Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

IPv6

IPv6-Profile
für die Öffentliche Verwaltung

Bundesverwaltungsamt
Der zentrale Dienstleister des Bundes

Das Projekt IPv6 wird durch das Bundesverwaltungsamt gemeinsam mit dem Bundesministerium des Innern, Referat IT 5, betreut.

Das vorliegende Dokument wurde durch die Bundesstelle für Informationstechnik des Bundesverwaltungsamtes in Zusammenarbeit mit den Firmen **BearingPoint**, **Cassini** und **Fraunhofer FOKUS** erstellt.

Ansprechpartner

Markus Richter

Bundesverwaltungsamt
Referat BIT A 5

E-Mail: LIR@bva.bund.de

Ansprechpartner zu Sicherheitsfragen

Markus de Brün

Bundesamt für Sicherheitsfragen in der Informationstechnik

E-Mail: ipv6@bsi.bund.de

Autoren

Jens Tiemann	Fraunhofer FOKUS
Gabriele Goldacker	Fraunhofer FOKUS
Joachim Kaeber	Fraunhofer FOKUS
Carsten Schmoll	Fraunhofer FOKUS
Tahar Schaa	Cassini Consiltung GmbH
Constanze Bürger	Bundesministerium des Innern

Impressum

Herausgeber Bundesverwaltungsamt
Version 1.1
Titelbild: www.sxc.hu

Inhaltsverzeichnis

1. Management Summary

Seit den Anfangstagen des Internets wird zur Übertragung der Daten das Internet-Protokoll in der Version 4 (IPv4) verwendet. Heute wird dieses Protokoll überall verwendet, auch in den internen Netzen von Behörden und Organisationen. Das Internet und alle Netze, welche IPv4 heute verwenden, stehen vor einem tiefgreifenden technischen Wandel, denn es ist zwingend für alle zum Nachfolger IPv6 zu wechseln.

Auf die oft gestellte Frage, welche wesentlichen Faktoren eine Migration zu IPv6 vorantreiben, gibt es zwei zentrale Antworten:

- Es gibt einen Migrationszwang, der auf die jetzt schon (in Asien) nicht mehr verfügbaren IPv4-Adressen zurückführen ist.
- Mit dem steigenden Adressbedarf für alle Klein- und Großgeräte, vom Sensor über Smartphones bis zur Waschmaschine, die über IP-Netze kommunizieren müssen, verschärft sich das Problem der zur Neige gegangenen IPv4-Adressräume.

Das Zusammenkommen beider Faktoren beschleunigt den Antrieb zur IPv6-Migration.

Es wird in Zukunft viele Geräte geben, die nur noch über eine IPv6-Adresse anstatt einer IPv4-Adresse verfügen und nur über diese erreichbar sind. Schon heute kann bei den aktuellsten Betriebssystemversionen IPv6 nicht mehr deaktiviert werden. Restliche IPv4-Adressen wird man bei Providern gegen entsprechende Gebühren noch mieten können. Bei einem Providerwechsel im Kontext einer Neuausschreibung von Dienstleistungen wird man diese jedoch nicht mehr „mitnehmen“ können. Damit bedeutet eine Migration zu IPv6 nicht nur die garantierte Verfügbarkeit ausreichend vieler IP-Adressen, sondern stellt auch die Erreichbarkeit eigener Dienstleistungen für die Zukunft sicher, ohne von einem Anbieter abhängig zu sein.

Mit der Beschaffung eines Adressblocks, der für die gesamte öffentliche Verwaltung dimensioniert ist, wurde durch das Ministerium des Innern in 2009 der erste Schritt getan. Der Adressbereich stellt sicher, dass in Zukunft Verwaltungseinheiten nur noch mit eindeutigen Adressbereichen kommunizieren und die Kommunikation so direkter, einfacher und effizienter wird. Das Management dieses Adressbereichs folgt den föderalen Strukturen von Bund, Ländern und Kommunen.

Der zweite Schritt war die Entwicklung von Maßnahmen um den Ein- und Umstieg auf IPv6-Adressen für die Verwaltungen zu fördern und zu unterstützen. Mit den vorliegenden Dokumenten sind die Ergebnisse jetzt verfügbar. Diese unterstützen den Beschaffungsprozess neuer Geräte, die Evaluierung vorhandener Hardware und Software und helfen bei der Einführung von und der Migration zu IPv6.

Beschaffungsprozesse und die Untersuchung bestehender Geräte werden durch das in diesem Dokument beschriebene IPv6-Profil der öffentlichen Verwaltung unterstützt. Die Definition von notwenigen, sinnvollen und optionalen Eigenschaften IPv6-tauglicher Geräte ermöglicht die detaillierte Festlegung von Auswahlkriterien. Dadurch können Anforderungen in Bezug auf Geräte (Router, Firewall …) und Kontext (Arbeitsplatz, mobil …) beschrieben werden, was die Überprüfung der Vorgaben vereinfacht. Die Profile können darüber hinaus auch dafür eingesetzt werden bestehende Infrastrukturelemente für ihren Einsatz in IPv6-Umgebungen zu überprüfen.

Mit dem Migrationsleitfaden liegt ein begleitendes Dokument vor, das die schrittweise Einführung von IPv6 beschreibt. Dort wird die Umstellung von Geräten und Netzen nach IPv6 beziehungsweise auf IPv4/IPv6-Dual-Stack-Betrieb dargestellt. Hierbei werden die Größe der Verwaltungen, ihre Aufgaben und Infrastrukturvarianten berücksichtigt. Die Kernaussagen sind in Form von Leitlinien zur Migration mit klaren Handlungsanweisungen und Checklisten im Anhang des Migrationsleitfadens zusammengefasst.

Die vorliegenden Dokumente berücksichtigen in besonderem Maße die Anforderungen und Eigenschaften der Verwaltung (z. B. vorhandene Netz-strukturen und Sicherheitsanforderungen) und schaffen dadurch für die Verwaltung die Grundlagen für einen gezielten und strukturieren Einstieg in die Umstellung zu IPv6.

Mit der Veröffentlichung der Dokumente unter http://www.ipv6.bva.bund.de stehen diese Informationen allen Interessierten zur Verfügung und bieten eine pragmatische Hilfe bei der Annäherung an das Thema IPv6 und bei der praktischen Umsetzung einer Migration.

2. Einleitung

Das vorliegende IPv6-Profil der öffentlichen Verwaltung bietet eine Unterstützung für die Beschaffung von neuen Hard- und Softwarekomponenten. Es spezifiziert, welche IPv6-Standards von einem Gerät oder System unterstützt werden müssen, um festgelegte Aufgaben zu erfüllen.

Das Profil besteht aus einer „Profilmatrix“, in der alle wesentlichen Angaben zusammengefasst sind und diesem Begleitdokument, das den Aufbau des Profils sowie einige Details des Profils näher erläutert. Das Profil kann auch genutzt werden, um bestehende Hard- und Software-Komponenten auf ihre IPv6-Tauglichkeit zu untersuchen.

Wichtig ist die Tatsache, dass IPv6 in den nächsten Jahren auf breiter Ebene eingeführt wird. Insbesondere bei Neubeschaffungen von Infrastruktur-komponenten (wie Routern, Gateways, Servern aber auch Anwendungen) muss eine Zukunftssicherheit der Investitionen durch die Berücksichtigung von IPv6 gewährleistet sein.

Die Einführung von IPv6 kann auf ganz verschiedene Weise vorgenommen werden:

- Auf bestehender, aktueller Infrastruktur kann IPv6 im ganzen Netz oder in einzelnen Teilen zusätzlich zu IPv4 genutzt werden (Dual-Stack-Ansatz bzw. Teilmigration),

- In neu aufzubauenden Netzen mit klar definierten Aufgaben und Schnitt-stellen kann ggf. ausschließlich IPv6 zum Einsatz kommen (IPv6-only-Betrieb).

Der begleitende Migrationsleitfaden [IPv6_Migration] bietet sowohl Hilfestellung zur Planung als auch zur konkreten Umsetzung bei der Einführung von IPv6.

Beim Aufbau von IPv6-Netzen, unabhängig ob auf der Basis bestehender Komponenten oder im Rahmen von Neubeschaffungen, steht die genaue Analyse der Einsatzszenarien am Anfang. Darauf aufbauend kann festgelegt werden, welche Netzfunktionen genutzt werden sollen. Diese Festlegung von Einsatz-bedingungen ist eine wichtige Grundlage für die Nutzung des Profils. Über diese Bedingungen wird gesteuert, welche Funktionsblöcke des Profils zu betrachten sind und dementsprechend von konkreten Geräten unterstützt werden müssen. Erst über die Festlegung der Einsatzbedingungen kann eine sinnvolle Auswahl von Geräteanforderungen anhand des Profils festgelegt werden. So ist es nicht sinnvoll in einer Ausschreibung pauschal die „Erfüllung des IPv6-Profils“ zu fordern.

Vielmehr ist das Profil als eine Art Checkliste zu verstehen, um die Profilteile zu bestimmen, die für das vorgesehene Netzwerk wichtig sind und diese dann für eine Ausschreibung zu verwenden. Alternativ man kann zu ausgewählten Anforderungen des Profils eine Stellungnahme von Herstellern anfordern, um nähere Informationen zu den Funktionen eines Geräts zu erhalten. In beiden Fällen dient das Profil als Grundlage für den Austausch zwischen Kunde und

Hersteller, auf Basis der Auflistung relevanter IPv6-Standards (Request for Comments, RFC).

Abschließend soll noch darauf hingewiesen werden, dass die Erfüllung des Profils durch verschiedene Systeme von mehreren Herstellern nicht automatisch zu einem funktionsfähigen Netzwerk führt. Die Erfüllung von spezifizierten Profilanforderungen ist ***eine notwendige*** Bedingung für den späteren reibungslosen Betrieb. Das Profil beschreibt in diesem Zusammenhang nur, was ein Gerät grundsätzlich können muss.

Die konkrete Konfiguration eines Geräts ist nicht Bestandteil des Profils. Passen die Konfigurationen (bspw. die Art der Adressvergabe, die Verschlüsselung eines Tunnels) von zwei Standard-konformen Systemen nicht zueinander, so wird die Kommunikation nicht funktionieren. In der Praxis können außerdem noch Probleme aufgrund von leicht unterschiedlichen Implementierungen der Standards auftreten bzw. aufgrund eines unterschiedlichen Verständnisses der Hersteller bei Detailfragen der Standards. Hilfreich sind Interoperabilitätstests, welche die Zusammenarbeit in konkreten, realistischen Szenarien zum Ziel haben und damit die konkrete Eignung nachweisen können. Weiterhin empfiehlt sich der Aufbau eines kleinen Testnetzes bzw. die Nutzung von Teststellungen für infrage kommende Geräte.

2.1. Zweck und Aufbau des Dokuments

Dieses Begleitdokument erläutert das IPv6-Profil, das in Form einer „Profilmatrix“ vorliegt. Es soll nochmals darauf hingewiesen werden, dass das Profil grundsätzlich keine Konfigurationsempfehlungen enthält. Im Profil wird dargestellt, welche Funktionen in den Geräten und Systemen vorhanden sein müssen; nur in wenigen Ausnahmefällen wird aus Gründen der Netzwerksicherheit auch im Profil auf die Konfiguration eingegangen. Weitere Hinweise zur Konfiguration von Geräten finden sich im Migrationsleitfaden [IPv6_Migration].

Da es für Hardware-Komponenten international bereits eine Reihe von Profilen gibt, werden diese im Anschluss in Kapitel 3 kurz vorgestellt und bewertet.

In Kapitel 4 wird das IPv6-Hardwareprofil für die öffentliche Verwaltung beschrieben. Detailinformationen zu den einzelnen Geräteklassen (Geräteprofilen) sind im Dokument „Profilmatrix“ zu finden. Dort sind sowohl die im Projekt erarbeiteten Empfehlungen für die öffentlichen Verwaltungen als auch die Vorgaben anderer, vergleichbarer Profile (vgl. Kapitel 3) aufgeführt.

In Kapitel 5 werden die von der Migration betroffenen Software-Komponenten auf IPv6-spezifische Anforderungen hin untersucht.

2.2. Methodik

Bereits eine erste Sichtung der vorgefundenen Profile ergab, dass diese nicht miteinander konkurrierende, sondern vielmehr komplementäre Ansätze darstellen, um Anforderungen an IPv6-fähige Komponenten mit jeweils eigenen Sichtweisen und Schwerpunkten zu formulieren.

Für die Erarbeitung eines eigenen IPv6-Profils für die öffentliche Verwaltung wurden die existierenden Profile einander in tabellarischer Form gegenübergestellt, um gemeinsame Strukturelemente herauszuarbeiten und in einer konsistenten Form zu konsolidieren.

Alle betrachteten Profile nehmen Bezug auf relevante RFCs und legen jeweils Anforderungsgrade für verschiedene Geräteklassen fest. Sie geben also Empfehlungen ab, ob und inwieweit diese RFCs (verpflichtend oder auch nur optional) in spezifischen Implementierungen umzusetzen sind.

Neben Unterschieden in der verwendeten Terminologie fällt auch sofort der unterschiedliche Grad der Detaillierung auf: So werden in einem Dokument einige RFCs in Gänze als verpflichtend bezeichnet, während ein anderes Dokument detailliert auf einzelne, im jeweiligen RFC spezifizierte Merkmale, Funktionen oder Protokollelemente eingeht, um diese separat je Gerätetyp mit einer Empfehlung zu versehen.

Ergebnis dieser Arbeiten ist eine Sammlung von Tabellenblättern, in denen in stark strukturierter Form sowohl die Anforderungsgrade der vorgefundenen Profildokumente als auch die in zahlreichen Diskussionen (auch mit externen Gesprächspartnern) gefundenen Projekt-Empfehlungen aufgeführt sind. In der praktischen Arbeit kann es hilfreich sein, auch andere Profile zu nutzen, wobei das vorliegende Profil den Einstieg erleichtert. Bei der Darstellung der Anforderungsgrade fremder Profile in der „Profilmatrix“ des IPv6-Profils der ÖV sollte beachtet werden, dass fremde Profile nicht immer vollständig in das gewählte Schema passen und es daher zu ungenauen Aussagen kommen kann.

Das Profil wurde mit Herstellern von Sicherheitsgeräten diskutiert und abgestimmt. Weitere Rückmeldungen zum Profil werden weiterhin entgegen genommen und fließen ggf. in Überarbeitungen des Profils ein.

Da die Entwicklung von IPv6 weiterhin sehr dynamisch ist, sind auch die Empfehlungen dazu weiter zu entwickeln. Es werden neue RFCs mit Bezug zu IPv6 erscheinen, bestehende werden aktualisiert, und nicht zuletzt sind auch praktische Erfahrungen zu erwarten, die eine Fortschreibung dieses Dokuments erforderlich machen werden.

3. Existierende IPv6-Profile

Die Protokolle des Internets sind in Standards (STDs) und sogenannten Requests for Comments (RFCs) der Internet Engineering Task Force (IETF) spezifiziert. Etwa 200 Dokumente beschreiben die Familie der IPv6-Protokolle sowie notwendige Anpassungen oder Optionen anderer Protokolle, damit diese mit IPv6-Systemen zusammenarbeiten können.

