSI guide (0.14), but extensively handled in the NIST guide (0.86). Multihoming is very common today as it improves reachability of sites even if one of its ISPs should fail. There are new issues arising with multihoming because of IPv6 routing. While the NIST guide considers these as relevant, the BSI guide does not.

Routing Protocols is the only subcategory that shows a different picture. This time the BSI guide exceeds the NIST guide in completeness and depth. Routing protocols are of medium importance. All in all both guides do well in covering this subcategory although depth of coverage should be increased, as low depth is not sufficient. Finally, Protocol Independent Multicast (PIM) is a subcategory of minor importance. The NIST guide once again has higher completeness and depth values for this subcategory than the BSI guide. Taking the low importance into consideration, coverage of both guides seems to be sufficient.

Figure 12 shows the average depth of the RFCs that are covered from this category. As the figure reveals, both guides provide only low depth for most topics of this category. Still the NIST guide does better in all of them. Worth mentioning is that both guides focus especially on the *DNS Specification* as

the BSI guide achieves a depth of 0.8 (high) and the NIST guide even a score of 1 (very high). It should be noted though that both guides only covered the main RFCs for this subcategory.

Figure 12. Average depth of routing and Domain Name System (DNS).



The last category to be compared is *Transition Methods*. The NIST guide covers 39% more of the relevant RFCs than the BSI guide. Both guides go into more detail with *Dual Stack* than with *Tunneling* and *Translation*. *Dual Stack* is covered more broadly as well as in more detail by the NIST guide. It is the most important topic, thus, depth should be better than medium, and examples should be given on how to deploy a dual stack infrastructure. Both guides achieve only low scores and have room for improvement.

Tunneling and *Translation* are important topics as the results of the survey show. However, both guides discourage the use of these methods as they should only be used as a last resort and be replaced as soon as alternatives become available. Nevertheless, they must be covered by a secure deployment guide because they can introduce security issues.

Figure 13 shows the average depth of RFCs that are covered for this category. As the figure shows, the NIST guide provides a medium level of detail for *Dual Stack* and *Tunneling*, while the BSI guide has medium to low depth for these subcategories. Both have only less than 0.5 depth in the subcategory *Translation*. According to these results translation methods are seen as least important by both guides.

Weighted Completeness: This score was established by combining the weights established by using AHP and the survey, and multiplying them with the completeness values derived by the evaluation. Table 9 shows the results for the two guides. Because the weights are all close, the weighted completeness differs only to a small extent from the completeness without weights. The difference between the two guides without weights was 0.51, and with weights 0.49. The impact of the weights was positive for the BSI guide and negative for the NIST guide, and brought both a little closer together. All in all this does not change the assessment that the NIST guide is far ahead in terms of completeness and covers a lot more of the relevant RFCs than the BSI guide does.

Figure 13. Average depth of transition methods.

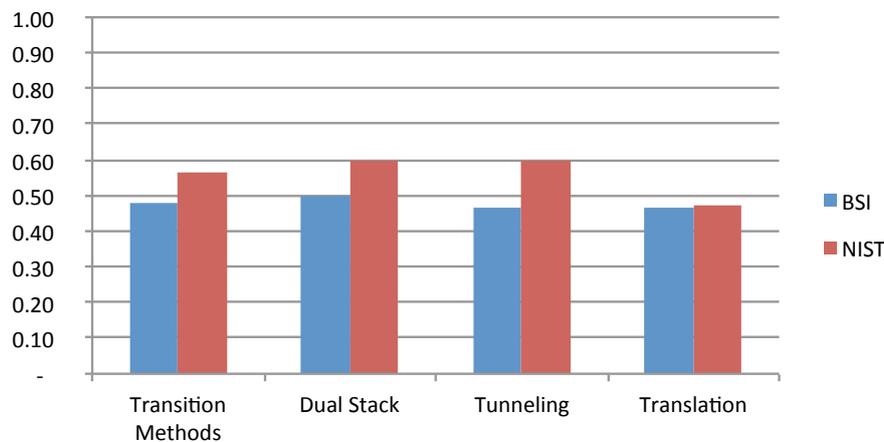


Table 9. Comparison of weighted completeness.

Category	Weight	BSI	NIST
Specification and Address format	0.22	0.10	0.19
IPsec and ICMPv6	0.14	0.03	0.12
DHCPv6 and Autoconfiguration	0.21	0.06	0.18
Routing and DNS	0.24	0.06	0.17
Transition Methods	0.20	0.07	0.15
Total	1.00	0.32	0.81

7. Results and Recommendations

This section summarizes the results of the evaluation and comparison of both guides. Furthermore, areas for possible improvements are given. Table 10 shows the results and recommendations for the NIST guide derived from the evaluation of topicality, completeness and depth. Table 11 does the same for the BSI guide.

The NIST guide should improve in topicality. Published RFCs on IPv6 since 2010 should be considered for coverage. There are also newer versions of some RFCs, which should be updated and changes should be checked and included into the guide as well. Some of the covered transition methods are outdated and should be considered for removal from the guide. NIST is recommended to take new developments, IETF standards, and security breaches relevant for IPv6 deployments into account in order to keep the guide up to date. Since the guide already features a very high completeness, it is only recommended to keep an eye on new developments, so that this score would stay high in future versions of the guide.

From the viewpoint of content depth, the guide could improve by incorporating practical examples for concrete infrastructures and distinguishing between different security requirements. This is one important feature of the BSI guide that could increase the quality of the NIST guide as well. There are some areas where depth could still be positively increased by extending explanations or providing better examples. These areas are DHCPv6, ND, IPsec, DNS security issues, Routing Protocols, and

Dual Stack. Depth of the coverage of ICMPv6 specification could be decreased since the discussion is rather extensive.

As Table 11 shows, topicality of the BSI guide is good because the new version was published more recently. It is only recommended to check for new relevant security breaches and IETF standards on regular basis to keep the guide up to date. Completeness, however, is very low throughout the guide, as the guide focuses on only the most relevant RFCs, technologies, and methods. Nevertheless coverage of IPsec, DHCPv6, DNS security issues, Multihoming, Dual Stack, and Tunneling should be increased. Cryptographic Methods and DNSSEC, which are not covered so far, should at least be mentioned in order to let readers know about their existence.

Table 10. NIST—Results and recommendations.

Criteria	Results	Recommendations
Topicality	<ul style="list-style-type: none"> ● Most of the content is still valid and up to date. ● Some RFCs have newer versions, see Section 4.2 ● RFCs published after 2010 are not covered. ● Some methods and techniques are outdated. 	<ul style="list-style-type: none"> ● Update RFC versions and check for changes. ● Consider coverage of RFCs published after 2010. ● Reconsider coverage of outdated or discouraged methods (e.g., NAT-PT). ● Watch out for new security breaches. ● Watch out for changes in IETF standards.
Completeness	<ul style="list-style-type: none"> ● High completeness (0.82). ● High weighted completeness (0.81). ● Strong focus on broad coverage of IPv6-relevant topics. ● Many missing RFCs are later than 2010. 	<ul style="list-style-type: none"> ● Watch out for new RFCs.
Depth	<ul style="list-style-type: none"> ● Very detailed explanations for specifications. ● Generally well aligned with importance ratings of the survey. ● Highly informative character. ● Average depth of covered RFCs at 0.54 (medium to low). ● Many RFCs are only mentioned or briefly explained. ● Only few practical examples. 	<ul style="list-style-type: none"> ● Include practical examples for concrete infrastructures. ● Distinguish between different security requirements. ● Increase depth for DHCPv6. ● Increase depth for ND and IPsec. ● Coverage of ICMPv6 could be reduced. ● Increase depth for DNS security issues. ● Increase depth for Routing Protocols. ● Increase depth for Dual Stack.

Table 11. BSI—Results and recommendations.

Criteria	Results	Recommendations
Topicality	<ul style="list-style-type: none"> • Content is up to date. 	<ul style="list-style-type: none"> • Watch out for new security breaches. • Watch for changes in IETF standards.
Completeness	<ul style="list-style-type: none"> • Focuses on techniques used in practice. • Focuses on main specifications. • Low overall completeness (0.31). • Low weighted completeness (0.32). • Low coverage of IPsec, Mobile IPv6, DHCPv6, DNS security issues, Multihoming and Translation. • No coverage of Cryptographic Methods, IKEv2 and DNSSEC. 	<ul style="list-style-type: none"> • Increase coverage of IPsec and Cryptographic Methods. • Increase coverage of DHCPv6. • Increase coverage of DNS security issues, DNSSEC and Multihoming. • Increase coverage of Dual Stack and Tunneling. • Watch out for new relevant RFCs.
Depth	<ul style="list-style-type: none"> • High depth score for main specifications. • Very low overall depth (0.17). • Medium to low depth of covered RFCs (0.56). • Low content depths due to low completeness. 	<ul style="list-style-type: none"> • Generally increase depth by giving practical examples. • Increase depth for IPv6 Specification. • Increase depth for IPsec. • Increase depth for DHCPv6. • Increase depth for DNS security issues, Multihoming and Routing Protocols. • Increase depth for Dual Stack and Tunneling.

As can be seen in the comparison of the two guides, the depth of covered RFCs is actually not as bad as it seems when analyzing the overall depth. Nonetheless, content depth could generally be increased by incorporating more practical examples, and also the main IPv6 specification could be covered in more detail. This is even more important for IPsec, DHCPv6, DNS security issues, Multihoming, Routing Protocols, Dual Stack and Tunneling. These are all relevant topics and should be explained in more detail and with examples.

Besides these results and recommendations, there are also other aspects to look at. In particular, the BSI guide features very well designed deployment scenarios, which are worth mentioning, but could not be evaluated with the formal scores used in this study. Also, the NIST guide has some qualities that can not be captured by only using completeness and depth. Table 12 lists the pros and cons of the two guides, taking the so far not covered aspects into consideration.

Table 12. Pros and cons of the guides.

	BSI	NIST
Pros	<ul style="list-style-type: none"> • Topical secure deployment guide. • Focus on main IPv6 features relevant for actual implementation. • Various infrastructure examples for a deployment. • Recommendations for different security requirements. • Good, compact overview of IPv6 features. • Easy to understand for experienced practitioners. 	<ul style="list-style-type: none"> • Very good introduction to IPv6 and relevant topics. • Covers almost all IPv6 topics by at least mentioning them. • Good and understandable summaries and explanations of difficult topics. • Sticks very close to the RFC content. • Features a checklist for actual deployments. • Suitable for complete IPv6 beginners.
Cons	<ul style="list-style-type: none"> • Falls short on transition methods. • Explanations of IPv6 relevant topics not very detailed. • Readers should not be completely new to IPv6. • Readers must know about methods and technologies which already existed for IPv4. • Some topics such as IPsec, DNSSEC, or Cryptographic Methods are not covered at all or only very superficially. 	<ul style="list-style-type: none"> • Falls short on practical examples not covered by the RFCs. • Some information seems too detailed or irrelevant for an actual deployment. • Also covers old and experimental techniques and methods not useful for actual deployments. • No differentiation of security requirements.

The evaluation has shown that the two guides by BSI and NIST differ a lot. While the NIST guide focuses on complete coverage of all relevant topics and sticks close to the IETF standards, it is sometimes overloaded with details and falls short on practical implementation examples. Nonetheless, it provides a very good introduction and explains possible security issues of most of the relevant topics. Practitioners looking for a detailed guide and who do not have much knowledge about IPv6 should choose this guide as a preparation for a real deployment. They can be sure that almost all relevant information is covered or at least referenced. As actual deployment scenarios differ, the guide does not distinguish between scenarios, and practitioners have to decide themselves which parts of the guide are relevant for the individual case.

The BSI guide tries to cover only the most relevant topics for an actual deployment and thus leaves out many other issues. The level of detail for covered topics is good, while other relevant information gets neither mentioned, nor referenced in any way. The guide is particularly useful for practitioners with good experience with IPv4 and at least some with IPv6. The main features are the different infrastructure

scenarios with recommendations for several security requirements. The guide does not provide many practical examples of how to use IPv6, but clearly states which technologies and methods should be used to keep the network secure. Transition methods are mostly discouraged by the guide and thus barely covered. Practitioners seeking information about the use of transition methods should consider additional sources of information. Last but surely not least for an international audience of practitioners, it is required to understand German as the relevant version of the guide is so far published in German only.

8. Limitations and Future Work

The scores used to evaluate the two guides by NIST and BSI can also be used to evaluate other deployment guides or books for IPv6. Furthermore the BSI and NIST guides should be reevaluated when updated versions get published. For this purpose the list of relevant RFCs should be kept up to date as well. One could also investigate in future work if these guides offer misleading advice induced by governmental organizations that could lead to a weakening of security, such as in the case of the U.S. National Security Agency weakening a certain cryptographic standard issued by NIST [66].

The importance ratings and the weights established in the survey are gathered for a general deployment scenario and by interviewing a limited group of experts. A larger survey, ideally repeated on a regular basis, could lead to more robust importance weightings of categories and also reflect changes of the audiences over time.

In practice, there are various deployment scenarios with differing requirements. For example, stateless autoconfiguration might be interesting for infrastructures with many flexible workstations, but has minor relevance for an IPv6 deployment in a datacenter where often static configurations are preferred. Importance ratings and weights should be calculated for the different (and possibly individual) scenarios and applied for evaluation of the guides. Last but not least, the two guides should be also applied in a real IPv6 deployment to evaluate the actual usefulness in a controlled practical environment.

9. Conclusions

In this article, two main scores for the evaluation of the secure deployment guides by NIST and BSI were developed. Completeness is a score evaluating the coverage of relevant RFCs published by the IETF. This score was also weighted for importance by using the weights established using the method of AHP on the results of the survey. The second score, content depth, is based on completeness and indicates to what extent the relevant RFCs are covered. Both scores were applied using the individual RFCs and aggregated for subcategories and main categories. As another contribution, a complete list and topical classification of relevant RFCs published by the IETF can be found in Appendix A. This is also basis for the evaluation of the guides performed in this paper.

Furthermore, the survey revealed not only weights for the main categories but also an importance ranking for the subcategories, which were also used in the evaluation. After the survey was performed and scores were calculated, both guides were evaluated individually and then compared to each other. The evaluation showed that both guides provide valid and good information for practitioners seeking information for a secure deployment. While the BSI guide is less detailed and focused on main specification and most relevant topics, the NIST guide is more comprehensive and detailed, sticking

closer to the contents of the RFCs. However, the BSI guide features various implementation scenarios and takes different security requirements into consideration.

Both guides have proven to be valid choices for preparation of a secure deployment of IPv6. While some possibilities for improvement have been found, none of these findings have been critical. Possible improvements were established and recommended for both guides. Recommendations were made to increase topicality, completeness and depth based on the results of the survey and the evaluation.

Conflicts of Interest

The authors declare no conflict of interest.

Appendix

A. List of Relevant RFCs for IPv6

This section shows tables with IPv6-relevant RFCs that were used to measure completeness of the security guides. Table A1 explains the columns of the following tables.

Table A1. Explanation of columns for the following RFC tables.

RFC	Number of the RFC
Title	Title of the RFC
Type	Type of the RFC: <ul style="list-style-type: none"> • BCP—Best Current Practice. • Info—Informational RFC (e.g., idea, usage, note to the community). • Exp—Very early standard stage for experimental usage. • Proposed—Proposition for a standard. • Draft—Draft standard with at least two independent implementations. • Standard—Official Internet standard.
N1	Completeness score for the NIST deployment guide. Value of 1 if RFC is covered, or value of 0 if RFC is not covered in the deployment guide by NIST.
N2	Depth score for the NIST deployment guide. Values are explained in Section 3.1.
B1	Completeness score for the BSI deployment guide. Value of 1 if RFC is covered, or value of 0 if RFC is not covered in the deployment guide by BSI.
B2	Depth score for the BSI deployment guide. Values are explained in Section 3.1

A.1. IPv6 Specification and Address Format

Table A2. RFCs on IPv6 specification and address format.

RFC	Title	Type	N1	N2	B1	B2
Specification						
	IPv6 Specification	draft		high		low
2460 [23]	Header format		1	high	1	medium
	Extension headers		1	high	1	low
	Minimum traffic size		1	high	1	medium
	Upper layer issues		1	medium	0	missing
Address Features						
4291 [36]	IPv6 Addressing Architecture	draft	1	high	1	high
	Model		1	very high	1	high

Table A2. Cont.

RFC	Title	Type	N1	N2	B1	B2
	Textual prefix representation		1	very high	1	very high
	Address types		1	high	1	high
	Address scope		1	high	1	medium
	Anycast addresses		1	low	1	high
	Multicast addresses		1	very high	1	high
5375 [67]	IPv6 Unicast Address Assignment Considerations	info	1	medium	0	missing
5952 [68]	Recommendations for secure textual representation of addresses	info	0	missing	1	very high
3587 [69]	Global Unicast address format	info	1	high	0	missing
2526 [70]	Reserved Subnet IPv6 Anycast addresses	proposed	1	medium	1	high
3879 [71]	Deprecating site-local addresses	proposed	1	high	1	high
4193 [72]	Unique local IPv6 Unicast addresses	proposed	1	low	1	medium
3849 [73]	IPv6 address prefix reserved for documentation	info	1	high	1	medium
2375 [74]	Multicast address assignment	info	1	low	1	low
5156 [75]	Special-use IPv6 addresses	info	1	high	1	high
4007 [76]	IPv6 scoped address architecture	proposed	1	low	1	medium
6724 [77]	Default address selection	proposed	1	low	0	missing
3531 [78]	A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block	Info	1	high	0	missing
3972 [79]	Cryptographically Generated Addresses (CGA)	proposed	1	low	0	missing
IPv6 Header						
2675 [80]	IPv6 Jumbograms	proposed	1	medium	1	low
2711 [81]	IPv6 router alert option	proposed	1	low	1	low
6398 [82]	IP Router Alert Considerations and Usage	BCP	0	missing	0	missing
5095 [83]	Deprecation of type 0 routing headers in IPv6	proposed	1	medium	0	missing
2474 [84]	Definition of the DS-field in IPv4 and IPv6 headers	proposed	1	low	1	low
1809 [85]	Using the flow label field in IPv6	info	1	low	1	low
6437 [86]	IPv6 Flow Label Specification	proposed	1	low	1	low
6564 [87]	A Uniform Format for IPv6 Extension Headers	proposed	0	missing	0	missing
5722 [88]	Handling of Overlapping IPv6 Fragments	proposed	0	missing	0	missing
4489 [89]	A Method for Generating Link-Scoped IPv6 Multicast Addresses	proposed	0	missing	0	missing
3306 [90]	Unicast-Prefix-based IPv6 Multicast Addresses	proposed	1	high	0	missing
4302 [91]	IP Authentication Header (AH)	proposed	1	low	1	low
4303 [92]	IP Encapsulating Security Payload (ESP)	proposed	1	low	1	low
Mobile IPv6						
	Mobility support for IPv6	proposed	1	medium	1	low
	Mobile IPv6 security		1	high	0	missing
	Mobility Header		1	medium	0	missing
	Mobility Options		1	medium	0	missing
6275 [93]	ICMP Messages		1	high	0	missing
	Neighbor Discovery		1	low	0	missing
	Correspondent Node Operations		1	low	0	missing
	Home Agent Operations		1	low	0	missing
	Mobile Node Operations		1	low	0	missing
	Security Considerations		1	high	1	low
4283 [94]	Mobile node identifier options for MIPv6	proposed	0	missing	0	missing
4866 [95]	Enhanced route optimization for MIPv6	proposed	0	missing	1	low
3776 [96]	Using IPSec to protect MIPv6 signaling between Mobile Nodes and HA	proposed	1	low	0	missing
4225 [97]	Mobile IP Version 6 Route Optimization Security Design Background	info	1	low	0	missing
4285 [98]	Authentication Protocol for Mobile IPv6	info	1	medium	0	missing
4487 [99]	Mobile IPv6 and Firewalls: Problem Statement	info	1	medium	1	low
4449 [100]	Securing Mobile IPv6 Route Optimization Using a Static Shared Key	proposed	1	medium	0	missing

Table A2. Cont.

RFC	Title	Type	N1	N2	B1	B2
4882 [101]	IP Address Location Privacy and Mobile IPv6: Problem Statement	info	1	medium	0	missing
4877 [102]	Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture	proposed	1	medium	0	missing
4640 [103]	Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)	info	1	low	0	missing
5026 [104]	Mobile IPv6 Bootstrapping in Split Scenario	proposed	1	low	0	missing
5555 [105]	Mobile IPv6 Support for Dual Stack Hosts and Routers	proposed	1	low	0	missing

A.2. IPsec and ICMPv6

Table A3. RFCs on IPsec and ICMPv6.

RFC	Title	Type	N1	N2	B1	B2
ICMPv6 Specification						
	ICMPv6	draft	1	high	1	medium
	Message Formats		1	medium	0	missing
4443 [34]	Error Messages		1	high	1	medium
	Informational Messages		1	high	1	medium
	Security Considerations		1	high	1	low
4884 [106]	Extended ICMP to Support Multi-Part Messages	proposed	0	missing	0	missing
4890 [61]	Recommendation for Filtering ICMPv6 Messages Firewalls	info	1	very high	1	high
Neighbor Discovery						
	Neighbor discovery	draft	1	high	1	medium
	Message Formats		1	medium	0	missing
	Router Discovery		1	low	1	low
4861 [35]	Neighbor unreachability Detection and Address Resolution		1	medium	1	medium
	Redirect Functions		1	low	1	medium
	Security Considerations		1	very high	1	high
3756 [107]	IPv6 Neighbor Discovery (ND) Trust Models and Threats	info	1	medium	1	high
5942 [108]	IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes	proposed	0	missing	0	missing
3971 [109]	Secure Neighbor Discovery (SEND)	proposed	1	low	0	missing
6494 [110]	Certificate Profile and Certificate Management for Secure Neighbor Discovery (SEND)	proposed	0	missing	0	missing
6495 [111]	Subject Key Identifier (SKI) Secure Neighbor Discovery (SEND) Name Type Fields	proposed	0	missing	0	missing
3122 [112]	Inverse neighbor discovery	proposed	0	missing	0	missing
Path MTU Discovery						
1981 [37]	Path MTU discovery	draft	1	medium	1	low
Multicast Listener Discovery						
2710 [113]	Multicast Listener Discovery (MLD) for IPv6	proposed	1	low	1	low
3590 [114]	Source Address Selection for the Multicast Listener Discovery (MLD) Protocol	proposed	0	missing	0	missing
3810 [115]	Multicast Listener Discovery Version 2 (MLDv2) for IPv6	proposed	1	low	1	low
4604 [116]	IGMPv3 and MLDv2 for Source-Specific Multicast	proposed	1	low	0	missing
4286 [117]	Multicast Routing Discovery	proposed	1	low	0	missing
IPsec						
2207 [118]	RSVP Extensions for IPSEC Data Flows	proposed	1	low	1	low
4230 [119]	RSVP Security Properties	info	1	low	0	missing

Table A3. Cont.