Die existierenden Profile beschreiben entweder nur Anforderungen, die Geräte bzw. Implementierungen erfüllen müssen, um erfolgreich an einer (RFC-konformen) IPv6-Kommunikation teilnehmen zu können, oder weiter gehende Bedingungen, beispielsweise an die Unterstützung bestimmter Qualitäts- oder Sicherheitsfunktionen und -merkmale. Dabei sind alle Profile als ein Schritt auf dem Weg zur Interoperabilität zwischen Geräten zu sehen. Das Zusammenarbeiten von Geräten hängt außerdem von der konkreten Konfiguration ab und kann kleinere Unterschiede in den Implementierungen, bspw. aufgrund von unterschiedlicher Interpretation der Standards, gestört werden.

In den folgenden Abschnitten sind die wesentlichen existierenden Profile dargestellt.

3.1. Requirements for IPv6 in ICT Equipment (ripe-554)

Das Réseaux IP Européens Network Coordination Centre (RIPE NCC) unterstützt die technische Koordination der Internet-Infrastruktur in Europa. In diesem Rahmen wird durch die IPv6-Working-Group ein Satz von „Requirements For IPv6 in ICT Equipment“ (Anforderungen für die Unterstützung von IPv6 in IKT-Geräten) entwickelt. Diese Anforderungen wurden im November 2010 im Dokument „ripe-501“ [ripe-501] beschrieben. Inzwischen liegt mit dem Dokument „ripe-554“ [ripe-554] vom Juni 2012 eine aktualisierte Version vor.

Das Dokument ripe-554 ist als unterstützende Sammlung von „Best Practices“ für die Beschaffung von IPv6-Geräten und -Dienstleistungen durch Verwaltungen und große Unternehmen angelegt.

Ripe-554 identifiziert für die wesentlichen Geräteklassen – Switches (unterschieden nach Endkunden- und Unternehmens-/ISP-Switches), Router, Endgeräte, Sicherheitsgeräte (unterschieden nach Paketfiltern, Application-Layer-Gateways und Intrusion-Prevention-Geräten), CPE-Router, Mobile Devices, Load Balancer – verpflichtend zu implementierende und optional zu unterstützende RFCs. Es wird empfohlen, Geräte mit einer großen Anzahl unterstützter optionaler RFCs zu bevorzugen.

ripe-554 ist relativ grob in der Betrachtung des referenzierten RFCs, da es nicht auf unabhängige Unterfunktionen und Optionen in den RFCs eingeht.

3.2. DoD Unified Capabilities Requirements 2008, Change 2

Das Dokument „Department of Defense Unified Capabilities Requirements 2008, Change 2 (UCR 2008, Change 2)“ [UCR08_2], welches entgegen dem Anschein des Titels vom Dezember 2010 stammt, beschreibt sehr umfangreich und ausführlich vielfältige Anforderungen an Geräte und Implementierungen für eine Zulassung durch das US-amerikanische Verteidigungsministerium[1]. In Unterkapitel 5.3.5 des Dokumentes sind die Anforderungen im Zusammenhang mit IPv6 aufgeführt. Das Dokument enthält als integralen Bestandteil die „DoD IPv6 Standard Profiles For IPv6 Capable Products Version 5.0“ vom Juli 2010.

Das Dokument enthält eine detaillierte Geräteklassifikation und identifiziert notwendige bzw. wünschenswerte oder optionale Funktionen anhand der Oberklassen einfaches Endgerät / einfacher Server, Router, Sicherheitsgerät (Paketfilter bzw. Application-Layer-Gateway), Switch und Endgerät (bzw. spezielle Anwendung).

Es wird nicht nur auf die Unterstützung von RFCs und Funktionen bzw. Optionen eingegangen, sondern es werden auch konkrete Forderungen bzw. Präferenzen beschrieben, wie diese Funktionen / Optionen zu nutzen sind.

3.3. IPv6 Ready Logo Program des IPv6-Forums

Das herstellergetriebene IPv6 Ready Logo Program [IPv6Ready] des IPv6-Forums umfasst Spezifikationen für Konformitäts- und Interoperabilitäts-Tests für elementare IPv6-Protokolle:

- die IPv6-Basis-Protokolle (einschließlich SLAAC2, ICMP3, Addressing Architecture, Explicit Congestion Notification, Neighbor Discovery und Path MTU4 Discovery)
- IPsec und IKEv2[5]
- Multicast Listener Discovery Version 2
- SNMP-MIBs[6]
- Mobile IPv6 und NEMO[7]
- DHCPv6[8]
- SIP[9]

[1] Department of Defense, DoD
[2] Stateless Address Autoconfiguration
[3] Internet Control Message Protocol
[4] Maximum Transfer Unit
[5] Internet Key Exchange
[6] Management Information Base
[7] Network Mobility
[8] Dynamic Host Configuration Protocol
[9] Session Initiation Protocol

Das IPv6-Forum bietet zu diesem Zweck fertige Testsuites für die automatisierte Abarbeitung an, deren erfolgreiches Absolvieren zum Führen des IPv6-Ready-Logos berechtigt. Die Tests werden von akkreditierten Testzentren angeboten, allerdings kann der Nachweis auch durch eine Selbsterklärung des Herstellers erfolgen.

Die Tests sind – zweckgemäß – sehr detailliert und umfangreich, berücksichtigen die unterschiedlichen Rollen der beteiligten Geräte (Geräteklassen) und gehen bis auf die Ebene einzelner Nachrichten und Nachrichtenwechsel hinunter. Andererseits ist der Satz der betrachteten RFCs gegenüber der Gesamtmenge (36 von über 200) relativ beschränkt.

Festlegungen, die an der Schnittstelle einer Komponente (über alle Protokollschichten) nicht überprüft werden können, entziehen sich naturgemäß den Tests eines solchen Programms. Auf ihre korrekte Implementierung kann daher nicht allein daraus geschlossen werden, dass ein betrachtetes Gerät mit dem IPv6 Ready Logo ausgestattet ist. Derartige Festlegungen betreffen beispielsweise Knoten-internes Management.

Die Schutzfunktionen von Paketfiltern und Application-Layer-Gateways werden vom IPv6 Ready Logo Program nicht erfasst, da sie nicht einheitlich standardisiert oder durch RFCs beschrieben sind, gegen die ein Test vorgenommen werden könnte.

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

Dieses in der Version 1.0 vom September 2008 erste öffentliche Profildokument [NIST_USGv6] wurde vom US-amerikanischen NIST[10], einer zum Handelsministerium gehörenden Institution, entwickelt.

Das Dokument unterscheidet zwischen Endgeräten, Routern und Sicherheitsgeräten (Paketfilter, Application-Layer-Gateways und Intrusion Detection / Prevention-Geräte).

Es kategorisiert die Netzfunktionen nach 12 Gruppen: Basisfunktionen, Routing, Dienstqualität, Transition zwischen IPv4 und IPv6, Link-Spezifika, Adressierung, IPsec-Protokollfamilie, Netz-Management, Multicasting, Mobilität, Anwendungsanforderungen und spezielle Anforderungen für Sicherheitsgeräte.

Im Dokument wird sehr detailliert auf die Einsatzumgebung und die Querbezüge zwischen Funktionen (auch aus verschiedenen RFCs) eingegangen. Da sich daraus sehr viele bedingte Anforderungen („Conditionals“) ergeben, erfordert das Verständnis des Dokumentes vergleichsweise viel Zeit und Aufwand.

Das Profil unterscheidet nur zwischen verpflichtenden und optionalen Funktionen, enthält sich aber jeglicher Bewertung der optionalen Funktionen. Für jede Funktion ist angegeben, welche RFCs (bzw. welche separat implementierbaren

[10] National Institute of Standards and Technology

Teile bestimmter RFCs) umgesetzt sein müssen, um die Funktion profilgemäß zu realisieren.

Dieses Dokument kommt in seinem Zweck der Aufgabe des vorliegenden Projektes am nächsten. Allerdings sind auch einige wesentliche Teile des Dokumentes durch den zwischenzeitlichen Fortschritt bei den IPv6-bezogenen Spezifikationen inzwischen teilweise veraltet oder müssen vom Leser zumindest auf aktuellere RFCs übertragen werden. Leider ist bislang keine aktuellere Version des Dokumentes öffentlich verfügbar.

3.5. Guidelines for the Secure Deployment of IPv6

Dieses ebenfalls vom NIST verfasste Dokument [NIST_119] vom Dezember 2010 ist in erster Linie ein IPv6-Tutorium; es hat aber einen besonderen Fokus auf die bislang noch nicht abschließend geklärten Sicherheitsrisiken beim Einsatz von IPv6-Protokollen (IPv6, ICMPv6).

3.6. IPv6 Node Requirements

RFC 6434 – IPv6 Node Requirements [RFC6434] vom Dezember 2011 (eine Aktualisierung von RFC 4294 vom April 2006 [RFC4294]) ist im Wesentlichen eine informelle Zusammenfassung der grundlegenden IPv6-RFCs und der enthaltenen Teilfunktionen sowie ihrer Relevanz.

Das Dokument unterscheidet nur zwischen Knoten (beliebigen IPv6-Geräten), Routern und Endgeräten. Damit wird den weiteren Transitsystemen, beispielsweise Sicherheitsgeräten ohne echte Routingfunktion, nur unzureichend Rechnung getragen.

3.7. Informative RFCs

Die RFC-Dokumente sind in verschiedene Kategorien eingeteilt:

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

Dementsprechend könnte man erwarten, dass alle relevanten Informationen für das IPv6-Profil in den Standard-Dokumenten zu finden sind, während es sich beispielsweise bei Dokumenten zu „Best Current Practice“ hauptsächlich um Konfigurationsempfehlungen handelt. In der Praxis sind die Grenzen nicht ganz so festgelegt. Der Hintergrund dafür ist hauptsächlich in dem Vorgehen bei der Standardisierung durch die IETF zu finden: Neue Themen (z. B. ein neuer Sicherheitsmechanismus) werden durchaus in verschiedenen Arbeitsgruppen oder mit verschiedenen Ansätzen diskutiert. Das Interesse an den Themen und die Beteiligung über die Dauer der Prozesse bis zur Veröffentlichung eines RFCs haben einen großen Einfluss auf die Arbeit und das Ergebnis. Daraus ergeben sich einerseits relevante, pragmatisch nutzbare Protokollspezifikationen,

andererseits aber auch Unklarheiten in Detailfragen und verschiedenartige RFC-Dokumente.

Einzelne RFCs der Kategorie „Informational“ kann man durchaus als alleinige Festlegung von relevanten Parametern betrachten und daher sind sie im IPv6-Profil zu finden. Im vorliegenden IPv6-Profil werden die unterschiedlichen Kategorien der RFCs nicht gekennzeichnet.

Einige RFCs liefern gut lesbare Zusammenfassungen oder Klarstellungen zu anderen RFCs bzw. Mechanismen, sodass es auch hilfreich sein kann, diese zu kennen. Im Weiteren dieses Abschnitts werden derartige Übersichts-RFCs kurz vorgestellt, die für die Arbeit mit IPv6 und dem Profil nützlich sind.

3.7.1 RFC 6434 – IPv6 Node Requirements

RFC 6434 („IPv6 Node Requirements“) [RFC6434] ist eine Grundlage dieses IPv6-Profils, wie im vorherigen Abschnitt beschrieben. Das Dokument fasst verschiedene Anforderungen an IPv6-Geräte (bspw. Endsysteme oder Router) zusammen, wobei die umfangreichen Anforderungen nach Protokollebenen (Sub-IP Layer und IP Layer) bzw. nach Protokollmechanismen (z. B. DNS und DHCP, Mobile IP, Sicherheit) strukturiert sind. Die Relevanz des Dokuments lässt sich auch daran erkennen, dass es sich um die zweite Version dieser Zusammenfassung handelt (dieser RFC ersetzt [RFC4294]). In dem Dokument wird das Zusammenspiel von Protokollen und Mechanismen deutlich, wobei überwiegend zu Details oder den Anforderungen auf die aktuellen RFCs verwiesen wird. Das Dokument legt aber auch eigene Anforderungsgrade fest, bspw. welche anderen RFCs bzw. welche Teile anderer RFCs oder implementiert werden müssen.

3.7.2 RFC 6204 – Basic Requirements for IPv6 Customer Edge Routers

Eine spezielle Geräteklasse sind Router in lokalen Netzen, die den Übergang zum Provider herstellen. Es sind verschiedene Bezeichnungen üblich je nach Einsatzszenario: Perimeter-Router, Edge Router, SOHO-Router (siehe Tabelle 1). RFC 6204 („Basic Requirements for IPv6 Customer Edge Routers“) [RFC6204] beschreibt Anforderungen in Bezug auf die WAN- und die LAN-Seite eines derartigen Routers sowie generelle Eigenschaften. Im RFC werden die verschiedenen Anforderungen entsprechend der typischen Aufgaben solcher Geräte deutlich, bspw. die Rolle des Routers bei der Adresskonfiguration in einem lokalen Netz. Anforderungen in Bezug auf Sicherheitsmechanismen sind weitgehend in einem weiteren RFC zu finden, der in RFC 6204 referenziert wird (RFC 6092: „Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service“ [RFC6092]).

Bei Erscheinen dieses Profils wurde schon intensiv an einem Nachfolgedokument gearbeitet [RFC6092bis], was insbesondere auf die Komplexität des Zusammenspiels von verschiedenen Protokollen und die rasante Entwicklung des Einsatzes von IPv6 zurückzuführen ist.

3.7.3 RFC 4864 – Local Network Protection for IPv6

Der Schwerpunkt des RFCs liegt auf der Darstellung, welche typischen, sicherheitsrelevanten Aufgaben in Netzen anfallen und welche IPv6-Mechanismen dabei angewendet werden können. Ausgangspunkt ist die Beobachtung, dass viele dieser Aufgaben bei IPv4 in der Praxis mittels Network Address Translation (NAT) realisiert werden. Da der Einsatz von NAT in Netzen nicht unproblematisch ist, wird in diesem RFC gegenübergestellt, wie typische Aufgaben, die in IPv4-Netzen von NAT übernommen werden, mittels vorhandener IPv6-Protokollmechanismen gelöst werden können.

3.7.4 RFC 6071 – IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap

Das Dokument [RFC6071] gibt eine Übersicht über die verschiedenen RFCs aus dem Bereich IPsec. Im Laufe der Standardisierung von IPsec sind eine Reihe von Dokumenten aus verschiedenen Arbeitsgruppen entstanden, sodass es schwer ist, eine Übersicht zu bekommen. In dieser Aufstellung werden die RFCs der IPsec-Protokollfamilie thematisch gruppiert und jeweils mit einer Kurzbeschreibung sowie Hintergrundinformationen vorgestellt.

4. IPv6-Profil für Hardware-Komponenten

Dieses Kapitel enthält eine Beschreibung der im Dokument „Profilmatrix“ dargestellten Anforderungen. Zunächst wird die generelle Struktur der Tabellenblätter eingeführt (Abschnitt 4.1). Darauf folgen Beschreibungen der Einzelblätter.