RFC	Title	Type	N1	N2	B1	B2
4301 [28]	Security Architecture for the Internet Protocol	proposed	1	medium	1	medium
3168 [120]	The Addition of Explicit Congestion Notification (ECN) to IP	proposed	1	low	0	missing
6040 [121]	Tunnelling of Explicit Congestion Notification	proposed	0	missing	0	missing
4304 [122]	ESN Addendum to IPsec DOI for ISAKMP	proposed	1	low	0	missing
4835 [123]	Cryptographic Algorithm Implementation Requirements for ESP and AH	proposed	1	medium	0	missing
4307 [124]	Cryptographic Algorithms for Use in the IKEv2	proposed	1	medium	0	missing
4308 [125]	Cryptographic Suites for IPsec	proposed	1	low	0	missing
5406 [126]	Guidelines for Specifying the Use of IPsec Version 2	BCP	1	low	0	missing
6379 [127]	Suite B Cryptographic Suites for IPsec	info	0	missing	0	missing
5374 [128]	Multicast Extensions to the Security Architecture for the Internet Protocol	proposed	1	medium	0	missing
5910 [129]	Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)	proposed	0	missing	0	missing
IKEv2						
5996 [130]	Internet Key Exchange Protocol Version 2 (IKEv2)	proposed	1	low	0	missing
6071 [131]	IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap	info	1	low	0	missing
5739 [132]	IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)	experimental	1	low	0	missing
5685 [133]	Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)	proposed	1	low	0	missing
5723 [134]	Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption	proposed	1	low	0	missing
5840 [135]	Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility	proposed	1	low	0	missing
5879 [136]	Heuristics for Detecting ESP-NUL packets	info	1	low	0	missing
5998 [137]	An Extension for EAP-Only Authentication in IKEv2	proposed	1	low	0	missing
6027 [138]	IPsec Cluster Problem Statement	info	1	low	0	missing
6290 [139]	A Quick Crash Detection Method for the Internet Key Exchange Protocol (IKE)	proposed	1	low	0	missing
6311 [140]	Protocol Support for High Availability of IKEv2/IPsec	proposed	1	low	0	missing
4555 [141]	IKEv2 Mobility and Multihoming Protocol (MOBIKE)	proposed	1	low	0	missing
4621 [142]	Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol	info	1	low	0	missing
Cryptographic Methods						
2404 [143]	The Use of HMAC-SHA-1-96 within ESP and AH	proposed	1	low	0	missing
2410 [144]	The Null Encryption Algorithm and Its Use With IPsec	proposed	1	low	0	missing
2451 [145]	The ESP CBC-Mode Cipher Algorithms	proposed	1	low	0	missing
3526 [146]	More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)	proposed	1	low	0	missing
3566 [147]	The AES-XCBC-MAC-96 Algorithm and Its Use with IPsec	proposed	1	low	0	missing
3602 [148]	The AES-CBC Cipher Algorithm and Its Use with IPsec	proposed	1	low	0	missing
3686 [149]	Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)	proposed	1	low	0	missing
4106 [150]	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	proposed	1	low	0	missing
4309 [151]	Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)	proposed	1	low	0	missing

Table A3. Cont.

RFC	Title	Type	N1	N2	B1	B2
4359 [152]	The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)	proposed	1	low	0	missing
4434 [153]	The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)	proposed	1	low	0	missing
4543 [154]	The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH	proposed	1	low	0	missing
5903 [155]	Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2	info	1	low	0	missing
4754 [156]	IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)	proposed	1	low	0	missing
4868 [157]	Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	proposed	1	low	0	missing
6379 [127]	Suite B Cryptographic Suites for IPsec	info	0	missing	0	missing
4894 [158]	Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec	info	1	low	0	missing
5114 [159]	Additional Diffie-Hellman Groups for Use with IETF Standards	info	1	low	0	missing
5282 [160]	Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) protocol	proposed	1	low	0	missing
5930 [161]	Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol	info	1	low	0	missing

A.3. DHCPv6 and Autoconfiguration

Table A4. RFCs on DHCPv6 and autoconfiguration.

RFC	Title	Type	N1	N2	B1	B2
Stateless Autoconfiguration						
4862 [24]	Stateless Address Autoconfiguration	draft	1	medium	1	medium
4941 [162]	Privacy Extensions for Stateless Address Autoconfiguration in IPv6	draft	1	high	1	medium
DHCPv6						
3315 [163]	Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	proposed	1	medium	1	medium
3319 [164]	Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers	proposed	1	low	0	missing
3633 [165]	IPv6 prefix options for DHCPv6	proposed	1	low	0	missing
3646 [166]	DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	proposed	1	low	0	missing
3736 [167]	Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6	proposed	1	low	1	low
3898 [168]	Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	proposed	1	low	0	missing
4075 [169]	Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6	proposed	1	low	0	missing
4361 [170]	Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)	proposed	1	low	0	missing
4477 [171]	Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues	info	1	low	0	missing
4994 [172]	DHCPv6 Relay Agent Echo Request Options	proposed	1	low	0	missing
6221 [173]	Lightweight DHCPv6 Relay Agent	proposed	0	missing	0	missing
6422 [174]	Relay-Supplied DHCP Options	proposed	0	missing	0	missing

A.4. Routing and DNS

Table A5. RFCs on routing and DNS.

RFC	Title	Type	N1	N2	B1	B2
DNS Specification						
3596 [175]	DNS Extensions for IPv6	proposed	1	very high	1	high
6672 [176]	DNAME Redirection in the DNS	proposed	0	missing	0	missing
3363 [177]	Representing IPv6 addresses in DNS	info	0	missing	0	missing
Security issues						
3364 [178]	Tradeoffs in DNS for IPv6	info	0	missing	0	missing
3901 [179]	DNS IPv6 transport operational guidelines	BCP	1	low	0	missing
4074 [180]	Common misbehavior against DNS queries for IPv6 addresses	info	1	medium	0	missing
4472 [181]	Operational Considerations an Issues with IPv6 DNS	info	1	medium	0	missing
4033 [39]	DNS Security Introduction and Requirements	proposed	1	medium	1	low
4034 [40]	Resource Records for the DNS Security Extensions	proposed	1	medium	0	missing
3833 [182]	Threat Analysis of the Domain Name System (DNS)	info	1	medium	0	missing
5358 [183]	Preventing Use of Recursive Nameservers in Reflector Attacks	BCP	1	medium	0	missing
5452 [184]	Measures for Making DNS More Resilient against Forged Answers	proposed	1	low	0	missing
DNSSEC						
4035 [41]	Protocol Modification for the DNS Security Extensions	proposed	1	medium	0	missing
4470 [42]	Minimally Covering NSEC Records and DNSSEC On-line Signing	proposed	0	missing	0	missing
6014 [43]	Cryptographic Algorithm Identifier Allocation for DNSSEC	proposed	0	missing	0	missing
3226 [185]	DNSSEC and IPv6 A6 aware server/resolver message size requirements	proposed	0	missing	0	missing
2845 [38]	Secret Key Transaction Authentication for DNS (TSIG)	proposed	1	medium	0	missing
3645 [186]	Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)	proposed	0	missing	0	missing
4635 [187]	HMAC SHA TSIG Algorithm Identifiers	proposed	1	low	0	missing
2930 [188]	Secret Key Establishment for DNS (TKEY RR)	proposed	1	low	0	missing
2931 [189]	DNS Request and Transaction Signatures (SIG(0)s)	proposed	1	low	0	missing
Multihoming						
3178 [190]	IPv6 Multi-homing support at site with exit routers	info	0	missing	0	missing
4218 [191]	Threats Relating to IPv6 Multihoming Solutions	info	1	low	0	missing
4177 [192]	Architectural Approaches to Multihoming for IPv6	info	1	medium	0	missing
5533 [193]	SHIM6: Level 3 Multihoming Shim Protocol for IPv6	proposed	1	medium	0	missing
5535 [194]	Hash-Based Addresses (HBA)	proposed	1	low	0	missing
5534 [195]	Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming	proposed	1	low	0	missing
3704 [196]	Ingress Filtering for Multihomed Networks	BCP	1	medium	1	low
Routing Protocols						
2080 [197]	RIPng for IPv6	proposed	1	low	1	low
4760 [198]	Multiprotocol Extensions for BGP-4	draft	1	low	1	low
2545 [199]	Use of BGP-4 Multiprotocol Extension for IPv6 Inter-domain routing	proposed	0	missing	1	low
5340 [200]	OSPF for IPv6	proposed	1	medium	1	low
4552 [201]	Authentication/Confidentiality for OSPFv3	proposed	1	low	1	low
PIM						
5294 [202]	Host Threats to Protocol Independent Multicast (PIM)	info	1	low	0	missing
4609 [203]	Protocol Independent Multicast - Sparse Mode (PIM - SM) Multicast Routing Security Issues and Enhancements	info	1	low	0	missing

Table A5. Cont.

RFC	Title	Type	N1	N2	B1	B2
3956 [204]	Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address	proposed	1	low	1	low
4601 [205]	Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	proposed	1	low	1	low
5059 [206]	Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)	proposed	0	missing	0	missing
5796 [207]	Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages	proposed	1	low	0	missing
6227 [208]	PIM Group-to-Rendezvous Point Mapping	proposed	0	missing	0	missing

A.5. Transition Methods

Table A6. RFCs on transition methods.