4.1. Struktur der Profiltabellen

Um die Informationen, die in ihrer Gesamtheit ein Geräteprofil ergeben, möglichst einfach auffindbar zu machen, ist das Profil im Wesentlichen entlang zweier Dimensionen strukturiert:

- Geräteklassen
- Funktionskategorien

Die verschiedenen Geräteklassen sind jeweils auf einem eigenen Tabellenblatt beschrieben (siehe Abschnitt 4.1.1).

Die Empfehlungen zu einzelnen Funktionen sind hierarchisch nach Kategorien strukturiert (siehe Abschnitt 4.1.2).

Um Redundanzen in der Beschreibung zu vermeiden, wird zunächst der IPv6-Knoten als Basis für alle Geräte definiert. In allen weiteren Geräteklassen sind nur die über den Knoten hinausgehenden Anforderungen definiert.

4.1.1 Geräteklassen

Die existierenden Profile beschreiben verschiedene Geräteklassen. So werden in RFC 2460 – Internet Protocol, Version 6 (IPv6) Specification [RFC2460] die Geräteklassen Knoten („Node“), Router und Endgerät („Host“) definiert:

```
2. Terminology
  node   - a device that implements IPv6.
  router - a node that forwards IPv6 packets
           not explicitly addressed to itself.
  host   - any node that is not a router.
```

Im vorliegenden IPv6-Profil für die öffentliche Verwaltung wird die Menge der Geräteklassen erweitert. Dies führt zu der in Abbildung 1 dargestellten Hierarchie von Geräteklassen. Die „weißen Knoten“ sind Strukturierungshilfen, ohne dass für sie eigene Blätter angelegt wurden.

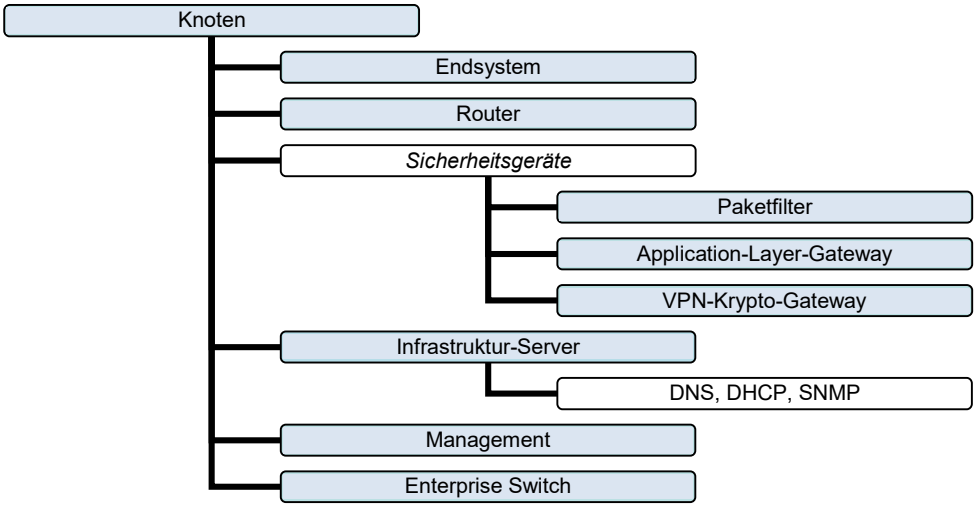


Abbildung 1: Hierarchie von Geräteklassen

Diese Klassen repräsentieren zunächst nur abstrahierte Komponenten. So sind in der Abstraktion „Knoten“ die Anforderungen zusammengefasst, die auf alle konkreten IPv6-Geräte zutreffen. Ein konkretes Gerät kann die Funktionalität mehrerer Geräteklassen implementieren. Beispielsweise realisieren heute gängige SOHO-DSL-Router Funktionen aus den Geräteklassen Router, Paketfilter, DNS- / DHCP-Server und ggf. andere, sodass für die Betrachtung des konkreten Geräts mehrere Profiltabellen herangezogen werden müssen (vgl. Abbildung 2). Eine Besonderheit stellen Sicherheitsgeräte dar: Aufgrund der besonderen Anforderungen kann es bei ihnen zu Abweichungen von den Anforderungen an den Knoten kommen.

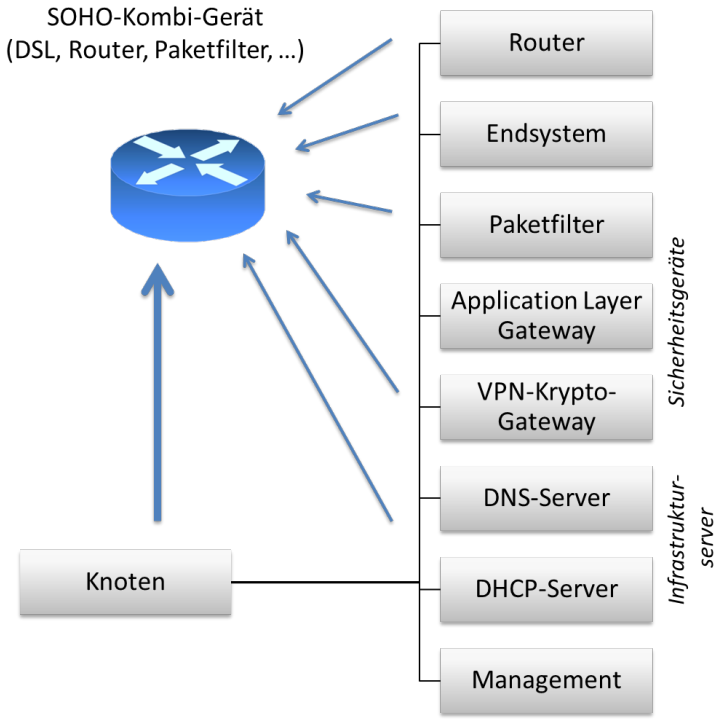


Abbildung 2: Komplexe Geräteklasse am Beispiel eines SOHO-Routers

Das IPv6-Profil orientiert sich an folgenden Prinzipien:

- Jede Funktion ist möglichst nur in einer Geräteklasse aufgeführt. Ausnahmen sind nur in begründeten Fällen möglich, etwa wenn einer Funktion einer bestimmten Geräteklasse (z. B. Router) ein höherer Anforderungsgrad als in der Basisklasse (Knoten) zugeordnet ist.

- Der Anforderungsgrad im Knoten kann für Router oder Endsysteme erhöht, nicht aber vermindert werden. So sind einige Funktionen aus dem Bereich „Stateless Address Autoconfiguration (SLAAC)“ für Knoten im Allgemeinen „empfohlen“, für Endsysteme hingegen „verpflichtend“. Für Sicherheitsgeräte ist in speziellen Fällen auch eine Reduzierung der Anforderung möglich, beispielsweise bei einer bestimmten, festen Anordnung von Geräten im Netz.

- Die im Tabellenblatt „Management“ aufgeführten Funktionen beschreiben in der Summe keine Geräteklasse, sondern bilden die für verschiedene Klassen relevanten Aspekte einer gegebenenfalls vorhandenen Management-Schnittstelle ab.

Als Einstieg in die einzelnen Geräteprofile empfiehlt sich Tabelle 1. In der ersten Spalte sind konkrete Geräte aufgeführt, wie sie in der ÖV gebräuchlich sind und deren Bezeichnungen sich auch in anderen Dokumenten wiederfinden. Die rechte Spalte gibt an, welche Tabellenblätter (d. h. konzeptionelle Geräteklassen) hierbei zu betrachten sind.

Gerät		Tabellenblätter
Endsystem		
	Arbeitsplatz, Desktop	Endsystem, Knoten, ggf. Management
	Notebook, Tablet	Endsystem, Knoten, ggf. Management, Paketfilter
	Server (Anwendung)	Endsystem, Knoten, Management
Router		
	SOHO-Router	Router, Knoten, Paketfilter, DNS- / DHCP-Server
	Perimeter-Router Edge-Router Border-Router	Router, Knoten, Management
	Infrastruktur-Router	Router, Knoten, ggf. DNS- / DHCP-Server, Management
(Layer2-) Switch		Enterprise Switch, Management
Sicherheitskomponente		
	Paketfilter	Paketfilter, typischerweise Router, Knoten, Management
	Application Layer Gateway (ALG), Proxy	Application Layer Gateway, ggf. Router, Knoten, Management
	Kryptobox VPN-Gateway	VPN-Krypto-Gateway, Knoten, ggf. Router, Paketfilter, Management
(Netzwerk-)Infrastruktur		
	DNS-Server DHCP-Server RADIUS-Server Tunnelbroker	Endsystem, Knoten, Infrastruktur-Server, Management

Tabelle 1: Zuordnung konkreter Geräte zu Tabellenblättern

4.1.2 Funktionskategorien

Die pro Geräteklasse in einem Tabellenblatt aufgeführten Funktionen sind in einer Hierarchie gruppiert, normalerweise bestehend aus der Kategorie, zur Kategorie gehörende, relevante RFCs und ausgewählte Merkmale / Funktionen aus dem RFC. Abbildung 3 zeigt ein Beispiel für diesen Strukturierungsansatz.

Zunächst sind die generischen Kategorien aufgeführt, die für mehrere Klassen relevant sind. Darauf folgen solche, die die eigentliche Kernfunktionalität einer Geräteklasse ausmachen.

Die folgende Aufzählung enthält eine Beschreibung der *generischen Funktionskategorien*:

- **Grund-Anforderungen**: Diese Funktionen sind für eine erfolgreiche IPv6-Kommunikation notwendig. Hierzu gehören insbesondere das IPv6-Protokoll, ICMPv6, Neighbor Discovery sowie Funktionen zur Ermittlung der maximalen Paketgröße (MTU Discovery).
- **Adressierung**: Hierzu gehören die Semantik und Formatierung der Adressen sowie die Adress-Konfiguration.
- **DNS-Resolver**: Zu dieser Kategorie gehören alle Unterschiede zwischen klientenseitigem DNS für IPv4 und für IPv6.
- **Transitionsmechanismen**: In diese Kategorie fallen Technologien, die dem Übergang von IPv4 auf IPv6 dienen.
- **NAT-Nachfolge**: In dieser Kategorie wird auf Mechanismen eingegangen, wie die Funktionen, die NAT bei IPv4 erbringt, in einer IPv6-Umgebung bereitgestellt werden können.
- **IPsec-Protokollfamilie**: In dieser Kategorie befinden sich die Sicherheitsfunktionen.
- **Multicast**: Diese Kategorie beinhaltet die Unterstützung von Multicast.
- **Dienstgüte** (Quality of Service, QoS): Zu dieser Kategorie gehören die Funktionen zur Unterstützung verschiedener Dienstgüte-Klassen.
- **Mobilität**: Diese Kategorie umfasst Funktionen für den Einsatz von Mobile IPv6.
- **Netzwerk-/System-Management-Schnittstelle**: Hier sind die Management-spezifischen Protokolle beschrieben, soweit diese nicht in die übergreifende Pseudo-Geräteklasse „Management“ ausgegliedert sind.

Eine ähnliche Kategorisierung findet sich in [UCR08_2].

Die daran anschließende Beschreibung von Anforderungen an *gerätespezifische Funktionen* (z. B. Router, Endsystem, Paketfilter) ist naturgemäß eher uneinheitlich.

4.1.3 Beschreibung der Tabellenspalten

Während die genaue Zeilenstruktur der Tabellenblätter spezifisch für die jeweils beschriebene Geräteklasse ist, ist die Spaltenstruktur der Blätter einheitlich (siehe Tabelle 2).

Spaltenbezeichnung	Inhalt
Kategorie **Kategorie** **Kategorie**	Ggf. mehrstufig gegliederte Funktionskategorie (vgl. 4.1.2)
RFC	Nummer des maßgeblichen RFCs
Titel	Titel des maßgeblichen RFCs
Merkmal, Funktion	Benennung der zu bewertenden Funktion
Projekt-Empfehlung	IPv6-Profil der öffentlichen Verwaltung
Kommentar	ggf. Anmerkungen
ripe-554 (Nachfolge ripe-501)	Empfehlung des jeweiligen Profil-Dokuments
NIST	
ipv6ready.org	
RFC 6434 **IPv6 Node Requirements**	
US DoD UCR 2008 Change 2[11]	
IPv6 Standard Profiles v5.0	

Tabelle 2: Beschreibung der Tabellenspalten

Da nicht alle referenzierten Profildokumente zu allen Funktionen oder Merkmalen Stellung beziehen, sind die Spalten unterschiedlich stark gefüllt. Ggf. finden sich auch zu Kategorien Hinweise, ob und wie ein bestimmtes Profil diese Geräteklasse oder Kategorie behandelt.

Aufgrund des unterschiedlichen Aufbaus des vorliegenden Profils und der anderen, in der gleichen Tabelle dargestellten Profile in Bezug auf Geräteklassen ist die Darstellung der Anforderungsgrade der anderen Profile nicht immer päzise und dient hauptsächlich der Information. Im Zweifelsfall ist das jeweilige Profil im Orginal zu betrachten.

[11] Werden die gleichen Anforderungen von den UCR und den IPv6 Standard Profiles erhoben, so sind in der Tabelle nur die UCR-Anforderungen aufgeführt.

4.1.4 Anforderungsgrade

Die bestehenden IPv6-Profile benutzen eine jeweils eigene Terminologie, um den Grad der Anforderung auszudrücken. Wir haben diese Begriffe (z. B. „must“, „should“, „can“, aber auch „mandatory“ und „optional“) auf eine durchgängige, deutschsprachige Terminologie abgebildet, die in Tabelle 3 zusammengefasst ist.

	Erläuterung
verpflichtend	Die beschriebene Eigenschaft muss in dieser Form aus technischen oder aus administrativen Gründen umgesetzt werden, da anders das gewollte Verhalten nicht erreicht werden kann.
empfohlen	Die Nutzung der Funktion wird als sinnvoll angesehen. Abhängig von den Gegebenheiten und Anforderungen im Einzelfall darf hiervon auch abgewichen werden.
optional	Die beschriebene Funktion ist optional.
nicht empfohlen	Die Funktion sollte nicht genutzt werden.
verboten	Die Funktion darf nicht genutzt werden.
zur Information	Weiterführende Information, z. B. Übersichtsdokumente
In den Beschreibungen der Fremdprofile außerdem: (diese Angaben sind nicht vollständig und dienen nur zur Information)	
erwähnt	Der RFC / die Funktion wird zwar erwähnt, aber nicht bewertet.
n. erw. / nicht erwähnt	Der RFC / die Funktion wird nicht erwähnt.

Tabelle 3: Definition der Anforderungsgrade

Für RFCs mit lediglich informellem Charakter wurde keine Empfehlung im IPv6-Profil für die öffentliche Verwaltung ausgesprochen. Sie enthalten keine konkrete, implementierbare Spezifikation, sondern beschreiben Anforderungen an eine Implementierung oder mögliche Realisierungen.

4.1.4.1 Bedingte Anforderungen

Sowohl in den vorhandenen Profilen als auch in diesen Profil-Empfehlungen gibt es Anforderungen, die nur bei Vorliegen bestimmter Randbedingungen sinnvoll sind. Solche Bedingungen sind in der jeweiligen Tabellenzelle formuliert.