RFC	Title	Type	N1	N2	B1	B2
Dual Stack						
2529 [49]	Transmission of IPv6 over IPv4 Domains without Explicit Tunnels	proposed	1	high	1	low
4942 [209]	IPv6 Transition/Coexistence Security Considerations	info	1	medium	1	medium
4554 [210]	Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks	info	1	low	0	missing
4852 [211]	IPv6 Enterprise Network Analysis - IP Layer 3 Focus	info	1	medium	0	missing
Tunneling						
4213 [46]	Basic transition mechanisms for IPv6 hosts and routers	proposed	1	medium	1	medium
4891 [212]	Using IPsec to Secure IPv6-in-IPv4 Tunnels	info	1	low	0	missing
2473 [213]	Generic packet tunneling in IPv6 specification	proposed	1	medium	0	missing
4380 [51]	Teredo: tunneling IPv6 over UDP through NATs	proposed	1	high	1	low
5991 [214]	Teredo Security Update	proposed	0	missing	0	missing
6081 [215]	Teredo Extensions	proposed	0	missing	0	missing
3056 [48]	Connection of IPv6 domains via IPv4 clouds	proposed	1	medium	1	low
3964 [216]	Security Considerations for 6to4	info	1	medium	0	missing
4659 [217]	BGP-MPLS IP VPN extension for IPv6 VPN	proposed	0	missing	0	missing
4798 [218]	Connecting IPv6 islands over MPLS	proposed	0	missing	0	missing
3068 [219]	An Anycast Prefix for 6to4 Relay Routers	proposed	1	medium	1	medium
5569 [220]	IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)	info	1	low	1	low
5969 [50]	6rd Protocol Specification	proposed	1	medium	0	missing
5214 [52]	Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)	info	1	high	1	low
3053 [53]	IPv6 Tunnel Broker	info	1	medium	0	missing
5572 [221]	IPv6 Tunnel Broker with the Tunnel Setup Protocol (TSP)	EXP	1	medium	0	missing
Translation						
6145 [56]	IP/ICMP Translation Algorithm	proposed	0	missing	0	missing
2766 [57]	NAT-PT	info	1	medium	1	medium
4966 [58]	Reasons to Move the Network Address Translation - Protocol Translator (NAT-PT) to Historic Status	info	1	medium	1	low
6052 [45]	IPv6 Addressing of IPv4/IPv6 Translators	proposed	1	low	0	missing
6144 [222]	Framework for IPv4/IPv6 Translation	info	0	missing	0	missing
2767 [223]	Dual stack hosts using Bump in Stack techniques (BIS)	info	1	low	0	missing
6535 [224]	Dual-Stack Hosts Using "Bump-in-the-Host" (BIH)	proposed	0	missing	0	missing
3142 [59]	IPv6 to IPv4 transport relay translator (TRT)	info	1	medium	0	missing
5389 [225]	Session Traversal Utilities for NAT (STUN)	proposed	1	low	0	missing
3089 [226]	A SOCKS-based IPv6/IPv4 Gateway Mechanism	info	1	low	0	missing
2694 [227]	DNS extensions to Network Address Translators (DNS_ALG)	info	1	low	0	missing

Table A6. *Cont.*

RFC	Title	Type	N1	N2	B1	B2
6146 [228]	Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers	proposed	0	missing	1	low
6147 [229]	ENS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers	proposed	0	missing	0	missing

A.6. Other RFCs Relevant for IPv6

The following RFCs could not be fit into any of the other categories. They were not taken into account for the evaluation of the secure deployment guides. Nevertheless, they are listed here for completeness.

Table A7. Other RFCs relevant for IPv6.

RFC	Title	Type	N1	N2	B1	B2
5211 [230]	Internet Transition Plan	info	1	medium	0	missing
4864 [231]	Local network protection for IPv6	info	0	missing	0	missing
5157 [232]	IPv6 Implications for Network Scanning	info	1	medium	0	missing
6434 [233]	IPv6 node requirements	info	0	missing	1	low
6177 [234]	IPv6 Address Assignment to End Sites	BCP	1	low	0	missing
2072 [235]	Router Renumbering Guide	info	1	low	0	missing
4057 [236]	IPv6 Enterprise Network Scenarios	info	1	high	0	missing
5082 [237]	The Generalized TTL Security Mechanism (GTSM)	proposed	1	medium	0	missing
4192 [238]	Procedures for Renumbering an IPv6 Network	info	1	high	0	missing
4311 [239]	Host to router load sharing	proposed	1	low	0	missing
2894 [240]	Router renumbering for IPv6	proposed	1	low	0	missing
5798 [241]	VRRPv4 for IPv4 and IPv6	proposed	0	missing	1	medium
2464 [242]	IPv6 over Ethernet	proposed	0	missing	0	missing
2590 [243]	IPv6 over FR	proposed	0	missing	0	missing
5072 [244]	IPv6 over PPP	draft	0	missing	0	missing
5172 [245]	Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol	proposed	0	missing	0	missing
3111 [246]	SLP modifications for IPv6	proposed	0	missing	0	missing
2428 [247]	FTP extensions for IPv6 and NATs	proposed	0	missing	0	missing
4293 [248]	MIB for IP	proposed	0	missing	1	low
4292 [249]	IP Forwarding Table MIB	proposed	0	missing	0	missing
4022 [250]	MIB for TCP	proposed	0	missing	0	missing
4113 [251]	MIB for UDP	proposed	0	missing	0	missing
4807 [252]	IPsec Security Policy Database Configuration MIB	proposed	1	low	0	missing
5519 [253]	Multicast Group Membership Discovery MIB	proposed	0	missing	0	missing
4001 [254]	Textual conventions for Internet network addresses	proposed	0	missing	0	missing

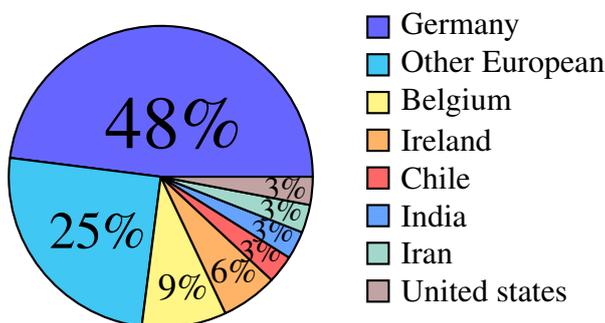
B. About the Survey Participants

In order to achieve useful results with the survey, high-quality input by expert practitioners was necessary who knew about IPv6 and have possibly implemented it as well. Therefore, the Web was searched for expert forums and blogs, and four sources were identified. Two of the sources were expert groups with restricted access in social networks for professionals (Xing and LinkedIn). Another source was an IPv6 group on Facebook, with restricted access as well. The last source was the IPv6 forum of Hurricane Electric, a large ISP in the USA. The survey results show that of the valid participants, *i.e.*, participants who answered at least all comparison questions of the survey, and not only with default

values; six people came from LinkedIn, eight from Facebook and the other 20 either from Xing or the Hurricane Electric forum.

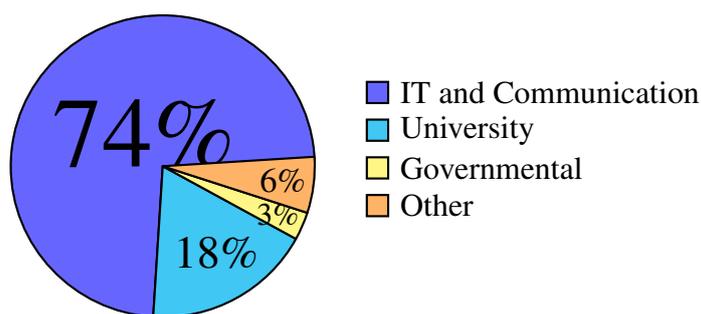
Participants of the survey have also been asked to give background information. These questions were about the country of origin, the industry they work in, their job role and department. Most participants of the survey came from Germany (48%). The rest was spread over several countries. There were three participants from Belgium and two from Ireland. It is worth mentioning that only five of the 34 valid participants came from outside of Europe. Figure A1 shows a graphical representation of the origins of the participants.

Figure A1. Origin of participants (n = 34).



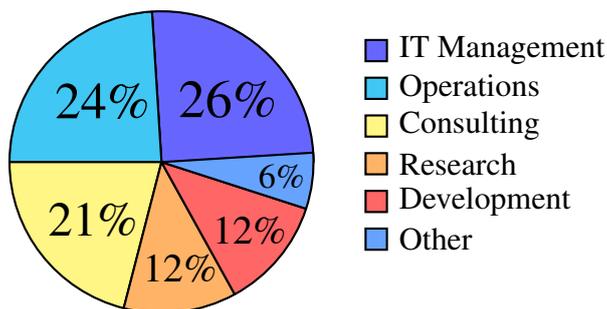
Participants were also asked to give information about the industry they work in. The choices given were university, government, IT and communication industry, or other (Figure A2). The clear majority of the participants came from the IT and communication industry (25 of 34). One of the participants came from a governmental organization and six from a university, while two did not belong to any of the three.

Figure A2. Industries of participants (n = 34).



Another question regarding background information of the participants was for the department that they were working for (Figure A3). Six choices were given: development, research, consulting, operations, IT management and other. Due to the industry most participants work in, it was not surprising to find that most participants came from consulting (7), operations (8) and IT management (9). Four participants each work in development and research departments, while two did not fit into any of the given choices.

Figure A3. Work departments of participants (n = 34).



In question four the participants were asked to provide information about their job role. This was an open question, so every participant could write down their own answer, which were mapped to the following categories: Network/System Architect, Management/CEO, Student/Trainee, Consultant, Security Engineer, Other (Figure A4). Surprisingly many CEO’s and managers (9) took part in the survey. This might indicate high interest of decision makers on the topic. Another well represented group was the group of network and system architects (9) as well as security engineers.

Figure A4. Job roles of participants (n = 34).

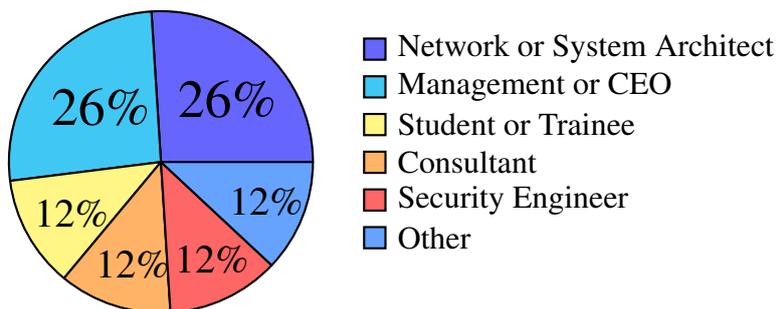
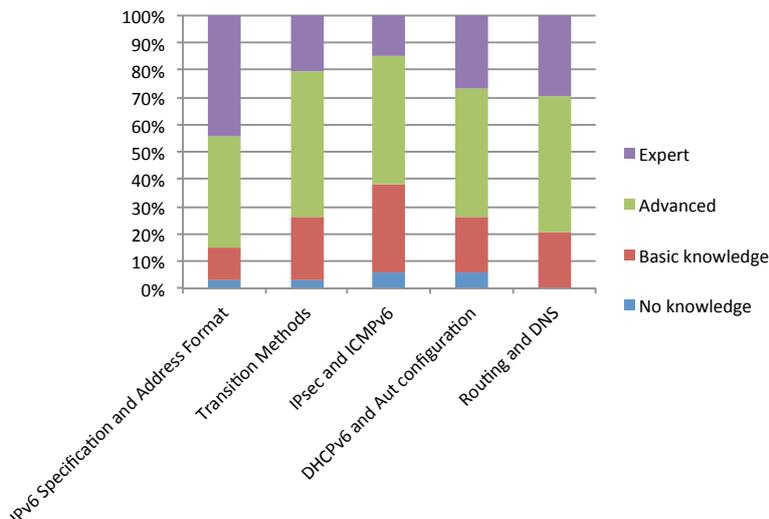


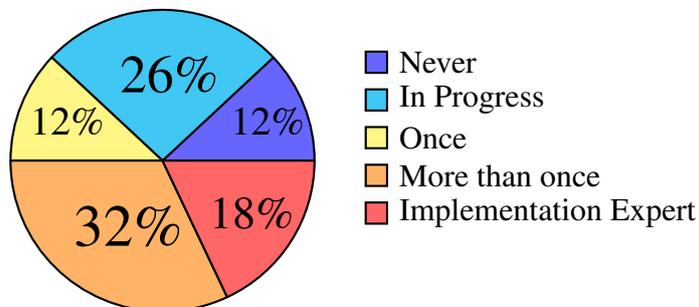
Figure A5 shows the results of a self-assessment on IPv6 knowledge in the five categories shown at the bottom. There are only few people who had no knowledge in one ore more areas. Only one person did not know about the *IPv6 Specification and Address format* and *Transition Methods*. Two did not know much about *IPsec and ICMPv6* and *DHCPv6 and Autoconfiguration*. *Routing and DNS* is the only category where everybody had at least basic knowledge. More than 60% have at least advanced experience in all five categories, with *IPsec and ICMPv6* having the least and *IPv6 Specification and Adressformat* having the most experts.

Figure A5. IPv6 knowledge.



The last background question of the survey was about experience with the implementation of IPv6. Figure A6 shows the results. 12% never implemented IPv6, while 26% of the participants are in progress of deployment, and another 12% did it once. 50% have implemented IPv6 more than once and 18% of these even consider themselves as implementation experts.

Figure A6. How often have you implemented IPv6? (n = 34).



References

1. Deering, S.; Hinden, R. *Internet Protocol, Version 6 (IPv6) Specification*; RFC 1883; IETF: Fremont, CA, USA, 1995.
2. IANA. Internet Protocol Version 6 Address Space, 2012. Available online: <http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml> (accessed on 7 January 2014).
3. Frankel, S.; Graveman, R.; Pearce, J.; Rooks, M. *Guidelines for the Secure Deployment of IPv6—Recommendations of the National Institute of Standards and Technology*; Technical Report; NIST: Gaithersburg, MD, USA, 2010.
4. Hagen, S. *IPv6 Essentials*; Essentials Series; O’Reilly Media: Cambridge, MA, USA, 2006.
5. Hagen, S. *IPv6: Grundlagen, Funktionalität, Integration*; Sunny Connection AG: Maur, Switzerland, 2009.
6. Loshin, P. *IPv6, Theory, Protocol and Practice*; Elsevier: San Francisco, CA, USA, 2004.
7. Soliman, H. *Mobile IPv6*; Addison-Wesley, Pearson Education: Boston, MA, USA, 2004.

8. Radhakrishnan, R.; Jamil, M.; Mehfuz, S.; Moinuddin. Security Issues in IPv6. In Proceedings of the Third International Conference on Networking and Services (INCS 2007), Athens, Greece, 19–25 June 2007; p. 110.
9. Žagar, D.; Grgić, K.; Rimac-Drlje, S. Security aspects in IPv6 networks—Implementation and testing. *Comput. Electr. Eng.* **2007**, *33*, 425–437.
10. Caicedo, C.; Joshi, J.; Tuladhar, S. IPv6 security challenges. *Computer* **2009**, *42*, 36–42.
11. Turiel, A. IPv6: New technology, new threats. *Netw. Secur.* **2011**, *2011*, 13–15.
12. Gold, S. IPv6 migration and security. *Netw. Secur.* **2011**, *2011*, 15–18.
13. Van Heerden, R.; Bester, I.; Burke, I. A Review of IPv6 Security Concerns. In Proceedings of the Fourth Workshop on ICT Uses in Warfare and the Safeguarding of Peace (IWSP'12), Johannesburg, South Africa, 16 August 2012.
14. Barker, K. The security implications of IPv6. *Netw. Secur.* **2013**, *2013*, 5–9.
15. Hogg, S.; Vyncke, E. *IPv6 Security*; Cisco Press: Indianapolis, IN, USA, 2009.
16. Minoli, D.; Kouns, J. *Security in an IPv6 Environment*; Taylor & Francis: Boca Raton, FL, USA, 2009.
17. Hamdy, S. *IPv6 Secorvo White Paper*; Technical Report; Secorvo: Karlsruhe, Germany, 2013.
18. Durdagi, E.; Buldu, A. IPV4/IPV6 security and threat comparisons. *Procedia Soc. Behav. Sci.* **2010**, *2*, 5285–5291.
19. Rostanski, M.; Mushynskyy, T. Security Issues of IPv6 Network Autoconfiguration. In Proceedings of the 12th International Conference on Computer Information Systems and Industrial Management Applications (CISIM 2013), Krakow, Poland, 25–27 September 2013; Springer: Heidelberg, Germany, 2013; pp. 218–228.
20. Modares, H.; Moravejosharieh, A.; Lloret, J.; Salleh, R. A survey of secure protocols in mobile IPv6. *J. Netw. Comput. Appl.* **2013**, in press.
21. Dunlop, M.; Groat, S.; Urbanski, W.; Marchany, R.; Tront, J. The blind man's bluff approach to security using IPv6. *IEEE Secur. Priv.* **2012**, *10*, 35–43.
22. Syed, A.R.; Gillela, K.; Kumar, P.P.; Venugopal, C. Outline of IPv6 topology and best-practice security rules. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 1106–1111.
23. Deering, S.; Hinden, R. *Internet Protocol, Version 6 (IPv6) Specification*; RFC 2460; IETF: Fremont, CA, USA, 1998.
24. Thomson, S.; Narten, T.; Jinmei, T. *IPv6 Stateless Address Autoconfiguration*; RFC 4862; IETF: Fremont, CA, USA, 2007.
25. Claffy, K. Tracking IPv6 evolution: Data we have and data we need. *SIGCOMM Comput. Commun. Rev.* **2011**, *41*, 43–48.
26. Dell, P. Two economic perspectives on the IPv6 transition. *Info* **2010**, *12*, 3–14.
27. Srisuresh, P.; Egevang, K. *Traditional IP Network Address Translator (Traditional NAT)*; RFC 3022; IETF: Fremont, CA, USA, 2001.
28. Kent, S.; Seo, K. *Security Architecture for the Internet Protocol*; RFC 4301; IETF: Fremont, CA, USA, 2005.
29. Botterman, M. *IPv6 Deployment Survey*; Technical Report; GNKS Consult: Rotterdam, The Netherlands, 2011.

30. RIPE. Last/8 Phases. Available online: <http://www.ripe.net/internet-coordination/ipv4-exhaustion/last-8-phases> (accessed on 7 January 2014).
31. Internet Society. IPv6 Launch. Available online: <http://www.worldipv6launch.org/measurements/> (accessed on 7 January 2014).
32. NRO. IPv6 Deployment Survey. Available online: http://www.nro.net/wp-content/uploads/ipv6_deployment_survey.pdf (accessed on 7 January 2014).
33. Bais, E.; Palet, J. *Removal of Multihomed Requirement for IPv6 PI*; Technical Report; RIPE NCC: Amsterdam, The Netherlands, 2011.
34. Conta, A.; Deering, S.; Gupta, M. *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*; RFC 4443; IETF: Fremont, CA, USA, 2006.
35. Narten, T.; Nordmark, E.; Simpson, W.; Soliman, H. *Neighbor Discovery for IP Version 6 (IPv6)*; RFC 4861; IETF: Fremont, CA, USA, 2007.
36. Hinden, R.; Deering, S. *IP Version 6 Addressing Architecture*; RFC 4291; IETF: Fremont, CA, USA, 2006.
37. McCann, J.; Deering, S.; Mogul, J. *Path MTU Discovery for IP Version 6*; RFC 1981; IETF: Fremont, CA, USA, 1996.
38. Gudmundsson, O.; Eastlake, D., 3rd.; Wellington, B. *Secret Key Transaction Authentication for DNS (TSIG)*; RFC 2845; IETF: Fremont, CA, USA, 2000.
39. Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S. *DNS Security Introduction and Requirements*; RFC 4033; IETF: Fremont, CA, USA, 2005.
40. Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S. *Resource Records for the DNS Security Extensions*; RFC 4034; IETF: Fremont, CA, USA, 2005.
41. Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S. *Protocol Modifications for the DNS Security Extensions*; RFC 4035; IETF: Fremont, CA, USA, 2005.
42. Weiler, S.; Ihren, J. *Minimally Covering NSEC Records and DNSSEC On-Line Signing*; RFC 4470; IETF: Fremont, CA, USA, 2006.
43. Hoffman, P. *Cryptographic Algorithm Identifier Allocation for DNSSEC*; RFC 6014; IETF: Fremont, CA, USA, 2010.
44. Hong, Y.G.; Hagino, J.; Savola, P.; Castro, E.M. *Application Aspects of IPv6 Transition*; RFC 4038; IETF: Fremont, CA, USA, 2005.
45. Bao, C.; Huitema, C.; Bagnulo, M.; Boucadair, M.; Li, X. *IPv6 Addressing of IPv4/IPv6 Translators*; RFC 6052; IETF: Fremont, CA, USA, 2010.
46. Nordmark, E.; Gilligan, R. *Basic Transition Mechanisms for IPv6 Hosts and Routers*; RFC 4213; IETF: Fremont, CA, USA, 2005.
47. BSI. *Sichere Anbindung von Lokalen Netzen an das Internet*; Technical Report; Bundesamt für Sicherheit in der Informationstechnik: Bonn, Germany, 2007.
48. Carpenter, B.; Moore, K. *Connection of IPv6 Domains via IPv4 Clouds*; RFC 3056; IETF: Fremont, CA, USA, 2001.
49. Carpenter, B.; Jung, C. *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*; RFC 2529; IETF: Fremont, CA, USA, 1999.