Bedingungen, die für ganze Funktionskategorien gelten, sind auf die Kategorienebene hochgezogen. So wird z. B. der Einsatz von SNMP empfohlen. Damit verbundene Anforderungen sind natürlich nur dann zu beachten, wenn der Mechanismus tatsächlich eingesetzt werden soll.

In den Abschnitten 4.2 – 4.5 werden, soweit für erforderlich gehalten, einzelne Empfehlungen erläutert oder Hintergründe zu diesen Empfehlungen beschrieben. Es empfiehlt sich, den jeweiligen Abschnitt zusammen mit dem zugehörigen Tabellenblatt zu lesen.

Generell soll noch darauf hingewiesen werden, dass zusätzliche Funktionen nicht immer vorteilhaft sind. Zusätzliche Funktionen können einen vergrößerten Konfigurationsaufwand erfordern und insbesondere schlecht konfigurierte Systeme können von Angreifern als Einfallstor missbraucht werden. Zu beschaffende Geräte sollten daher den geplanten Funktionsumfang aufweisen oder höchstens für einen absehbar erweiterten Einsatz vorbereitet sein.

4.1.5 Beispiele zum Lesen der „Profilmatrix“

Im Folgenden werden einige Beispiele vorgestellt, wie das Profil zu lesen ist. Zur besseren Lesbarkeit wurden typische Beispiele aus dem Profil ausgeschnitten. In den Beispielen wird nur auf einzelne Aspekte eingegangen, die Beispiele lassen sich aber bei Bedarf im Profil leicht wiederfinden.

Blatt Knoten:

Kategorie	Kategorie	Kategorie	RFC	Titel	Merkmal, Funktion	Projekt- Empfehlung	Kommentar
Kommunikation des IPv6-Knotens							
	Grund-Anforderungen						
		Basis					
			RFC 2460		Internet Protocol, Version 6 (IPv6) Specification	verpflichtend	
					Flow Label Feld wird nicht genutzt und ignoriert (solange RFC 6437 nicht implementiert)	verpflichtend	

Abbildung 3: Profil-Beispiel 1 – Merkmal/Funktion mit Anforderungsgrad

Im ersten Beispiel sieht man unter dem RFC auch eine weitere Zeile, in der ein Detail des RFCs hervorgehoben wird. Ein Merkmal oder eine Funktion, die im RFC beschrieben ist, wird in dem Profil gesondert behandelt und mit einem eigenen Anforderungsgrad versehen. Dabei kann es sich, wie in diesem Fall, um eine Festlegung einer Option handeln, die im RFC selbst offen gelassen wurde. Oder es kann explizit ein anderer Anforderungsgrad festgelegt werden, als im RFC vorgesehen wurde.

Blatt Management:

Kategorie	Kategorie	Kategorie	RFC	Titel	Merkmal, Funktion	Projekt- Empfehlung	Kommentar
Geräte-Funktionalität							
	Management und -Konfiguration					verpflichtend	
					Zugang zu Management / Konfiguration über IPv6 und IPv4	empfohlen	
					Abschaltbarkeit des nicht für Management / Konfiguration verwendeten Protokolls	empfohlen	wenn eine separate Management- / Konfigurations schnittstelle benutzt wird

Abbildung 4: Profil-Beispiel 2 – Merkmal/Funktion ohne RFC

Das zweite Beispiel zeigt Anforderungen des Profils, die nicht über RFCs festgelegt werden. Hierbei handelt es sich meist um abstraktere Anforderungen, die typischerweise nicht in einzelnen RFCs oder Teilen des Geräts zu finden sind, sondern eine funktionale Anforderung an das gesamte Gerät darstellen. Im zweiten Beispiel wird empfohlen, dass das Gerät sowohl über IPv4 als auch IPv6 zu konfigurieren sein soll – dabei kommen dann eine Reihe von IPv6-RFCs zum Einsatz sowie zusätzlich IPv4-RFCs, auf die nicht näher eingegangen wird. Einige Empfehlungen werden im Kommentarfeld näher erläutert, wobei auch Bedingungen genannt sein können, unter denen eine Empfehlung relevant ist.

Blatt Knoten:				
	SEND, wenn Einsatz geplant		empfohlen	nur wenige Implementierungen verfügbar
	RFC 3971	Secure Neighbor Discovery (SEND)	verpflichtend	
	RFC 3972	Cryptographically Generated Addresses (CGAs)	verpflichtend	

Abbildung 5: Profil-Beispiel 3 – Bedingung „wenn Einsatz geplant“

Bei Funktionen kann auch eine Bedingung für einen gesamten Funktionsblock angegeben sein. Bspw. ist die IPv6-Funktion SEND (SEcure Neighbor Discovery) zum Betrieb von IPv6 nicht unbedingt nötig, daher sind einige RFCs nur dann zu betrachten, wenn diese Funktion eingesetzt werden soll. Der Einsatz hängt vom Szenario ab, bspw. benötigen nur wenige Systeme eine Unterstützung der Mobilität (Mobile IP).

In anderen Fällen wird der Einsatz von Funktionen durch das Profil empfohlen, insbesondere aus Gründen der Sicherheit. Hat man sich in einem ersten Schritt für den Einsatz einer Funktion entschieden, dann kann danach ein RFC verpflichtend sein, da eine tatsächlich genutzte Funktion Standard-konform realisiert sein muss.

Praktisch bedeutet dies, dass in einem ersten Schritt die Bedingung für den Funktionsblock festgelegt wird, und in einem zweiten Schritt wird dann entweder der gesamte Block gestrichen (Einsatz ist nicht geplant) oder der gesamte Block ist wie jede andere Zeile des Profils zu behandeln, unter Berücksichtigung der normalen Anforderungsgrade des Profils.

Blatt Knoten:				
	RFC 4864	Local Network Protection for IPv6	zur Information	Zusammenstellung entspr. RFCs und nativer IPv6-Eigenschaften

Abbildung 6: Profil-Beispiel 4 – fehlender Anforderungsgrad

Das vierte Beispiel zeigt, dass in Einzelfällen der Anforderungsgrad auch fehlen kann. In diesen Fällen kann die Kenntnis des RFCs hilfreich sein oder er wird bspw. von anderen Profilen referenziert. Handelt es sich bspw. um zusätzliche Informationen, so ist eine Umsetzung des RFCs in einem Gerät im engeren Sinn nicht möglich und daher kann auch kein Anforderungsgrad festgelegt werden. Das Kommentarfeld informiert über den Grund für den fehlenden Anforderungsgrad.

Auch wenn für einen RFC in seiner Gesamtheit kein Anforderungsgrad angegeben ist, können einzelne in diesem RFC beschriebene Funktionen einen Anforderungsgrad besitzen. Dies ist insbesondere der Fall, wenn ein als „informational“ eingestufter RFC trotzdem für einzelne Funktionen eine Empfehlung oder Festlegung enthält, die über andere – in der Regel ältere – RFCs hinausgeht.

Blatt Knoten:					
	IKEv1, wenn Einsatz geplant			empfohlen	zwecks Interoperabilität mit Knoten, die nicht IKEv2-fähig sind
	RFC 2409 (VERALTET!)	IKE version 1 (IKEv1)		verpflichtend	zwecks Interoperabilität mit Knoten, die nicht IKEv2-fähig
			Verwerfen weiterer Antworten nach Erhalt der ersten kryptografisch korrekten Antwort	verpflichtend	

Abbildung 7: Profil-Beispiel 5 – veralteter RFC

Im Profil sind vereinzelt RFCs als veraltet markiert, wie im fünften Beispiel dargestellt. Es lassen sich grob zwei Arten von Nachfolge-RFCs unterscheiden:

- die nahtlose Weiterentwicklung von RFCs, wobei einige Klarstellungen bzw. Fehlerbereinigungen vorgenommen werden und normalerweise der neuere RFC große Teile des alten RFCs weiterhin abdeckt
- die Beschreibung von (zusätzlichen) neuen Protokollen und Funktionen, die inkompatibel zum alten RFC sind oder es wurden wesentliche Erweiterungen vorgenommen

Im Fall der nahtlosen Weiterentwicklung kann man pragmatisch beide RFCs als gleichwertig betrachten. Ggf. wird in der Gerätedokumentation oder in diesem bzw. einem anderen Profil noch auf die alte Version verwiesen. Es gibt aber auch Fälle, in denen neue und wesentlich veränderte Protokollversionen zur Verfügung stehen, die sich aber entweder noch nicht im praktischen Einsatz / in Produkten durchgesetzt haben oder bei denen die alte Protokollversion noch im normalen Betrieb unterstützt werden muss. Wie hier im fünften Beispiel spielt das veraltete Protokoll bzw. der entsprechende RFC eine eigenständige Rolle und wird daher im Profil aufgeführt. Auch veraltete RFCs können mit einem Anforderungsgrad „verpflichtend“ versehen sein, wenn sie zumindest für einige Einsatzszenarien weiterhin relevant sind. Das Kommentarfeld informiert über den Grund für die Nennung des RFCs. Generell sind aktuelle RFCs inklusive ihrer Fehlerberichtigungen („verified errata“) zu verwenden.

4.2. Knoten

Knoten sind das grundlegende Element eines IP-Netzes und stellen im Gegensatz zu Router und Endsystem keine physisch vorhandene und eigenständige Netzkomponente dar, sondern ein abstraktes Element, das die Grundfunktionen der Kommunikation in den realen Netzkomponenten realisiert. Der Vorteil dieser Darstellung liegt darin, dass gleiche Eigenschaften der an einer Kommunikationsbeziehung beteiligten Komponenten hier zusammengefasst werden können. Somit wird die Darstellung vereinfacht und die Herstellung von Interoperabilität zwischen Netzkomponenten wird erleichtert.

Die spezifischen Anforderungen an Knoten gliedern sich in folgende Bereiche:

- die Kommunikation des IPv6-Knotens,
- das Netzwerk- oder Systemmanagement und
- die Link-spezifischen Anforderungen.

4.2.1 Kommunikation des IPv6-Knotens

Zur Kommunikation des Knotens gehören alle Funktionen, um an der Kommunikation in einem IPv6-Netz teilnehmen zu können.

4.2.1.1 Grund-Anforderungen

Die Grundlage der Kommunikation ist die IPv6-Basisspezifikation in RFC 2460. Wird keine auf dem Flow Label des IPv6-Headers basierende Funktionalität genutzt, so muss das Feld ungenutzt bleiben (auf null gesetzt) und ignoriert werden. Wird dagegen eine solche Funktionalität genutzt, so ist die Umsetzung nach RFC 6437 („IPv6 Flow Label Specification“) verpflichtend.

Entsprechend RFC 5722 („Handling of Overlapping IPv6 Fragments“) ist die Verwendung von überlappenden Paket-Fragmenten aus Sicherheitsgründen verboten.

RFC 6540 – IPv6 Support Required for All IP-Capable Nodes beschreibt das Problem, dass der Begriff “IP” in älteren RFCs implizit für IPv4 stand und für IPv6 hauptsächlich eigene RFCs geschaffen wurden. Deshalb ist in einigen Zusammenhängen nicht ganz klar, welche IP-Versionen unterstützt werden müssen. Dieser RFC legt dazu als „Best Practice“ fest, dass

- neue IP-Implementierungen IPv6 unterstützen müssen,
- Updates von bestehenden IP-Implementierungen IPv6 unterstützen sollen,
- die IPv6-Unterstützung bezüglich Funktionalität und Qualität gleichwertig oder besser im Vergleich zur IPv4-Unterstützung sein muss und
- bei IP-Netzfunktionen IPv4/IPv6-Koexistenz angestrebt werden soll, wobei IPv4 für die Funktion nicht notwendig sein darf.

Aus Sicherheitsgründen müssen einzelne ICMPv6-Funktionen konfigurierbar sein, damit die Netzinfrastruktur nicht unnötig offen gelegt wird bzw. keine Denial-of-Service-Attacken möglich sind.

Die Umsetzung und der Einsatz des Neighbor-Discovery-Protokolls (NDP) sind verpflichtend. Zum Schutz gegen böswillige Nachbarn werden allerdings einzelne Anforderungen beim Einsatz von NDP verschärft.

RFC 5942 („IPv6 Subnet Model“) enthält einige Klarstellungen über das IPv6-Subnet-Modell in Zusammenhang mit dem Einsatz von NDP und dient der Information.

Mit Secure Neighbor Discovery (SEND) steht ein Mechanismus zur Verfügung, das automatische Netzwerkmanagement von IPv6 absichert. Der Einsatz von SEND wird empfohlen, auch wenn bisher nur wenige Implementierungen verfügbar sind.

Der Bereich Transfer enthält grundlegende Funktionen zur Kommunikation eines Knotens im IPv6-Netz, die mit der Übertragung von Daten oder der Koordination von Geräten zusammenhängen.

- Eine wesentliche Grundlage für die Funktion von IPv6-Kommunikation ist die Path MTU Discovery, da eine Fragmentierung durch Router nicht vorgesehen ist. Path MTU Discovery muss also von Knoten unterstützt werden, wobei zur Ermöglichung einer sinnvollen, leistungsfähigen Kommunikation der jeweilige Knoten die Verarbeitung von Paketen mit mindestens 1500 Oktetts ermöglichen sollte. Wenn ein Knoten eine „Packet Too Big“ ICMP Nachricht als Antwort auf unfragmentierte, minimal große Pakete <= 1280 Oktetts (festgelegt in RFC 2460) erhält, so soll er einen Fragment Header in diese Pakete einfügen, wie in RFC 2460 und RFC 1981 spezifieziert. Erhaltene Nachrichten, die aus nur einem Fragment bestehen, sollten behandelt werden wie in RFC 6946 (“Processing of IPv6 "Atomic" Fragments”) beschrieben.

- IPv6-Jumbograms sind Pakete bis zu einer theoretischen Größe von 4 GByte, die in Zukunft insbesondere bei Spezialanwendungen zur Übertragung von großen Datenmengen genutzt werden können. Zu beachten ist hierbei, dass herkömmliche Transportprotokolle (z. B. TCP, UDP) diese Paketgrößen bei Weitem nicht erreichen und damit spezialisierte Protokolle zum Einsatz kommen werden. Derzeit sind auch keine Schicht-2-Übertragungsverfahren üblich, die diese Paketgrößen unterstützen.

- Die Router-Advertisement-(RA)-Nachrichten des Neighbor-Discovery-Protokolls (NDP) enthalten ein 8-Bit-Feld für einzelne Flags, mit RFC 5175 („IPv6 Router Advertisement Flags Option“) wird eine Erweiterung definiert, die eine Erweiterung der Flags für zukünftige Anwendungen erlaubt.

- Die IPv6 Router Alert Option nach RFC 2711 basiert auf einem Hop-by-Hop-Header, der Router entlang des Pfads auf eine notwendige Behandlung von Paketen aufmerksam macht. Diese Funktion kann bei bestimmten Protokollen (bspw. RSVP) eine effizientere Behandlung der Pakete in Routern ermöglichen.