50. Townsley, W.; Troan, O. *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)—Protocol Specification*; RFC 5969; IETF: Fremont, CA, USA, 2010.
51. Huitema, C. *Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)*; RFC 4380; IETF: Fremont, CA, USA, 2006.
52. Templin, F.; Gleeson, T.; Thaler, D. *Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)*; RFC 5214; IETF: Fremont, CA, USA, 2008.
53. Durand, A.; Fasano, P.; Lento, D. *IPv6 Tunnel Broker*; RFC 3053; IETF: Fremont, CA, USA, 2001.
54. Xia, H. Evaluating DSTM—An IPv6 Transition Mechanism for IPv6 Dominant Networks. Available online: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.110.2552> (accessed on 12 December 2013).
55. AlJa'afreh, R.; Mellor, J.; Kamala, M.; Kasasbeh, B. Bi-directional Mapping System as a New IPv4/IPv6 Translation Mechanism. In Proceedings of the Tenth International Conference on Computer Modeling and Simulation (UKSIM '08), Cambridge, UK, 1–3 April 2008; IEEE Computer Society: Los Alamitos, CA, USA, 2008, pp. 40–45.
56. Li, X.; Bao, C.; Baker, F. *IP/ICMP Translation Algorithm*; RFC 6145; IETF: Fremont, CA, USA, 2011.
57. Tsirtsis, G.; Srisuresh, P. *Network Address Translation—Protocol Translation (NAT-PT)*; RFC 2766; IETF: Fremont, CA, USA, 2000.
58. Aoun, C.; Davies, E. *Reasons to Move the Network Address Translator—Protocol Translator (NAT-PT) to Historic Status*; RFC 4966; IETF: Fremont, CA, USA, 2007.
59. Hagino, J.; Yamamoto, K. *An IPv6-to-IPv4 Transport Relay Translator*; RFC 3142; IETF: Fremont, CA, USA, 2001.
60. Saaty, T.L. Decision making with the analytic hierarchy process. *Int. J. Serv. Sci.* **2008**, *1*, 83–98.
61. Davies, E.; Mohacsi, J. *Recommendations for Filtering ICMPv6 Messages in Firewalls*; RFC 4890; IETF: Fremont, CA, USA, 2007.
62. Common Vulnerabilities and Exposures (CVE). Available online: <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=IPv6> (accessed on 7th January 2014).
63. NIST. About NIST, 2013. Available online: http://www.nist.gov/public_affairs/nandyou.cfm (accessed on 7 January 2014).
64. NIST. Computer Security Division, 2013. Available online: <http://www.nist.gov/itl/csd/index.cfm> (accessed on 7 January 2014).
65. BSI. *Sichere Anbindung von Lokalen Netzen an das Internet (Isi-LANA) v.2.0*; Technical Report; Bundesamt für Sicherheit in der Informationstechnik: Bonn, Germany, 2012.
66. Zetter, K. How a Crypto “Backdoor” Pitted the Tech World Against the NSA. *Wired Threat Level*, 2013. Available online: <http://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/> (accessed on 7 January 2014).
67. Van de Vlede, G.; Popoviciu, C.; Chown, T.; Bonness, O.; Hahn, C. *IPv6 Unicast Address Assignment Considerations*; RFC 5375; IETF: Fremont, CA, USA, 2008.
68. Kawamura, S.; Kawashima, M. *A Recommendation for IPv6 Address Text Representation*; RFC 5952; IETF: Fremont, CA, USA, 2010.

69. Hinden, R.; Deering, S.; Nordmark, E. *IPv6 Global Unicast Address Format*; RFC 3587; IETF: Fremont, CA, USA, 2003.
70. Johnson, D.; Deering, S. *Reserved IPv6 Subnet Anycast Addresses*; RFC 2526; IETF: Fremont, CA, USA, 1999.
71. Huitema, C.; Carpenter, B. *Deprecating Site Local Addresses*; RFC 3879; IETF: Fremont, CA, USA, 2004.
72. Hinden, R.; Haberman, B. *Unique Local IPv6 Unicast Addresses*; RFC 4193; IETF: Fremont, CA, USA, 2005.
73. Huston, G.; Lord, A.; Smith, P. *IPv6 Address Prefix Reserved for Documentation*; RFC 3849; IETF: Fremont, CA, USA, 2004.
74. Hinden, R.; Deering, S. *IPv6 Multicast Address Assignment*; RFC 2375; IETF: Fremont, CA, USA, 1998.
75. Blanchet, M. *Special-Use IPv6 Addresses*; RFC 5156; IETF: Fremont, CA, USA, 2008.
76. Deering, S.; Haberman, B.; Jinmei, T.; Nordmark, E.; Zill, B. *IPv6 Scoped Address Architecture*; RFC 4007; IETF: Fremont, CA, USA, 2005.
77. Thaler, D.; Draves, R.; Matsumoto, A.; Chown, T. *Default Address Selection for Internet Protocol Version 6 (IPv6)*; RFC 6724; IETF: Fremont, CA, USA, 2012.
78. Blanchet, M. *A Flexible Method for Managing the Assignment of Bits of an IPv6 Address Block*; RFC 3531; IETF: Fremont, CA, USA, 2003.
79. Aura, T. *Cryptographically Generated Addresses (CGA)*; RFC 3972; IETF: Fremont, CA, USA, 2005.
80. Borman, D.; Deering, S.; Hinden, R. *IPv6 Jumbograms*; RFC 2675; IETF: Fremont, CA, USA, 1999.
81. Partridge, C.; Jackson, A. *IPv6 Router Alert Option*; RFC 2711; IETF: Fremont, CA, USA, 1999.
82. Le Faucheur, F. *IP Router Alert Considerations and Usage*; RFC 6398; IETF: Fremont, CA, USA, 2011.
83. Abley, J.; Savola, P.; Neville-Neil, G. *Deprecation of Type 0 Routing Headers in IPv6*; RFC 5095; IETF: Fremont, CA, USA, 2007.
84. Nichols, K.; Blake, S.; Baker, F.; Black, D. *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*; RFC 2474; IETF: Fremont, CA, USA, 1998.
85. Partridge, C. *Using the Flow Label Field in IPv6*; RFC 1809; IETF: Fremont, CA, USA, 1995.
86. Amante, S.; Carpenter, B.; Jiang, S.; Rajahalme, J. *IPv6 Flow Label Specification*; RFC 6437; IETF: Fremont, CA, USA, 2011.
87. Krishnan, S.; Woodyatt, J.; Kline, E.; Hoagland, J.; Bhatia, M. *A Uniform Format for IPv6 Extension Headers*; RFC 6564; IETF: Fremont, CA, USA, 2012.
88. Krishnan, S. *Handling of Overlapping IPv6 Fragments*; RFC 5722; IETF: Fremont, CA, USA, 2009.
89. Park, J.S.; Shin, M.K.; Kim, H.J. *A Method for Generating Link-Scoped IPv6 Multicast Addresses*; RFC 4489; IETF: Fremont, CA, USA, 2006.
90. Haberman, B.; Thaler, D. *Unicast-Prefix-Based IPv6 Multicast Addresses*; RFC 3306; IETF: Fremont, CA, USA, 2002.

91. Kent, S. *IP Authentication Header*; RFC 4302; IETF: Fremont, CA, USA, 2005.
92. Kent, S. *IP Encapsulating Security Payload (ESP)*; RFC 4303; IETF: Fremont, CA, USA, 2005.
93. Perkins, C.; Johnson, D.; Arkko, J. *Mobility Support in IPv6*; RFC 6275; IETF: Fremont, CA, USA, 2011.
94. Patel, A.; Leung, K.; Khalil, M.; Akhtar, H.; Chowdhury, K. *Mobile Node Identifier Option for Mobile IPv6 (MIPv6)*; RFC 4283; IETF: Fremont, CA, USA, 2005.
95. Arkko, J.; Vogt, C.; Haddad, W. *Enhanced Route Optimization for Mobile IPv6*; RFC 4866; IETF: Fremont, CA, USA, 2007.
96. Arkko, J.; Devarapalli, V.; Dupont, F. *Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents*; RFC 3776; IETF: Fremont, CA, USA, 2004.
97. Nikander, P.; Arkko, J.; Auro, T.; Montenegro, G.; Nordmark, E. *Mobile IP Version 6 Route Optimization Security Design Background*; RFC 4225; IETF: Fremont, CA, USA, 2005.
98. Patel, A.; Leung, K.; Khalil, M.; Akhtar, H.; Chowdhury, K. *Authentication Protocol for Mobile IPv6*; RFC 4285; IETF: Fremont, CA, USA, 2006.
99. Le, F.; Faccin, S.; Tschofenig, H. *Mobile IPv6 and Firewalls: Problem Statement*; RFC 4487; IETF: Fremont, CA, USA, 2006.
100. Perkins. *Securing Mobile IPv6 Route Optimization Using a Static Shared Key*; RFC 4449; IETF: Fremont, CA, USA, 2006.
101. Koodli, R. *IP Address Location Privacy and Mobile IPv6: Problem Statement*; RFC 4882; IETF: Fremont, CA, USA, 2007.
102. Devarapalli, V.; Dupont, F. *Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture*; RFC 4877; IETF: Fremont, CA, USA, 2007.
103. Patel, A.; Giaretta, G. *Problem Statement for Bootstrapping Mobile IPv6 (MIPv6)*; RFC 4640; IETF: Fremont, CA, USA, 2006.
104. Giaretta, G.; Kempf, J.; Devarapalli, V. *Mobile IPv6 Bootstrapping in Split Scenario*; RFC 5026, 2007.
105. Soliman, H. *Mobile IPv6 Support for Dual Stack Hosts and Routers*; RFC 5555; IETF: Fremont, CA, USA, 2009.
106. Bonica, R.; Gan, D.; Tappan, D.; Pignataro, C. *Extended ICMP to Support Multi-Part Messages*; RFC 4884; IETF: Fremont, CA, USA, 2007.
107. Nikander, P.; Kempf, J.; Nordmark, E. *IPv6 Neighbor Discovery (ND) Trust Models and Threats*; RFC 3756; IETF: Fremont, CA, USA, 2004.
108. Singh, H.; Beebe, W.; Nordmark, E. *IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes*; RFC 5942; IETF: Fremont, CA, USA, 2010.
109. Arkko, J.; Kempf, J.; Zill, B.; Nikander, P. *SEcure Neighbor Discovery (SEND)*; RFC 3971; IETF: Fremont, CA, USA, 2005.
110. Gagliano, R.; Krishnan, S.; Kukec, A. *Certificate Profile and Certificate Management for SEcure Neighbor Discovery (SEND)*; RFC 6494; IETF: Fremont, CA, USA, 2012.
111. Gagliano, R.; Krishnan, S.; Kukec, A. *Subject Key Identifier (SKI) SEcure Neighbor Discovery (SEND) Name Type Fields*; RFC 6495; IETF: Fremont, CA, USA, 2012.

112. Conta, A. *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*; RFC 3122; IETF: Fremont, CA, USA, 2001.
113. Deering, S.; Fenner, W.; Haberman, B. *Multicast Listener Discovery (MLD) for IPv6*; RFC 2710; IETF: Fremont, CA, USA, 1999.
114. Haberman, B. *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*; RFC 3590; IETF: Fremont, CA, USA, 2003.
115. Vida, R.; Costa, L. *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*; RFC 3810; IETF: Fremont, CA, USA, 2004.
116. Holbrook, H.; Cain, B.; Haberman, B. *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*; RFC 4604; IETF: Fremont, CA, USA, 2006.
117. Haberman, B.; Martin, J. *Multicast Router Discovery*; RFC 4286; IETF: Fremont, CA, USA, 2005.
118. Berger, L.; O'Malley, T. *RSVP Extensions for IPSEC Data Flows*; RFC 2207; IETF: Fremont, CA, USA, 1997.
119. Tschofenig, H.; Graveman, R. *RSVP Security Properties*; RFC 4230; IETF: Fremont, CA, USA, 2005.
120. Ramakrishnan, K.; Floyd, S.; Black, D. *The Addition of Explicit Congestion Notification (ECN) to IP*; RFC 3168; IETF: Fremont, CA, USA, 2001.
121. Briscoe, B. *Tunneling of Explicit Congestion Notification*; RFC 6040; IETF: Fremont, CA, USA, 2010.
122. Kent, S. *Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)*; RFC 4304; IETF: Fremont, CA, USA, 2005.
123. Manral, V. *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*; RFC 4835; IETF: Fremont, CA, USA, 2007.
124. Schiller, J. *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*; RFC 4307; IETF: Fremont, CA, USA, 2005.
125. Hoffman, P. *Cryptographic Suites for IPsec*; RFC 4308; IETF: Fremont, CA, USA, 2005.
126. Bellovin, S. *Guidelines for Specifying the Use of IPsec Version 2*; RFC 5406; IETF: Fremont, CA, USA, 2009.
127. Law, L.; Solinas, J. *Suite B Cryptographic Suites for IPsec*; RFC 6379; IETF: Fremont, CA, USA, 2011.
128. Weis, B.; Gross, G.; Ignjatic, D. *Multicast Extensions to the Security Architecture for the Internet Protocol*; RFC 5374; IETF: Fremont, CA, USA, 2008.
129. Gould, J.; Hollenbeck, S. *Domain Name System (DNS) Security Extensions Mapping for the Extensible Provisioning Protocol (EPP)*; RFC 5910; IETF: Fremont, CA, USA, 2010.
130. Kaufman, C.; Hoffman, P.; Nir, Y.; Eronen, P. *Internet Key Exchange Protocol Version 2 (IKEv2)*; RFC 5996; IETF: Fremont, CA, USA, 2010.
131. Frankel, S.; Krishnan, S. *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap*; RFC 6071; IETF: Fremont, CA, USA, 2011.

132. Eronen, P.; Laganier, J.; Madson, C. *IPv6 Configuration in Internet Key Exchange Protocol Version 2 (IKEv2)*; RFC 5739; IETF: Fremont, CA, USA, 2010.
133. Daevarapalli, V.; Weniger, K. *Redirect Mechanism for the Internet Key Exchange Protocol Version 2 (IKEv2)*; RFC 5685; IETF: Fremont, CA, USA, 2009.
134. Sheffer, Y.; Tschofenig, H. *Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption*; RFC 5723; IETF: Fremont, CA, USA, 2010.
135. Grewal, K.; Montenegro, G.; Bhatia, M. *Wrapped Encapsulating Security Payload (ESP) for Traffic Visibility*; RFC 5840; IETF: Fremont, CA, USA, 2010.
136. Kivinen, T.; McDonald, D. *Heuristics for Detecting ESP-Null Packets*; RFC 5879; IETF: Fremont, CA, USA, 2010.
137. Eronen, P.; Tschofenig, H.; Sheffer, Y. *An Extension for EAP-Only Authentication in IKEv2*; RFC 5998; IETF: Fremont, CA, USA, 2010.
138. Nir, Y. *IPsec Cluster Problem Statement*; RFC 6027; IETF: Fremont, CA, USA, 2010.
139. Nir, Y.; Wierbowski, D.; Detienne, F.; Sethi, P. *A Quick Crash Detection Method for Internet Key Exchange Protocol (IKE)*; RFC 6290; IETF: Fremont, CA, USA, 2011.
140. Singh, R.; Kalyani, G.; Nir, Y.; Sheffer, Y.; Zhang, D. *Protocol Support for High Availability of IKEv2/IPsec*; RFC 6311; IETF: Fremont, CA, USA, 2011.
141. Eronen, P. *IKEv2 Mobility and Multihoming Protocol (MOBIKE)*; RFC 4555; IETF: Fremont, CA, USA, 2006.
142. Kivinen, T.; Tschofenig, H. *Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol*; RFC 4621; IETF: Fremont, CA, USA, 2006.
143. Madson, C.; Glenn, R. *The Use of HMAC-SHA-1-96 within ESP and AH*; RFC 2404; IETF: Fremont, CA, USA, 1998.
144. Glenn, R.; Kent, S. *The NULL Encryption Algorithm and Its Use With IPsec*; RFC 2410; IETF: Fremont, CA, USA, 1998.
145. Pereira, R.; Adams, R. *The ESP CBC-Mode Cipher Algorithms*; RFC 2451; IETF: Fremont, CA, USA, 1998.
146. Kivinen, T.; Kojo, M. *More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)*; RFC 3526; IETF: Fremont, CA, USA, 2003.
147. Frankel, S.; Herbert, H. *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*; RFC 3566; IETF: Fremont, CA, USA, 2003.
148. Frankel, S.; Glenn, R.; Kelly, S. *The AES-CBC Cipher Algorithm and Its Use with IPsec*; RFC 3602; IETF: Fremont, CA, USA, 2003.
149. Housley, R. *Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)*; RFC 3686; IETF: Fremont, CA, USA, 2004.
150. Viega, J.; McGrew, D. *The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)*; RFC 4106; IETF: Fremont, CA, USA, 2005.
151. Housley, R. *Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)*; RFC 4309; IETF: Fremont, CA, USA, 2005.
152. Weis, B. *The Use of RSA/SHA-1 Signatures within Encapsulating Security Payload (ESP) and Authentication Header (AH)*; RFC 4359; IETF: Fremont, CA, USA, 2006.

153. Hoffman, P. *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*; RFC 4434; IETF: Fremont, CA, USA, 2006.
154. McGrew, D.; Viega, J. *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*; RFC 4543; IETF: Fremont, CA, USA, 2006.
155. Fu, D.; Solinas, J. *Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2*; RFC 5903; IETF: Fremont, CA, USA, 2010.
156. Fu, D.; Solinas, J. *IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA)*; RFC 4754; IETF: Fremont, CA, USA, 2007.
157. Kelly, S.; Frankel, S. *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec*; RFC 4868; IETF: Fremont, CA, USA, 2007.
158. Hoffman, P. *Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec*; RFC 4894; IETF: Fremont, CA, USA, 2007.
159. Lepinski, M. *Additional Diffie-Hellman Groups for Use with IETF Standards*; RFC 5114; IETF: Fremont, CA, USA, 2008.
160. Black, D.; McGrew, D. *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*; RFC 5282; IETF: Fremont, CA, USA, 2008.
161. Shen, S.; Mao, Y.; Murthy, N. *Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange Version 02 (IKEv2) Protocol*; RFC 5930; IETF: Fremont, CA, USA, 2010.
162. Narten, T.; Draves, R.; Krishnan, S. *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*; RFC 4941; IETF: Fremont, CA, USA, 2007.
163. Droms, R.; Bound, J.; Volz, B.; Lemon, T.; Perkins, C.; Carney, M. *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*; RFC 3315; IETF: Fremont, CA, USA, 2003.
164. Schulzrinne, H.; Volz, B. *Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers*; RFC 3319; IETF: Fremont, CA, USA, 2003.
165. Troan, O.; Droms, R. *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) Version 6*; RFC 3633; IETF: Fremont, CA, USA, 2003.
166. Droms, R. *DNS Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*; RFC 3646; IETF: Fremont, CA, USA, 2003.
167. Droms, R. *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*; RFC 3736; IETF: Fremont, CA, USA, 2004.
168. Klusivalingam, V. *Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*; RFC 3898; IETF: Fremont, CA, USA, 2004.
169. Kalusivalingam, V. *Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6*; RFC 4075; IETF: Fremont, CA, USA, 2005.
170. Lemon, T.; Sommerfield, B. *Node-specific Client Identifiers for Dynamic Host Configuration Protocol Version Four (DHCPv4)*; RFC 4361; IETF: Fremont, CA, USA, 2006.
171. Chown, T.; Venaas, S.; Strauf, C. *Dynamic Host Configuration Protocol (DHCP): IPv4 and IPv6 Dual-Stack Issues*; RFC 4477; IETF: Fremont, CA, USA, 2006.

172. Zeng, S.; Volz, B.; Kinnear, K.; Brzozowski, J. *DHCPv6 Relay Agent Echo Request Option*; RFC 4994; IETF: Fremont, CA, USA, 2007.
173. Miles, D.; Ooghe, S.; Dec, W.; Krishnan, S.; Kavanagh, A. *Lightweight DHCPv6 Relay Agent*; RFC 6221; IETF: Fremont, CA, USA, 2011.
174. Lemon, T.; Wu, Q. *Relay-Supplied DHCP Options*; RFC 6422; IETF: Fremont, CA, USA, 2011.
175. Thomson, S.; Huitema, C.; Ksinant, V.; Souissi, M. *DNS Extensions to Support IP Version 6*; RFC 3596; IETF: Fremont, CA, USA, 2003.
176. Rose, S.; Wijngaards, W. *DNAME Redirection in the DNS*; RFC 6672; IETF: Fremont, CA, USA, 2012.
177. Bush, R.; Durand, A.; Fink, B.; Hain, T.; Gudmundsson, O. *Representing Internet Protocol Version 6 (IPv6) Addresses in the Domain Name System (DNS)*; RFC 3363; IETF: Fremont, CA, USA, 2002.
178. Austein, R. *Tradeoffs in Domain Name System (DNS) Support for Internet Protocol Version 6 (IPv6)*; RFC 3364; IETF: Fremont, CA, USA, 2002.
179. Durand, A.; Ihren, J. *DNS IPv6 Transport Operational Guidelines*; RFC 3901; IETF: Fremont, CA, USA, 2004.
180. Morishita, Y.; Jinmei, T. *Common Misbehavior Against DNS Queries for IPv6 Addresses*; RFC 4074; IETF: Fremont, CA, USA, 2005.
181. Durand, A.; Ihren, J.; Savola, P. *Operational Considerations and Issues with IPv6 DNS*; RFC 4472; IETF: Fremont, CA, USA, 2006.
182. Atkins, D.; Austein, R. *Threat Analysis of the Domain Name System (DNS)*; RFC 3833; IETF: Fremont, CA, USA, 2004.
183. Damas, J.; Neves, F. *Preventing Use of Recursive Nameservers in Reflector Attacks*; RFC 5358; IETF: Fremont, CA, USA, 2008.
184. Hubert, A.; van Mook, R. *Measures for Making DNS More Resilient against Forged Answers*; RFC 5452; IETF: Fremont, CA, USA, 2009.
185. Gudmundsson, O. *DNSSEC and IPv6 A6 Aware Server/Resolver Message Size Requirements*; RFC 3226; IETF: Fremont, CA, USA, 2001.
186. Kwan, S.; Garg, P.; Gilroy, J.; Esibov, L.; Westhead, J.; Hall, R. *Generic Security Service Algorithm for Secret Key Transaction Authentication for DNS (GSS-TSIG)*; RFC 3645; IETF: Fremont, CA, USA, 2003.
187. Eastlake, D., 3rd. *HMAC SHA TSIG Algorithm Identifiers*; RFC 4635; IETF: Fremont, CA, USA, 2006.
188. Eastlake, D., 3rd. *Secret Key Establishment for DNS (TKEY RR)*; RFC 2930; IETF: Fremont, CA, USA, 2000.
189. Eastlake, D., 3rd. *DNS Request and Transaction Signatures (SIG(0)s)*; RFC 2931; IETF: Fremont, CA, USA, 2000.
190. Hagino, J.; Snyder, H. *IPv6 Multihoming Support at Site Exit Routers*; RFC 3178; IETF: Fremont, CA, USA, 2001.
191. Nordmark, E. *Threats Relating to IPv6 Multihoming Solutions*; RFC 4218; IETF: Fremont, CA, USA, 2005.