4.2.1.2 Header Compression

Unter Header Compression versteht man verschiedene Methoden, die übertragenen Nachrichtenköpfe typischer Internet-Protokolle wie IP (IPv4 oder IPv6), UDP, TCP usw. so kurz wie möglich zu halten. In der Regel wird dabei auf die Übertragung von redundanten Daten verzichtet, d. h. keine Übertragung von Daten, die den jeweiligen Kommunikationspartnern bereits bekannt sind. Ein typisches Beispiel ist der Verzicht auf die explizite Übertragung der Nachrichtenlänge, da diese anhand der Nachrichtenbegrenzungen ermittelt werden kann.

Header Compression erfordert stets den Einsatz zueinander kompatibler Kompressionskomponenten bei allen Kommunikationspartnern. In vielen Fällen verursacht Header Compression einen erhöhten Verarbeitungsaufwand bei den Kommunikationspartnern. Durch den Verzicht auf Daten werden außerdem bestimmte Fehler nicht erkannt (z. B. evtl. ein Segmentverlust bei fehlender Angabe der Nachrichtenlänge).

Header Compression ist für allgemeine Szenarien öffentlicher Verwaltungen optional, da sie nur unter bestimmten Bedingungen, beispielsweise einer sehr geringen verfügbaren Übertragungsrate, nützlich ist.

Das ggf. eingesetzte Verfahren ist in der Regel durch die Verfügbarkeit der entsprechenden Komponenten für die eingesetzten Kommunikationssysteme beeinflusst. Für sehr leistungsschwache Systeme kann auch die Komplexität des Verfahrens bei der Auswahl bestimmend sein.

Das modernste und effizienteste Header-Compression-Verfahren ist Robust Header Compression (ROHC, RFC 5795 und weitere). Dieses Verfahren ist formal in eine Rahmenspezifikation und verschiedene Profile gegliedert.

Ist der Einsatz von ROHC geplant, dann müssen die Rahmenspezifikation RFC 5795 („The RObust Header Compression (ROHC) Framework“) und die Profile für TCP/IP (RFC 4996) sowie für RTP, UDP, IP ESP und UDP-Lite (RFC 5225) unterstützt werden.

Werden die überholten Profile für RTP, UDP, ESP (und unkomprimierte Nachrichten) gemäß RFC 3095 unterstützt, dann ist auch die Implementierung von RFC 4815 („Corrections and Clarifications to RFC 3095“) verpflichtend, RFC 3843 („ROHC Profile for IP“) und RFC 4362 („ROHC: A Link-Layer Assisted Profile for IP/UDP/RTP“) sind optional.

Für den Einsatz über PPP steht mit RFC 3241 („ROHC over PPP“) eine angepasste Variante von ROHC zur Verfügung.

Zwei ältere aber funktionstüchtige Header-Compression-Verfahren sind in RFC 2507 („IP Header Compression“) für Punkt-zu-Punkt-Links und in RFC 2508 („Compressing IP/UDP/RTP Headers for Low-Speed Serial Links“) spezifiziert.

Payload Compression

Neben einer Header Compression ist es auch optional möglich, Payload Compression vorzunehmen, d. h. eine (aus Sicht der betroffenen Anwendung) verlustfreie Komprimierung der Nutzdaten von Nachrichten. (Ein analoges Beispiel aus dem Bereich der Datenspeicherung ist das „Zippen“ von Dateien.)

Für diesen Zweck steht die Rahmenspezifikation RFC 3173 („IP Payload Compression Protocol (IPComp)“) zur Verfügung, die den Einsatz verschiedener konkreter Kompressionsalgorithmen ermöglicht.

Für Payload Compression gelten dieselben Rahmenbedingungen und Konsequenzen wie für Header Compression (geringe Übertragungsrate, höherer Verarbeitungsaufwand).

4.2.1.3 Adressierung

Im Abschnitt „Allgemein“ sind relevante RFCs zu IPv6-Adressen und Adressbereichen zusammengefasst. Aus der IPv6-Adressarchitektur wird die Verwendung von IPv4-mapped Adressen in öffentlichen Netzen nicht empfohlen, Grund sind mögliche Sicherheitsrisiken durch inhärente Mehrdeutigkeit der Adressen.

Die Nutzung von Site-local-Adressen ist nicht mehr erlaubt, mit den Unique-local-Adressen (ULA) steht ein Konzept für ähnliche Anforderungen zur Verfügung.

Für alle Knoten ist die Unterstützung von manueller/statischer Adresskonfiguration als grundlegender Mechanismus verpflichtend (für Endsysteme und bestimmte Klassen von Routern kommen weitere Arten der Adresskonfiguration hinzu).

Für alle Knoten (Ausnahmen für Sicherheitsgeräte siehe entsprechende Tabellenblätter) ist die Implementierung von RFC 4862 („IPv6 Stateless Address Autoconfiguration“) verpflichtend, wobei die Nutzung von Stateless Address Autoconfiguration (automatischer Adresskonfiguration von Endsystemen) abschaltbar und konfigurierbar sein muss. Zu beachten ist hierbei, dass RFC 4862 mehrere Klassen von Funktionen enthält: einerseits einen Mechanismus zur automatischen Adresskonfiguration von Endsystemen, und andererseits wichtige, für den Betrieb von IPv6-Netzen grundlegende Funktionen, die unabhängig von der automatischen Adresskonfiguration sind. Zwei dieser Funktionen sollen hier hervorgehoben werden: Link Local Address Configuration und Duplicate Address Detection. Die automatische Generierung von Link-lokalen Adressen ist eine notwendige Voraussetzung für den Prozess der automatischen Konfiguration von Netzen. Die Duplicate Address Detection (DAD) ist eine verpflichtende Funktion zur Erhaltung der Funktionsfähigkeit des Netzes. In bestimmten Einsatzbereichen, beispielsweise bei Mobile IP, kann optional auch die Optimistic DAD nach RFC 4429 eingesetzt werden.

Steht DHCPv6 zur Verfügung, so ist die Nutzung automatischer Adress-konfiguration entsprechend RFC 4862 nicht empfohlen. Im Fall der Nutzung automatischer Adresskonfiguration kann optional zusätzlich Stateless DHCPv6 genutzt werden, um Informationen über Infrastruktur-Server (wie DNS oder NTP) zu verteilen.

4.2.1.4 DNS-Resolver

Das DNS-System ist in weiten Bereichen nicht IPv6-spezifisch, ist aber aufgrund von Erweiterungen für den Einsatz zusammen mit IPv6 und der grundsätzlichen Bedeutung der Funktionen im Profil aufgeführt. Zu beachten ist, dass nicht alle Knoten einen DNS-Resolver benötigen. Da das aber die Ausnahme ist, wird der Einsatz von DNS als verpflichtend angegeben.

Die Umsetzung der Router-Advertisement-(RA)-Option zur Konfiguration des DNS-Servers nach RFC 6106 ist empfohlen, um zukünftig eine weitgehende Autokonfiguration über RA zu ermöglichen.

Es wird der Einsatz von DNSSEC empfohlen, wenn die Voraussetzungen dafür gegeben sind, da es sich bei DNS um eine kritische Infrastruktur zum Betrieb von IP-Netzen handelt, die es abzusichern gilt.

4.2.1.5 Transitionsmechanismen

Die verschiedenen Transitionsmechanismen zu IPv6 (auch Migration genannt) sind in RFC 4213 („Basic Transition Mechanisms for IPv6 Hosts and Routers“) aufgeführt.

Teredo sollte nur in begründeten Ausnahmefällen eingesetzt werden.

4.2.1.6 NAT-Nachfolge

Die Entwicklung des Internets und seiner Nutzung ließ früh erkennen, dass die Anzahl der IPv4-Adressen nicht mehr ausreichen würde. Das führte im Wesentlichen zu zwei Entwicklungen: den Arbeiten an dem IPv6-Protokoll mit einem wesentlich größeren Adressraum und der Einwicklung von Network Address Translation (NAT) als Brückentechnologie. Während die Einführung von IPv6 bekanntermaßen auf sich warten ließ, zeigte sich, dass der NAT-Mechanismus auch für eine Reihe von anderen Netzwerkproblemen genutzt werden konnte. Wichtige Funktionen von NAT im praktischen Einsatz sind das Verbergen der (Adressen der) lokalen Netzinfrastruktur aus Sicherheitsgründen und die Dauerhaftigkeit der internen IP-Adressen auch bei einem Providerwechsel bzw. bei Multihoming. Allerdings bricht NAT mit dem Ende-zu-Ende-Prinzip, das beim Design der IP-Protokolle vorgesehen ist. Dieses besagt, dass eine Kommunikationsverbindung von den Endsystemen gesteuert und transparent über das IP-Netz abgewickelt wird. Insbesondere kann ein IP-Netz im Wesentlichen zustandslos arbeiten. D. h., für die Funktionsfähigkeit des Netzes ist es nicht erforderlich, Informationen über einen Datenstrom von IP-Paket zu IP-Paket zu speichern bzw. diese IP-Pakete zu verändern. Davon unberührt ist die Verwendung von Proxy oder Application-Layer-Gateway, welche die Protokoll-

schichten berücksichtigen und sich daher logisch einfach in die Kommunikationsinfrastruktur einfügen lassen.

Über das Für und Wider von NAT wurden viele Diskussionen geführt, die hier nicht wiederholt werden sollen. Wichtig zu wissen ist, dass das Ende-zu-Ende-Prinzip eine Grundlage des Designs von IP-Protokollen ist (und damit eine Annahme, auf die sich Protokoll- und Anwendungsentwickler verlassen) und dass NAT andererseits in der Praxis als einfache Funktion zum Lösen von Netzwerkaufgaben eingesetzt wird. Beides zusammen kann in einigen Situationen zu Problemen führen.

Mit IPv6 ist der Einsatz von NAT nicht mehr notwendig. RFC 4864 („Local Network Protection for IPv6") [RFC4864] beschreibt eine Reihe von IPv6-Mechanismen und wie diese zur Lösung von Netzwerkaufgaben eingesetzt werden können. Hilfreich ist dabei die Gegenüberstellung des zu erreichenden Zwecks, der entsprechenden NAT-Funktion bei IPv4 sowie des entsprechenden Mechanismus bei IPv6.

Mit RFC 6296 („IPv6-to-IPv6 Network Prefix Translation") [RFC6296] steht nach langer Diskussion ein mit NAT verwandter Mechanismus auch für IPv6 zur Verfügung, dessen Einsatz aber nicht empfohlen wird. Die üblichen Netzwerkaufgaben lassen sich mit anderen IPv6-Mechanismen lösen. So wird die Dauerhaftigkeit der IP-Adressen über das Adressschema der ÖV sichergestellt. Die interne Adress- und Netzstruktur ist durch das üblicherweise eingesetzte ALG bzw. Proxy oder Reverse-Proxy nicht sichtbar.

4.2.1.7 IPsec-Protokollfamilie

Zur Absicherung der Kommunikation wird der Einsatz von IPsec empfohlen. Die vorherrschende Verwendung ist der Aufbau von Tunneln zwischen verschiedenen Netzen oder Teilnetzen.

Die aktuelle, empfohlene Version von IPsec („IPsec v3") ist in RFC 4301 („Security Architecture for the Internet Protocol") [RFC4301] definiert.

Eine IPsec Security Association (SA), welche gleichzeitig IPv4 und IPv6 Subnetze koppelt, ist verboten. IPv4- und IPv6-IPsec-Verbindungen müssen jeweils einen eigenen Sessionkey in eigenen SAs verwenden. Dies schließt nicht den Transport von IPv4 in IPv6 oder IPv6 in IPv4 im IPsec-Tunnelmodus ein. Diese Betriebsart ist explizit empfohlen.

Mit dem Einsatz von IPsec in der aktuellen Form ist auch IKEv2 verbunden. In speziellen Szenarien ist der Einsatz von IKEv1 möglich, insbesondere auch, wenn die Interoperabilität mit Knoten sichergestellt werden soll, die noch nicht IKEv2-fähig sind.

Optional ist auch der Betrieb von IPsec-v2 möglich.

Zum Einsatz von kryptografischen Algorithmen gibt das vorliegende Profil nur eine Übersicht über mögliche Standards, bei der konkreten Auswahl und

Konfiguration ist die Technische Richtlinie TR-02102 („Kryptographische Verfahren: Empfehlungen und Schlüssellängen“) des BSI [TR02102] zu beachten. Dabei muss sichergestellt sein, dass die aktuellste Version dieser Richtlinie genutzt wird.

4.2.1.8 Multicast

Im Profil wird Multicast in seiner Rolle als notwendiger Basis-Mechanismus für das IPv6-Netzwerkmanagement betrachtet. Diese Sichtweise umfasst derzeit nicht die Verwendung von Multicast aus Anwendungssicht, bspw. für Multimedia-Anwendungen.

Zur Unterstützung von Multicast Listener Discovery (MLD) ist eine der Spezifikationen RFC 3810, RFC 5790 oder RFC 2710 erforderlich und damit verpflichtend. Priorität hat MLDv2 (RFC 3810), das die Funktionalität von MLDv1 (RFC 2710) um Source-Specific Multicast erweitert. Lightweight MLDv2 (RFC 5790) ist eine vereinfachte Teilmenge von MLDv2 ohne ‚Exclude‘-Funktionalität (Ausschließen von Paketen von unerwünschten Source-Adressen). Wenn MLDv1 (RFC 2710) benutzt wird, ist RFC 3590 („Source Address Selection for MLD“) verpflichtend und alle Knoten auf dem gleichen Link müssen den MLDv1-Modus anwenden.

4.2.1.9 Dienstgüte (Quality-of-Service, QoS)

Im Bereich der Dienstgüte kommen verschiedene Verfahren zum Einsatz, allerdings zumeist lokal begrenzt, in einzelnen administrativen Bereichen oder im Übergang zu einem ausgewählten Provider aufgrund von Absprachen. Nur der Einsatz von DiffServ hat eine nennenswerte Verbreitung, insbesondere über rückwärts-kompatible Funktionen zur Nutzung des TOS-Feldes, wie es bei IPv4 im Header definiert war.

4.2.2 Netzwerk-/System-Management

Generell ist der Einsatz von Netzwerk-Management über SNMP für alle Knoten empfohlen. Der Betrieb des Netzwerk-Management-Systems über IPv4 oder IPv6 ist dabei zunächst einmal unabhängig von dem IPv6-Einsatz des Knotens, d. h., auch wenn der Knoten im IPv6-Wirkbetrieb arbeitet, können die entsprechenden Informationen mittels IPv4 über die Netzwerk-Management-Schnittstelle abgefragt werden. Für Neubeschaffungen ist die Möglichkeit der Nutzung von SNMP über IPv6 verpflichtend. Für den normalen Betrieb ist nur die passive Nutzung des Netzwerk-Management-Systems vorgesehen, d. h., das Auslesen von Informationen bspw. zur Aufbereitung eines Netzstatus. Aus Sicherheitsgründen ist das Setzen von Werten via Netzwerk-Management nur zulässig, wenn es notwendig ist.

Im Profil des Knotens werden einzelne, standardisierte MIBs für den Einsatz empfohlen. Grundsätzlich ist darauf zu achten, dass auch die Hersteller-spezifischen Erweiterungen der MIB für den Einsatz von IPv6 erweitert worden und verfügbar sind.

4.2.3 Link-spezifische Anforderungen

Der Netzzugang eines Knotens kann ganz allgemein über folgende Mechanismen erfolgen:

- direkte Verwendung von Datenübertragungsprotokollen
- Verwendung von virtuellen Links und Tunneln
- Verwendung von komplexen Zugangsnetzen, wie Mobilfunk

In diesem Abschnitt des Knotens sind typische Netzzugangstechnologien aus dem LAN- oder WAN-Bereich zu Referenzzwecken erwähnt, wobei die Aufzählung nicht vollständig ist. Ein Knoten wird nur die Technologien realisieren, die auch verwendet werden sollen.

Weitere Link-spezifische Anforderungen sind für den Router angegeben.

4.3. Router

Router sind wesentliche Komponenten jeder Netzwerkinfrastruktur. Ein Router ist ein Vermittlungsrechner, der Knoten und ganze Netze auf IP-Ebene koppelt. Er trifft Wegewahlentscheidungen anhand von Daten der IP-Ebene (OSI Layer 3), i. d. R. Regel basierend auf der Ziel-IP-Adresse.

Die spezifischen Anforderungen an Router gliedern sich in folgende Bereiche:

- die Kommunikation des Routers,
- die eigentlichen Routerfunktionen,
- die Funktionen zum Netzwerk- oder System-Management und
- die Link-spezifischen Anforderungen.

4.3.1 Kommunikation des Routers

Zur Kommunikation des Routers gehören alle Funktionen, die ein Router unterstützen muss, um selbst an der Kommunikation in einem IPv6-Netz teilnehmen zu können, und die Funktionen, die für das Management und den Schutz dieser Kommunikation erforderlich sind.

4.3.1.1 Grundanforderungen

Für Router muss das Antwortverhalten mit ICMP-Error-Nachrichten konfigurierbar sein, da zu viele derartige Nachrichten das Netz und den sendenden Router überlasten können.

Eine konkrete Konfigurationsalternative ist beispielsweise die Begrenzung der Rate solcher Nachrichten, bis hin zur (zeitweiligen) Abschaltung der überlasteten Funktion. Ein nicht konfigurierbares Antwortverhalten wäre ein Risiko für die Betriebssicherheit, da Angreifer vorsätzlich den Versand zu vieler ICMP-Error-Nachrichten verursachen könnten.

Auf allen Links sollte der MTU-Wert in Router-Advertisement-Nachrichten mit geschickt werden können, da auf diese Weise eine aufwändigere Ermittlung vermieden werden kann.

Zur Erkennung beabsichtigten oder auf Fehlern beruhenden Fehlverhaltens anderer Router sollte es möglich sein, inkonsistente Router-Advertisement-Nachrichten aufzuzeichnen. Inkonsistenzen können sich in widersprüchlichen Nachrichten eines oder mehrerer Router wiederspiegeln, ebenso können derartige Nachrichten „permanentem Wissen“ des aufzeichnenden Routers entgegenstehen.

Jumbogramme sollten von allen Routern unterstützt werden, da dies die Zukunftsfähigkeit dieser zentralen Komponenten verbessern kann.

4.3.1.2 Adressierung

Die Verwendung von 127-Bit-Präfixen auf Punkt-zu-Punkt-Links (gemäß RFC 6164) schränkt die Möglichkeit für Angriffe durch verdeckte Kanäle ein und muss daher unterstützt werden. Diese Funktion entspricht den 31-Bit-Präfixen, die unter IPv4 verbreitet sind.

SOHO-Router müssen automatische Konfiguration unterstützen, da diese in der Regel über den Internet-Dienstanbieter erfolgt. Zu diesem Zweck kann es erforderlich sein, dass ein SOHO-Router als DHCPv6-Klient gemäß RFC 3315 („Dynamic Host Configuration Protocol for IPv6 (DHCPv6)“) agieren kann. Ansonsten wird diese Art der Adresskonfiguration von Routern über DHCP nicht empfohlen. Wenn ein CE-Router sein Präfix über DHCP erhält, muss er RFC 3633 („IPv6 Prefix Options for DHCPv6“) unterstützen.

Es wird empfohlen, Privacy Extensions für die Adresskonfiguration von Routern gemäß RFC 4941 („SLAAC Privacy Extensions“) nicht zu verwenden, da Router für eine ordnungsgemäße Nutzbarkeit eine dauerhaft gültige Adresse benötigen.

4.3.1.3 DNS

SOHO-Router müssen DNS-Konfigurationsdaten mittels Router Advertisements gemäß RFC 6106 („IPv6 Router Advertisement Options for DNS Configuration“) verbreiten können.

4.3.1.4 Transitionsmechanismen

CE-Router müssen Generic Routing Encapsulation (GRE), wie in RFC 2784 („Generic Routing Encapsulation“) spezifiziert, und die spezielle Ausprägung der Kapselung in IPv6 nach RFC 2473 („Generic Packet Tunneling and IPv6“) unterstützen. Wenn kein VPN-Krypto-Gateway zusätzlich zum Einsatz kommt, gilt dies nach RFC 4891 („Using IPsec to Secure IPv6-in-IPv4 tunnels“) auch für IPsec im Transportmodus für IPv4-Tunnel, die IPv6-Pakete transportieren. In diesem Kontext sollten auch die Schlüssel- und Nummerierungserweiterungen zu GRE entsprechend RFC 2890 („Key and Sequence Number Extensions to GRE“) verfügbar sein.

4.3.1.5 IPsec-Protokollfamilie

Es gelten die Empfehlungen für Knoten.

4.3.1.6 Multicast

Wenn der Einsatz von Protocol Independent Multicast (PIM) geplant ist, sollte PIM – Sparse Mode (PIM-SM) nach RFC 4601 („PIM – Sparse Mode (PIM-SM)“) implementiert sein, sofern Source-Specific Multicast (SSM) verwendet werden soll. Ist die Verwendung von SSM nicht geplant, kann PIM-SM oder PIM – Dense Mode (PIM-DM) gemäß RFC 3973 („PIM – Dense Mode (PIM-DM)“) gewählt werden. Die Unterstützung von Rendezvous-Point-Adressen in Multicast-Adressen (für PIM-SM Any-Source Multicast entsprechend RFC 3956 („Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address“) ist optional.

4.3.1.7 Dienstgüte (Quality of Service, QoS)

Es gelten die Empfehlungen für Knoten.

4.3.1.8 Home Agent für Mobile IP

Soll der Router als Home Agent (HA) für Mobile IP eingesetzt werden, ergeben sich daraus einige Anforderungen:

- Die Home-Agent-Funktionen gemäß RFC 6275 („Mobility Support in IPv6“) sowie RFC 3776 („Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents“) und RFC 4877 („Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture“) müssen implementiert sein.

- Es wird empfohlen, RFC 4282 („The Network Access Identifier“), RFC4283 („Mobile Node Identifier option for MIPv6“) und RFC 5555 („Mobile IPv6 Support for Dual Stack Hosts and Routers“) ebenfalls zu unterstützen.

Es ist nicht abschließend und einheitlich festgelegt, ob Network Access Identifier oder andere Dienstanbieter-unabhängige Identifier für mobile Endgeräte im Kontext öffentlicher Verwaltungen genutzt werden. Trotzdem sollte ein Home Agent entsprechend vorbereitet sein, da die Nutzung Dienstanbieter-unabhängiger Identifier Sicherheitsvorteile bringen kann.

Da noch für längere Zeit zu erwarten ist, dass einem mobilem Endgerät je nach lokalen Gegebenheiten IPv6 oder IPv4 als native IP-Version zur Verfügung steht, sollte der zuständige Home Agent eine einheitliche und durchgängige Unterstützung für beide Protokollversionen bieten.

4.3.1.9 Mobiler Router

Mobile Router müssen RFC 3963 („Network Mobility (NEMO) Basic Support“) unterstützen.

4.3.2 Routerfunktionen

Die *Routerfunktionen* umfassen im Wesentlichen die unterschiedlichen Routingprotokolle, die in Abhängigkeit von den lokalen Gegebenheiten und der Rolle des Routers im Netz (Zugangsrouter oder netzinterner Router) zum Einsatz kommen können.

4.3.2.1 Grundanforderungen

In einem Netz, in dem DHCP über Link-Grenzen hinweg eingesetzt werden soll, muss jeder Router die DHCPv6-Relay-Funktion gemäß RFC 3315 unterstützen, da ansonsten DHCP-Nachrichten ihr Ziel nicht erreichen können.

4.3.2.2 Routingprotokolle

Es gibt eine Anzahl verschiedener Routingprotokolle, die alternativ oder in Abhängigkeit von der Rolle eines Routers auch gleichzeitig zum Einsatz kommen können.

Für Router an administrativen Grenzen, sogenannte Exterior Router oder CE Router (Customer Edge Router), gilt:

- Sie müssen das Border Gateway Protocol 4 (BGP-4, RFC 4271) sowie die darauf bezogenen Dokumente RFC 1772 („Application of the Border Gateway Protocol in the Internet“), RFC 4760 („Multiprotocol Extensions for BGP-4“) und RFC 2545 („Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing“) unterstützen. Erst RFC 4760 und RFC 2545 spezifizieren die notwendige Erweiterung des Protokolls zur Unterstützung von IPv6, während RFC 4271 und RFC 1772 ursprünglich nur für den Einsatz in einer reinen IPv4-Umgebung ausgelegt waren.

- RFC 5492 („Capabilities Advertisement with BGP-4“) sollte implementiert sein, damit die Router sich gegenseitig über ihre Fähigkeiten informieren und daraufhin die Abläufe zwischen sich entsprechend optimieren können.

- Es wird empfohlen, RFC 2918 („Route Refresh Capability for BGP-4“) zu unterstützen, der die erneute Anforderung bestimmter Routingdaten ermöglicht, die benachbarte Systeme zuvor bereits bekannt gegeben hatten.

- Um BGP-4 effizient verwenden und Routingtabellen effizient führen zu können, wird empfohlen, RFC 1997 („BGP Communities Attribute“) zu unterstützen. Damit kann die Verteilung von Routingdaten adressunabhängig entsprechend administrativer Anforderungen gesteuert werden. Ebenso wird empfohlen, RFC 5701 („IPv6 Address Specific BGP Extended Community Attribute“) zu unterstützen. Dieser spezifiziert eine größere Anzahl unterschiedlicher Community Identifier und eine Typisierung derselben und ermöglicht damit eine noch genauere Unterscheidung verschiedener „Communities“ und eine einfachere Filterung (nach Typ).

Der potenzielle Nutzen einer BGP- und MPLS-basierten Unterstützung virtueller privater Netze (VPNs) in und durch öffentliche Verwaltungen konnte noch nicht ermittelt werden. Insbesondere wäre eine solche Lösung mit anderen Alternativen im Hinblick auf Sicherheitsaspekte zu vergleichen.

Als internes Routingprotokoll innerhalb einer administrativen Domäne stehen mehrere Alternativen – Routing Information Protocol Next Generation (RIPng, RFC 2080), Open Shortest Path First (OSPF, RFC 5340 in Verbindung mit RFC 2328) und IS-IS (RFC 5308 in Verbindung mit RFC 1195 und RFC 5305 sowie mit ISO/IEC 10589:2002) – zur Verfügung. Die Auswahl ist dem Betreiber der jeweiligen Domäne überlassen und technisch unabhängig von den in anderen – insbesondere benachbarten – Domänen eingesetzten Verfahren.

- RIPng:
  RIPng für den Einsatz in einer IPv6-Umgebung ist vollständig in RFC 2080 („RIPng for IPv6“) beschrieben.

- OSPF:
  OSPF für den Einsatz in einer IPv6-Umgebung ist in RFC 5340 („OSPF for IPv6“) als Ergänzung / Änderung zu OSPF Version 2 (für IPv4, RFC 2328) beschrieben.

  Um die Verarbeitung von Routing-Nachrichten, die von unberechtigten Systemen stammen, zu verhindern, müssen die Nachrichten mindestens durch Authentifizierungsdaten entspr. RFC 4552 („Authentication/ Confidentiality for OSPFv3“) geschützt sein. RFC 4552 setzt die Verfügbarkeit von IPsec voraus.

- IS-IS:
  IS-IS in einer IPv6-Umgebung ist in RFC 5308 („Routing IPv6 with IS-IS“) als Ergänzung zu RFC 1195 („Use of OSI IS-IS for Routing in TCP/IP and Dual Environments“) in Verbindung mit RFC 5305 („IS-IS Extensions for Traffic Engineering“) beschrieben.

  RFC 1195 wiederum enthält lediglich Ergänzungen / Änderungen zu ISO/IEC 10589:2002 („Intermediate System to Intermediate System intra-domain routing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode network service” (ISO 8473)) und muss daher für IS-IS-Unterstützung ebenfalls implementiert sein.

4.3.2.3 Virtual Router Redundancy Protocol (VRRP)

Router innerhalb eines physischen Broadcast-LAN, also beispielsweise eines Ethernet- oder WLAN-basierten Netzes, können unter bestimmten Bedingungen die Aufgaben ausgefallener Router automatisch übernehmen.

RFC 5798 („Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6“) spezifiziert ein Protokoll zur Konfiguration und Durchführung einer solchen Aufgabenübernehme ohne Einbeziehung der betroffenen Endsysteme.

Da das Verfahren nach RFC 5798 deutlich schneller reagiert als die Neighbor- bzw. Router-Discovery-Verfahren, dabei außerdem weniger Kommunikationsaufwand und keine Maßnahmen der Endsysteme erfordert, ist seine Verfügbarkeit vorteilhaft.

4.3.3 Netzwerk-/System-Management

Die *Managementfunktionen* ermöglichen insbesondere die entfernte Abfrage von Daten, die auf dem Router über die abgewickelte Kommunikation gesammelt werden.

4.3.3.1 SNMP

Wenn SNMPv3 gemäß RFC 3410 („Simple Network Management Protocol version 3“) und folgenden eingesetzt werden soll, muss im Router auch RFC 3414 („SNMP User based Security Model“) implementiert sein, denn das Abfragen und insbesondere das Setzen von Routerparametern sind sicherheitskritische Funktionen, die gegen unbefugte Nutzung geschützt sein müssen.

Das Format, in dem – speziell bei Verwendung von SNMP – Managementdaten angegeben werden müssen, ist in Management Information Bases (MIBs) spezifiziert. Router, die SNMP unterstützen, müssen RFC 4293 („Management Information Base for the Internet Protocol (IP)“) und RFC 4292 („IP Forwarding Table MIB“) ebenfalls unterstützen.

Sofern IP Tunneling eingesetzt werden soll, muss in den entsprechenden Routern RFC 4087 („IP Tunnel MIB“) implementiert sein. Soll ein Router als Mobile IP Home Agent oder – seltener – als mobiler Knoten oder als Correspondent Node (Kommunikationspartner eines mobilen Knotens) eingesetzt werden, dann ist die Implementierung von RFC 4295 („Mobile IPv6 Management Information Base“) verpflichtend.

Die Unterstützung des RFC 3289 („Management Information Base for the Differentiated Services Architecture“) ist optional.

Wenn ein Router als RMON Agent (Remote Network Monitoring Agent) eingesetzt werden soll, muss RFC 3919 („Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)“) implementiert sein.