192. Huston, G. *Architectural Approaches to Multi-homing for IPv6*; RFC 4177; IETF: Fremont, CA, USA, 2005.
193. Nordmark, E.; Bagnulo, M. *Shim6: Level 3 Multihoming Shim Protocol for IPv6*; RFC 5533; IETF: Fremont, CA, USA, 2009.
194. Bagnulo, M. *Hash-Based Addresses (HBA)*; RFC 5535; IETF: Fremont, CA, USA, 2009.
195. Arkko, J.; van Beijnum, I. *Failure Detection and Locator Pair Exploration Protocol for IPv6 Multihoming*; RFC 5534; IETF: Fremont, CA, USA, 2009.
196. Baker, F.; Savola, P. *Ingress Filtering for Multihomed Networks*; RFC 3704; IETF: Fremont, CA, USA, 2004.
197. Malkin, G.; Minnear, R. *RIPng for IPv6*; RFC 2080; IETF: Fremont, CA, USA, 1997.
198. Bates, T.; Chandra, R.; Katz, D.; Rekhter, Y. *Multiprotocol Extensions for BGP-4*; RFC 4760; IETF: Fremont, CA, USA, 2007.
199. Marques, P.; Dupont, F. *Use BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*; RFC 2545; IETF: Fremont, CA, USA, 1999.
200. Coltun, R.; Ferguson, D.; Moy, J.; Lindem, A. *OSPF for IPv6*; RFC 5340; IETF: Fremont, CA, USA, 2008.
201. Gupta, M.; Melam, N. *Authentication/Confidentiality for OSPFv3*; RFC 4552; IETF: Fremont, CA, USA, 2006.
202. Savola, P.; Lingard, J. *Host Threats to Protocol Independent Multicast (PIM)*; RFC 5294; IETF: Fremont, CA, USA, 2008.
203. Savola, P.; Lehtonen, R.; Meyer, D. *Protocol Independent Multicast—Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements*; RFC 4609; IETF: Fremont, CA, USA, 2006.
204. Savola, P.; Haberman, B. *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*; RFC 3956; IETF: Fremont, CA, USA, 2004.
205. Fenner, B.; Handley, M.; Holbrook, H.; Kouvelas, I. *Protocol Independent Multicast—Sparse Mode (PIM-SM): Protocol Specification (Revised)*; RFC 4601; IETF: Fremont, CA, USA, 2006.
206. Bhaskar, N.; Gall, A.; Lingard, J.; Venaas, S. *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*; RFC 5059; IETF: Fremont, CA, USA, 2008.
207. Atwood, W.; Islam, S.; Siami, M. *Authentication and Confidentiality in Protocol Independent Multicast Sparse Mode (PIM-SM) Link-Local Messages*; RFC 5796; IETF: Fremont, CA, USA, 2010.
208. Li, T. *Design Goals for Scalable Internet Routing*; RFC 6227; IETF: Fremont, CA, USA, 2011.
209. Davies, E.; Krishnan, S.; Savola, P. *IPv6 Transition/Coexistence Security Considerations*; RFC 4942; IETF: Fremont, CA, USA, 2007.
210. Chown, T. *Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks*; RFC 4554; IETF: Fremont, CA, USA, 2006.
211. Bound, J.; Pouffary, Y.; Klynsma, S.; Chown, T.; Green, D. *IPv6 Enterprise Network Analysis—IP Layer 3 Focus*; RFC 4852; IETF: Fremont, CA, USA, 2007.
212. Parthasarathy, M.; Savola, P.; Tschofenig, H. *Using IPsec to Secure IPv6-in-IPv4 Tunnels*; RFC 4891; IETF: Fremont, CA, USA, 2007.

213. Conta, A.; Deering, S. *Generic Packet Tunneling in IPv6 Specification*; RFC 2473; IETF: Fremont, CA, USA, 1998.
214. Thaler, D.; Krishnan, S.; Hoagland, J. *Teredo Security Updates*; RFC 5991; IETF: Fremont, CA, USA, 2010.
215. Thaler, D. *Teredo Extensions*; RFC 6081; IETF: Fremont, CA, USA, 2011.
216. Savola, P.; Patel, C. *Security Considerations for 6to4*; RFC 3964; IETF: Fremont, CA, USA, 2004.
217. De Clercq, J.; Ooms, D.; Carugi, M.; le Faucheur, F. *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*; RFC 4659; IETF: Fremont, CA, USA, 2006.
218. De Clercq, J.; Ooms, D.; Prevost, S.; le Faucheur, F. *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*; RFC 4798; IETF: Fremont, CA, USA, 2007.
219. Huitema, C. *An Anycast Prefix for 6to4 Relay Routers*; RFC 3068; IETF: Fremont, CA, USA, 2001.
220. Despres, R. *IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)*; RFC 5569; IETF: Fremont, CA, USA, 2010.
221. Blanchet, M.; Parent, F. *IPv6 Tunnel Broker with Tunnel Setup Protocol (TSP)*; RFC 5572; IETF: Fremont, CA, USA, 2010.
222. Baker, F.; LI, X.; Bao, C.; Yin, K. *Framework for IPv4/IPv6 Translation*; RFC 6144; IETF: Fremont, CA, USA, 2011.
223. Tsuchiya, K.; Higuchi, H.; Atarashi, Y. *Dual Stack Hosts using the “Bump-In-the-Stack” Technique (BIS)*; RFC 2767; IETF: Fremont, CA, USA, 2000.
224. Huang, B.; Deng, H.; Savolainen, T. *Dual-Stack Hosts Using “Bump-in-the-Host” (BIH)*; RFC 6535; IETF: Fremont, CA, USA, 2012.
225. Rosenberg, J.; Mahy, R.; Matthews, P.; Wing, D. *Session Traversal Utilities for NAT (STUN)*; RFC 5389; IETF: Fremont, CA, USA, 2008.
226. Kitamura, H. *A SOCKS-based IPv6/IPv4 Gateway Mechanism*; RFC 3089; IETF: Fremont, CA, USA, 2001.
227. Srisuresh, P.; Tsirtsis, G.; Akkiraju, P.; Heffernan, A. *DNS Extensions to Network Address Translators (DNS_ALG)*; RFC 2694; IETF: Fremont, CA, USA, 1999.
228. Bagnulo, M.; Matthews, P.; von Beijnum, I. *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*; RFC 6146; IETF: Fremont, CA, USA, 2011.
229. Bagnulo, M.; Sullivan, A.; Matthews, P.; von Beijnum, I. *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*; RFC 6147; IETF: Fremont, CA, USA, 2011.
230. Curran, J. *An Internet Transition Plan*; RFC 5211; IETF: Fremont, CA, USA, 2008.
231. Van de Velde, G.; Droms, R.; Carpenter, B.; Klein, E. *Local Network Protection for IPv6*; RFC 4864; IETF: Fremont, CA, USA, 2007.
232. Chown, T. *IPv6 Implications for Network Scanning*; RFC 5157; IETF: Fremont, CA, USA, 2008.
233. Jankiewicz, E.; Loughney, J.; Narten, T. *IPv6 Node Requirements*; RFC 6434; IETF: Fremont, CA, USA, 2011.
234. Narten, T.; Huston, G.; Roberts, L. *IPv6 Address Assignment to End Sites*; RFC 6177; IETF: Fremont, CA, USA, 2011.

235. Berkowitz, H. *Router Renumbering Guide*; RFC 2072; IETF: Fremont, CA, USA, 1997.
236. Bound, J. *IPv6 Enterprise Network Scenarios*; RFC 4057; IETF: Fremont, CA, USA, 2005.
237. Gill, V.; Maeyer, D.; Pignataro, C. *The Generalized TTL Security Mechanism (GTSM)*; RFC 5082, IETF: Fremont, CA, USA, 2007.
238. Baker, F.; Lear, E.; Droms, R. *Procedures for Renumbering an IPv6 Network without a Flag Day*; RFC 4192; IETF: Fremont, CA, USA, 2005.
239. Hinden, R.; Thaler, D. *IPv6 Host-to-Router Load Sharing*; RFC 4311; IETF: Fremont, CA, USA, 2005.
240. Crawford, M. *Router Renumbering for IPv6*; RFC 2894; IETF: Fremont, CA, USA, 2000.
241. Nadas, S. *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6*; RFC 5798; IETF: Fremont, CA, USA, 2010.
242. Crawford, M. *Transmission of IPv6 Packets over Ethernet Networks*; RFC 2464; IETF: Fremont, CA, USA, 1998.
243. Conta, A.; Malis, A.; Mueller, M. *Transmission of IPv6 Packets over Frame Relay Networks Specification*; RFC 2590; IETF: Fremont, CA, USA, 1999.
244. Varada, S.; Haskins, D.; Allen, E. *IP Version 6 over PPP*; RFC 5072; IETF: Fremont, CA, USA, 2007.
245. Varada, S. *Negotiation for IPv6 Datagram Compression Using IPv6 Control Protocol*; RFC 5172; IETF: Fremont, CA, USA, 2008.
246. Guttman, E. *Service Location Protocol Modifications for IPv6*; RFC 3111; IETF: Fremont, CA, USA, 2001.
247. Allman, M.; Ostermann, S.; Metz, C. *FTP Extensions for IPv6 and NATs*; RFC 2428; IETF: Fremont, CA, USA, 1998.
248. Routhier, S. *Management Information Base for the Internet Protocol (IP)*; RFC 4293; IETF: Fremont, CA, USA, 2006.
249. Haberman, B. *IP Forwarding Table MIB*; RFC 4292; IETF: Fremont, CA, USA, 2006.
250. Raghunathan, R. *Management Information Base for the Transmission Control Protocol (TCP)*; RFC 4022; IETF: Fremont, CA, USA, 2005.
251. Fenner, B.; Flick, J. *Management Information Base for the User Datagram Protocol (UDP)*; RFC 4113; IETF: Fremont, CA, USA, 2005.
252. Baer, M.; Charlet, R.; Hardaker, W.; Story, R.; Wang, C. *IPsec Security Policy Database Configuration MIB*; RFC 4807; IETF: Fremont, CA, USA, 2007.
253. Chesterfield, J.; Haberman, B. *Multicast Group Membership Discovery MIB*; RFC 5519; IETF: Fremont, CA, USA, 2009.
254. Daniele, M.; Haberman, B.; Routhier, S.; Schoenwaelder, J. *Textual Conventions for Internet Network Addresses*; RFC 4001; IETF: Fremont, CA, USA, 2005.