4.3.3.2 IPFIX / Netflow

Ist der Einsatz von IPFIX / Netflow geplant, dann müssen Templates mit IPv6 Information Elements (IE) zur Verfügung stehen. Diese müssen vom Anbieter des genutzten Exporters bereitgestellt werden.

4.3.4 Link-spezifische Anforderungen

Die *Link-spezifischen Anforderungen* beschreiben, welche Standards, Empfehlungen (beispielsweise der ITU[12]) oder RFCs für die verschiedenen Linktypen gelten. Dabei wurden speziell die Anschlüsse an Zugangsnetze betrachtet, da dort eine große Vielfalt im Einsatz ist.

Zu den Link-spezifischen Anforderungen werden keine Bewertungen abgegeben, da sie einerseits – bezüglich der virtuellen Links – stark von den Bedürfnissen und der Nutzung des Netzes abhängen, in dem ein betrachteter Router eingesetzt wird, andererseits – bezüglich der Zugangsnetze – werden sie von den Betreibern der Zugangsnetze vorgegeben.

Weitere Link-spezifische Anforderungen sind für den Knoten angegeben.

4.3.4.1 Virtuelle Links

Virtuelle Links in einem Router können

- IPv6-Kommunikation über eine (teilweise) nur IPv4-fähige Infrastruktur – beispielsweise ein IPv4-Zugangsnetz – ermöglichen, z. B. gemäß RFC 4213 („Basic Transition Mechanisms for IPv6 Hosts and Routers“) oder RFC 5969 („IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) – Protocol Specification“),
- verschiedene Schicht-3-Protokolle über eine IPv6-Infrastruktur unterstützen, wie dies in RFC 2473 („Generic Packet Tunneling in IPv6 Specification“) spezifiziert ist und
- die Effizienz der Weiterleitung von Nachrichten erhöhen, beispielsweise durch das in RFC 3031 („Multiprotocol Label Switching Architecture“) beschriebene Verfahren, bei dem nicht für jedes Paket in jedem Router eine unabhängige Wegewahl durchgeführt wird, sondern Pakete vorkonfigurierten Routen zugeordnet werden.

4.4. Endsystem

Endsysteme sind die Endpunkte der Kommunikation, wobei sich eine Vielzahl von Geräteklassen unterscheiden lassen: Der PC am festen Arbeitsplatz in der Verwaltung, Notebooks mit mobilem Zugang, interne Server für Infrastrukturdienste und Server für den Betrieb von Diensten und Fachanwendungen.

Das Profil des Endsystems basiert auf dem Profil des Knotens, entsprechend finden sich in vielen Bereichen Hinweise auf Anforderungen an den Knoten.

4.4.1 Kommunikation des Endsystems

Zur Kommunikation des Endsystems gehören alle Funktionen, um an der Kommunikation in einem IPv6-Netz teilnehmen zu können.

[12] International Telecommunication Union

4.4.1.1 Grund-Anforderungen

Aus Sicherheitsgründen muss ein Endsystem so konfiguriert werden können, dass es nicht auf Redirect-Nachrichten des Neighbor-Discovery-Protokolls (NDP) reagiert.

Das beim Betrieb von IPv6 notwendige Verfahren Path MTU Discovery kann am Endsystem auch über vorhandene Protokolle auf höheren Schichten realisiert werden, wie es in RFC 4821 beschrieben ist.

4.4.1.2 Adressierung

Die Auswahl der Absenderadresse sollte über eine konfigurierbare Regeltabelle bestimmt werden können.

Jedes Endsystem muss neben der manuellen/statischen Adresskonfiguration, wie sie für jeden Knoten gefordert ist, auch automatische Adresskonfiguration unterstützen. Die Verfahren sind SLAAC oder DHCPv6.

Die Implementierung von Privacy Extensions nach RFC 4941 ist für Endsysteme verpflichtend.

Für hinreichend große Netze wird der Einsatz von DHCPv6 empfohlen. Beim Einsatz von DHCPv6 muss das Endsystem die DHCP-Klientenfunktion implementieren und es ist aus Sicherheitsgründen verpflichtet, DHCP-Optionen zu verwerfen, die für den jeweiligen Nachrichtentyp nicht vorgesehen sind.

4.4.1.3 DNS

Wird der Einsatz von DHCPv6 geplant, so muss auch die DHCPv6-Option zur Konfiguration des DNS-Servers unterstützt werden.

4.4.1.4 Mobile IPv6

Die Unterstützung von Mobile IP bezieht sich im Tabellenblatt „Endsystem“ auf zwei Klassen von Geräten, die im Folgenden unterschiedenen werden:

- Endsysteme, die mit mobilen Endsystemen kommunizieren
- Mobile Endsysteme

4.4.1.5 Nicht mobiles Endsystem, das mit mobilen Endsystemen kommunizieren kann

Die Kommunikation zwischen einem nicht mobilen und einem mobilen Endsystem, die Mobile IPv6 verwenden, kann optimiert werden, wenn das nicht mobile Endsystem den Route-Optimization-Mechanismus in Kapitel 8.2 von RFC 6275 („Mobility Support in IPv6“) unterstützt.

In diesem Fall kann das mobile Endsystem – sofern keine Sicherheitsbedenken bestehen – zulassen, dass die Kommunikation direkt zwischen den beiden Endsystemen abgewickelt wird, ohne dass der Home Agent des mobilen Endsystems stets als Vermittler benutzt wird. Dem nicht mobilen Endsystem wird

zu diesem Zweck die jeweils aktuelle direkte IPv6-Adresse (Care-of-Adresse) des mobilen Endsystems mitgeteilt.

Die Unterstützung des Route-Optimization-Mechanismus wird empfohlen.

4.4.1.6 Mobiles Endsystem

Für die Kommunikation mit mobilen Geräten steht Mobile IPv6 zur Verfügung. Dies ist in RFC 6275 („Mobility Support in IPv6“) spezifiziert. Ein entsprechendes mobiles Endsystem muss die in Kapitel 8.5 dieses RFCs beschriebenen Funktionen implementieren.

Mobile Endsysteme sollten den oben beschriebenen Route-Optimization-Mechanismus ebenfalls unterstützen, da er nur genutzt werden kann, wenn er von allen an einer Kommunikation beteiligten Endsystemen und Home Agents (siehe Kapitel 4.3) bereitgestellt wird.

Die in RFC 6275 spezifizierten Home-Agent-Funktionen werden in einem Endsystem nicht benutzt, eine Implementierung ist daher überflüssig.

Für das Management der Kommunikation mit mobilen Endsystemen müssen diese vertrauenswürdig – und je nach Bedarf auch vertraulich – Daten mit ihrem Home Agent (einer Komponente auf einem Router des Heimatnetzes) austauschen können. Dazu ist die Implementierung von RFC 3776 („Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”) und von RFC 4877 („Mobile IPv6 Operation With IKEv2 and the Revised IPsec Architecture“) verpflichtend.

Da mobile Endsysteme häufig auch in Netzen unterschiedlicher Betreiber eingesetzt werden, sollten sie RFC 4283 („Mobile Node Identifier option for MIPv6“) und RFC 4282 („The Network Access Identifier“) unterstützen, die eine von der Heimat-IPv6-Adresse des Endsystems unabhängige Identifikation von Gerät oder Nutzer – beispielsweise für Abrechnungszwecke – ermöglicht.

Da Mobile IPv6 ursprünglich nur für die Unterstützung von IPv6 ausgelegt war, jedoch mit wenigen Ergänzungen auch für IPv4 eingesetzt werden kann, empfiehlt es sich, eine gemeinsame Protokollspezifikation für beide IP-Varianten zu verwenden. Die erforderlichen Ergänzungen sind in RFC 5555 („Mobile IPv6 Support for Dual Stack Hosts and Routers“) beschrieben und sollten von mobilen Dual-Stack-Endsystemen implementiert werden.

4.4.2 Anwendungs-Unterstützung

Auf Endsystemen spielen nicht nur die direkten Netzfunktionen für die Funktionsfähigkeit unter IPv6 eine Rolle, sondern auch der umfangreiche Bereich der auf den Endsystemen laufenden Anwendungen, muss an bestimmten Stellen IPv6 unterstützen. Beispiele sind die Eingabemasken für IP-Adressen, insbesondere bei Web-Browsern, oder die Größe von internen Datenfeldern zum Speichern dieser Adressen. In diesem Abschnitt des Endsystems-Profils ist eine Reihe von RFCs aufgelistet, die APIs beschreiben, bei denen eine IPv6-Unterstützung

notwendig ist. Diese RFCs sind verpflichtend, wenn entsprechende Funktionen von Anwendungen genutzt werden, beispielsweise über den Zugriff auf Software-Bibliotheken.

Verwendet die Anwendung Multicast-Kommunikation, dann sind von den Anwendungen die genannten RFCs für die Auswahl und Nutzung der Multicast-Adressen zu berücksichtigen.

4.4.3 Netzwerk-/System-Management

Das Netzwerk und System-Management wird durch das Knoten-Profil beschrieben. Es wird empfohlen, insbesondere bei Servern die Host Resource MIB gemäß RFC 2790 zu verwenden, über die aktuelle Leistungsdaten des Endsystems abgefragt werden können. Allerdings sind diese Angaben nicht IPv6-spezifisch.

4.5. Sicherheitskomponenten

Unter dem Begriff Sicherheitskomponenten sind verschiedene Komponenten zusammengefasst:

- Paketfilter
- Application-Layer-Gateways
- VPN-Krypto-Gateways
- Intrusion-Detection/Prevention-Systeme (IDS, IPS)

Im Folgenden werden nur Empfehlungen und Bewertungen für die spezifische Funktionalität der jeweils betrachteten Komponente (also für Paketfilter bzgl. der Paketfilter-Funktion) gegeben. Komponenten, die daneben weitere Funktionen erfüllen (z. B. als Endsystem oder Router), müssen zusätzlich die Anforderungen der entsprechenden Geräteklasse(n) erfüllen.

Die spezifische Funktionalität von Sicherheitskomponenten ist (bisher) kaum in RFCs oder anderen Standards spezifiziert. Deshalb weichen sowohl die entsprechenden Blätter der Profilmatrix als auch diese Beschreibung deutlich von denen der Basis-Netzkomponenten (Endsysteme und Router) ab. Empfehlungen für diesen Bereich wurden um Erkenntnisse aus Untersuchungen zur IPv6-Sicherheit ergänzt [Cho09].

Die Funktionalität von IPv6-Paketfiltern und Application-Layer-Gateways ist durch lokale Funktionen in den entsprechenden Sicherheitskomponenten bestimmt, die von VPN-Krypto-Gateways durch bilaterale, teilweise proprietäre Protokolle zwischen miteinander kommunizierenden Gateways. Daher beschreiben die entsprechenden Blätter der „Profilmatrix“ vornehmlich notwendige bzw. wünschenswerte (beobachtbare) Fähigkeiten derartiger Komponenten, weniger, wie diese Fähigkeiten konkret implementiert sind.

Insbesondere für Sicherheitskomponenten wird darauf hingewiesen, dass bestimmte Funktionen bewusst nicht implementiert werden, da eine Vielzahl von Funktionen die Angriffsfläche erhöhen kann. In der Praxis muss darauf geachtet werden, dass ein Gerät dem Einsatzszenario entspricht. Daher kann es bei Sicherheitskomponenten zu gewollten Abweichungen von den Profilen kommen.

Auf Intrusion-Detection/Prevention-Systeme wird hier wegen der Vielfalt der Ansätze nicht eingegangen.

4.5.1 Allgemeine Anforderungen an Sicherheitskomponenten

Sicherheitskomponenten sind Transitsysteme, d. h., sie leiten eingehende Datenpakete weiter, wenn diese als unbedenklich eingestuft oder entsprechend geändert wurden.

Allen Transitsystemen gemein sind die Funktionskategorien:

- Allgemein
- Kommunikation des Transitsystems
- Netzwerk-/System-Management
- Unterstützung des Transitverkehrs
- Selbstschutz bei der Ausführung der spezifischen Schutzfunktionen

Es kann aufgrund von Sicherheitsanforderungen zu Abweichungen zwischen den inm IPv6-Profil beschriebenen Anforderungen und konkreten Funktionen von Sicherheitsgeräten kommen. Klären sSie die Einzelheiten mit dem jeweiligen Hersteller ab. Das Profil kann dabei in seiner Rolle als „Checkliste“ den Austausch unterstützen.

Allgemein gilt, dass die Funktionen und die Leistung einer IPv6-Sicherheits-komponente mindestens denen einer (vorhandenen) entsprechenden IPv4-Sicherheitskomponente in der konkreten Einsatzumgebung entsprechen sollten.

Bei einer Migration eines IPv4-Netz wird empfohlen, zunächst zu analysieren, welche Funktionen der Sicherheitskomponenten aus der IPv4-Konfiguration auf IPv6-Sicherheitskomponenten ausgedehnt werden sollten, um eine mindestens gleichwertige Funktionalität bei IPv6-Nutzung gegenüber der IPv4-Nutzung sicherzustellen.

Diese Analyse ist umso wichtiger, als die eigentlichen Sicherheitsfunktionen meistens nicht in Standards oder RFCs beschrieben sind und von den Herstellern mit individuellen Mechanismen und in unterschiedlichem Umfang implementiert werden.

Hier wird bei den *Funktionen der Sicherheitskomponenten* zwischen ihren generellen Kommunikationsfunktionen, der Unterstützung des Transitverkehrs,

den von der Komponente unterstützten Netzwerk-/System-Management-funktionen und den eigentlichen Schutzfunktionen unterschieden.

Kommunikationsfunktionen muss eine Sicherheitskomponente bereitstellen, um an der Kommunikation im IPv6-Netz teilnehmen zu können. Die Anforderungen entsprechen weitgehend denen an IPv6-Knoten, die in Abschnitt 4.2.1 erläutert sind.

Solange vertrauenswürdige Neighbor Discovery (z. B: mittels SEND) noch nicht verfügbar ist, sollten Sicherheitsgeräte eingehende Router Advertisements nicht umsetzen. Eine Fehlleitung des Datenverkehrs kann gerade in der Nähe zentraler Komponenten wie bspw. Sicherheitsgeräten gravierende Auswirkungen auf die Leistung und die Sicherheit eines Netzes haben.

Für Punkt-zu-Punkt-Links ist zur Verhinderung verdeckter Kanäle die Unterstützung von RFC 6164 („Using 127-Bit IPv6 Prefixes on Inter-Router Links“) verpflichtend.

Die Unterstützung von RFC 4862 („IPv6 Stateless Address Autoconfiguration“) ist nicht verpflichtend, jedoch wird empfohlen, die folgenden Funktionen zu unterstützen:

- Abschaltbarkeit von Address Autoconfiguration
- entsprechend die dauerhafte Setzbarkeit des „Managed address configuration“- und des „Other stateful configuration“-Kennzeichens in IPv6-Nachrichten
- Konfiguration der Link-local-Adressen mittels SLAAC
- Erkennung mehrfacher Adressvergabe (Duplicate Address Detection) mittels SLAAC
- Entsprechend Abschaltbarkeit der Erkennung mehrfacher Adressvergabe für Multicast-Schnittstellen mittels SLAAC

Nicht empfohlen wird allerdings, andere als Link-lokale Adressen tatsächlich mittels SLAAC zu konfigurieren.

Die *Unterstützung des Transitverkehrs* umfasst die zusätzlich erforderlichen Funktionen, um die die Sicherheitskomponente passierenden, zugelassenen Nutz- und Steuerdaten anforderungs- und protokollgemäß weiterleiten zu können. Dazu gehören:

- die empfohlene Unterstützung von Jumbogrammen,
- die Unterstützung der Neighbor Discovery anderer Knoten durch Router Advertisements und Router Solicitation und
- die Weiterleitung von DHCP-Nachrichten.

Die im jeweiligen Netz eingesetzten Mechanismen zur Unterstützung von Dienstgüte sollten implementiert sein, da Dienstgüte nur realisiert werden kann, wenn alle an einem Datenstrom beteiligten Komponenten geeignet handeln.

Im Bereich *Netzwerk-/Systemmanagement* wird eine Überwachung der Netzkomponenten empfohlen, typischerweise wird dabei SNMP eingesetzt. Details zu den SNMPv3-RFCs finden sich in Abschnitt 4.2.2 und dem zugehörigen Blatt der „Profilmatrix". Aus Sicherheitsgründen kann es erforderlich sein, dass ein SNMP-Proxy eingesetzt wird. Damit kann bspw. gesteuert werden, dass nur ein lesender Zugriff erlaubt wird und die Veränderung der Konfiguration eines Sicherheitsgeräts mittels Schreibzugriffen verhindert wird.

Die allgemeinen *Management- und Konfigurationsanforderungen*, die für alle IPv6-Geräte gelten, sind in Abschnitt 4.7 näher erläutert.

Sicherheitskomponenten müssen Funktionen zur Administration bereitstellen und gegen unautorisierten Zugang geschützt sein. Für den Zugang zu Konfigurationsfunktionen muss eine Autorisierung und Authentifizierung stattfinden. Falls der Verdacht eines unautorisierten Zugangs besteht, muss die Komponente entsprechende Ereignisse aufzeichnen und Alarme senden.

Bei der Ausführung der spezifischen Schutzfunktionen muss vermieden werden, dass ein Sicherheitsgerät damit seine eigene Funktionstüchtigkeit beeinträchtigt. Sicherheitskomponenten sind selbst prominente Angriffsziele, da durch einen erfolgreichen Angriff ganze Subnetze in Mitleidenschaft gezogen werden können.

Typische Angriffe zielen beispielsweise auf eine Fehl- oder Minderfunktion oder einen totalen Funktionsausfall bei Überlast ab.

Beim *Selbstschutz* müssen die Ressourcen für die Paketverarbeitung gegen Angriffe geschützt werden. Gleichzeitig muss aber sichergestellt werden, dass sich Pakete durch derartige Angriffe nicht der Analyse in der Sicherheitskomponente entziehen können. Es wird empfohlen, dass eine Sicherheitskomponente Pakete verwirft, die in einer Ressourcen-kritischen Situation nicht angemessen analysiert werden könnten.

Eine Sicherheitskomponente muss Schutzfunktionen gegen Fragmentierungsangriffe aufweisen. Dies ist sowohl in IPv4- als auch in IPv6-Netzen wichtig. In IPv6-Netzen ist zu beachten, dass Sicherheitskomponenten Pakete zu Analysezwecken reassemblieren müssen, obwohl dies bei IPv6 nur in den Endsystemen stattfinden sollte.

Generelle Anforderungen an den Selbstschutz (die sowohl für IPv4 als auch für IPv6 gelten), sind:

- Die qualitativen Schutzziele müssen auch unter schweren Lastbedingungen erreicht werden. Nötigenfalls muss die Komponente einen Alarm erzeugen und die Kommunikation vollständig blockieren.

- Konfigurations-Einstellungen sollten gegen Manipulation geschützt sein. Ein typischer Mechanismus ist die signierte Ablage einer Kopie – auch auf einer separaten Komponente – kombiniert mit dem regelmäßigen Vergleich der Einstellungen mit der Kopie.

4.5.2 IPv6-Paketfilter

Ein Paketfilter kontrolliert die Verbindung zwischen Netzen und schützt ein Netzwerk gegen Angriffe von außen. Er kann nicht gegen interne Angriffe und nur auf der Ebene schützen, auf der er eingesetzt wird (Analysetiefe der Pakete): Ein Paketfilter auf Netzwerkebene kann nicht gegen Angriffe auf Anwendungsebene schützen.

Generell ist zu beachten, dass der Einsatz von Paketfiltern nur eine von vielen Sicherheitsmaßnahmen ist. Es wird empfohlen, diese auf geeignete Weise mit weiteren Maßnahmen zu kombinieren (z. B. Intrusion-Detection-Systemen), um mehrere Verteidigungslinien aufzubauen.

Die Paketfilter-Funktionen werden in die folgenden Kategorien gruppiert:

- Allgemein
- Kommunikation des Paketfilters
- Unterstützung des Transitverkehrs
- Netzwerk-/System-Management
- Paketfilter-Funktionalität (Schutz-Funktionalität), bestehend aus
    - Selbstschutz des Paketfilter-Gerätes
    - Paketanalyse

Die Anforderungen aus den einzelnen Kategorien sind im Tabellenblatt „Paketfilter“ der „Profilmatrix“ angegeben und werden ggf. im Folgenden erläutert.

Die Anforderungen der Kategorien „Allgemein“, Kommunikation des Paketfilters, Unterstützung des Transitverkehrs und Netzwerk-/System-Management entsprechen denen, die für Sicherheitskomponenten generell gelten (siehe Abschnitt 4.5.1).

Arbeitet ein Gerät mit einer Paketfilter-Komponente – wie in der Praxis üblich – gleichzeitig als Router, müssen die im Tabellenblatt „Router“ der „Profilmatrix“ bzw. in Abschnitt 4.3 geforderten Funktionen für IPv6-Router in gleichem Maße unterstützt werden.

Die eigentliche Paketfilter-Funktionalität – das Schützen der ausgangsseitigen, netzinternen Netzkomponenten gegen Angriffe und das Schützen eingangsseitiger, netzinterner Daten gegen unerlaubte Verbreitung – umfasst den Schutz der eigenen Ressourcen gegen Angriffe und die Auswertung ankommender IP-Steuerdaten.

In einer Dual-Stack-Umgebung bearbeitet ein Paketfilter sowohl IPv6- als auch IPv4-Pakete oder nur eine IP-Protokollversion. Im letzteren Fall muss sichergestellt werden, dass alle Pakete der jeweils nicht unterstützten IP-Version verworfen werden.

Neben den allgemeinen *Selbstschutz*funktionen für Sicherheitskomponenten muss ein Paketfilter gegen Angriffe mit langen Ketten von Extension-Headern gewappnet sein. Angriffe mit Optionen in Hop-by-Hop-Extension-Headern sollten ebenfalls erkannt und behandelt werden. Diese Angriffsformen können nur in IPv6-Netzen auftreten.

4.5.2.1 Paketanalyse

Bei der *Auswertung ankommender Nutz- und Steuerdaten* unterscheiden wir die folgenden Kategorien:

- Funktionen für alle Pakete
- Fragmentierte Pakete
- Jumbogramme
- Gekapselte Pakete
- Pakete mit Extension-Headern
- ICMP-Pakete

Bei den *Funktionen für alle Pakete* sind folgende Besonderheiten zu beachten:

- Blockieren von Paketen anhand von Portnummern, Protokoll, IP-Adressen (verpflichtend): Es muss möglich sein, die Blockierung beliebiger Protokolle, Quell- und Ziel-Portnummern und Quell- und Ziel-IP-Adressen und beliebiger Kombinationen derartiger Werte zu konfigurieren. Diese Funktionalität ist gleichermaßen bei IPv4- und IPv6-Paketfiltern gefordert. Besonders zu berücksichtigen ist, dass alle IPv6-Adresstypen unterstützt werden.
- Asymmetrisches Blockieren (verpflichtend): Es muss möglich sein, die Blockierung auf Basis bestimmter IP-Header-Inhalte auf eine Übertragungsrichtung (abgehend oder ankommend) zu beschränken. Diese Funktionalität ist gleichermaßen bei IPv4- und IPv6-Paketfiltern gefordert.
- IP-Header-Analyse (verpflichtend): Da sich der IPv6-Header vom IPv4-Header unterscheidet, muss diese Funktion speziell für IPv6 zur Verfügung gestellt werden und alle verpflichtenden, bedingten und optionalen Header-Felder unterstützen.
- Behandlung von IPsec-Verkehr (verpflichtend): Ein Paketfilter muss je nach Bedarf des Betreibers IPsec-Verbindungen blockieren können

und/oder die Möglichkeit haben, IPsec-Verkehr auf der Basis bestimmter IP-Header-Inhalte selektiv zu blockieren.

- Stateful Packet Inspection (verpflichtend): Diese Funktionalität ist gleichermaßen für IPv4- und IPv6-Paketfilter gefordert. Es müssen jedoch spezielle Funktionen für IPv6-Pakete, beispielsweise für die Limitierung von ICMPv6-Paketen, bereitgestellt werden.

- Erkennung fehlerhaft geformter Pakete (verpflichtend): Dies ist auch in IPv4-Netzen notwendig. Da sich IPv4- und IPv6-Pakete unterscheiden, müssen spezielle Funktionen für IPv6-Pakete bereitgestellt werden.

- Erkennung von kleinen Paketen (<1280 Bytes) (empfohlen): Insbesondere sehr viele kleine Fragmente großer Nachrichten können ein Hinweis auf einen Denial-of-Service-Angriff sein. Diese Angriffsform ist auch in IPv4-Netzen möglich, es müssen aber wegen unterschiedlicher Paket-, Fragment- und Nachrichtengrößen sowie wegen der unterschiedlichen Fragmentierungsstrategie spezielle Funktionen für IPv6 bereitgestellt werden.

- Erkennung bekannter Angriffe (empfohlen): Diese Empfehlung selbst ist zwar unspezifisch und daher nicht justiziabel, stellt aber einen Platzhalter für konkrete bekannte Angriffe dar, die entweder von einem potenziellen Kunden oder einem Anbieter benannt werden können.

- Erkennung von Port Scans (empfohlen): Port-Scanning ist in der Regel die Vorstufe für gezielte Angriffe, kann aber selbst bereits einen Denial-of-Service-Angriff darstellen. Diese Funktionalität ist gleichermaßen bei IPv4- und IPv6-Paketfiltern sinnvoll.

- Erkennung von Host Scans (empfohlen): Host-Scanning ist in der Regel die Vorstufe für gezielte Angriffe, kann aber selbst bereits einen Denial-of-Service-Angriff darstellen. Diese Funktionalität ist gleichermaßen bei IPv4- und IPv6-Paketfiltern sinnvoll, bei IPv6-Netzen ist aber wegen des größeren Adressraumes, anderer Adresstypen und anderer Well-known-Adressen ein anderes Vorgehen von Angreifern zu erwarten.

- Port-to-Application Mapping (optional): Die bedingte Änderung des für eine Anwendung typischerweise benutzten Ports durch einen Paketfilter kann Angriffe verhindern und/oder verschiedenen Nutzergruppen Zugang zu einem unterschiedlichen Funktionsumfang einer Anwendung ermöglichen. Diese Funktionalität ist gleichermaßen bei IPv4- und IPv6-Paketfiltern sinnvoll.

Pakete dürfen sich nicht durch Fragmentierung oder die Verwendung von Extension-Headern der Analyse durch den Paketfilter entziehen können. Ein IPv6-Paketfilter muss Funktionen bereitstellen, um derartige Pakete analysieren zu können.

Bei der Behandlung *fragmentierter Pakete* sind folgende Besonderheiten zu beachten:

- Erfassen der Anzahl der fragmentierten Pakete pro Quell-IP-Adresse zwecks Erkennung möglicher Denial-of-Service-Angriffe (empfohlen)
- Reassemblieren von fragmentierten Paketen (empfohlen): Entgegen der Vorgabe in RFC 2460, dass nur Endsysteme reassemblieren, sollte ein IPv6-Paketfilter fragmentierte Pakete zwecks Analyse reassemblieren. Als unbedenklich eingestufte Fragmente können anschließend ohne erneute Fragmentierung weitergeleitet werden.

Bei der Behandlung *getunnelter Pakete* sind folgende Besonderheiten zu beachten:

- Erkennung, Analyse und Blockier-Funktionen für getunnelte Pakete (verpflichtend): In Erweiterung der Funktionalität für native Pakete muss es auch möglich sein, bestimmte Kapselungen vollständig zu blockieren.
- Stateful Packet Inspection (verpflichtend): Diese Funktionalität muss auch für gekapselte Pakete zur Verfügung stehen.
- Erkennung von IPv6-in-IPv6-Kapselung (verpflichtend): Dies kann ein Versuch sein, Pakete üblichen Analyse-Verfahren zu entziehen.

Bei der Behandlung von *Paketen mit Extension-Headern* sind folgende Eigenschaften zu beachten:

- Erkennung und Interpretation von Extension-Headern (verpflichtend): Dazu können beispielsweise folgende Unterfunktionen gehören:
    - Erkennung ungewöhnlicher Header-Reihenfolgen (verpflichtend)
    - Erkennung ungewöhnlicher Header-Wiederholungen (verpflichtend)
    - Erkennung ungewöhnlich vieler Optionen in Hop-by-Hop-Headern (verpflichtend)
    - Erkennung ungültiger Optionen (verpflichtend)
    - Erkennung von Padding-Bytes, die nicht mit Nullen gefüllt sind, (verpflichtend): Dies kann ein Anzeichen für den Versuch sein, einen verdeckten Kanal zu benutzen.

Bei der Behandlung von *ICMPv6-Paketen* ist Folgendes zu beachten:

- Filtern von ICMPv6-Paketen entsprechend RFC 4890 (verpflichtend): ICMPv6-Pakete dürfen nicht generell blockiert werden, da einige essenzielle Nachrichten enthalten (bspw. Message-too-big-Nachrichten).

4.5.3 Application-Layer-Gateways

Ein Application-Layer-Gateway hat die Aufgabe, die für die Abwicklung einer oder mehrerer Anwendungen erforderliche Kommunikation zu überwachen und ggf. zu verändern bzw. zu blockieren. Zu diesem Zweck werden Transportverbindungen im Application-Layer-Gateway terminiert. Das Application-Layer-Gateway führt ein internes Routing und Relaying der anwendungsorientierten Nachrichten zwischen eingangs- und ausgangsseitigen Transportverbindungen durch.

Formal könnte ein Application-Layer-Gateway unabhängig von der verwendeten IP-Protokollversion arbeiten, praktisch bestehen aber durch die Verfügbarkeit anderer und/oder zusätzlicher Funktionen in IPv6-Netzen auch Abhängigkeiten zur verwendeten IP-Version.

Die Application-Layer-Gateway-Funktionen werden in die folgenden Kategorien gruppiert:

- Allgemein
- Kommunikation des Application-Layer-Gateways
- Unterstützung des Transitverkehrs
- Netzwerk-/System-Management
- Filter-/Schutz-Funktionen, bestehend aus:
    - Selbstschutz des Application-Layer-Gateway-Gerätes
    - Paketanalyse

Die Anforderungen aus den einzelnen Kategorien sind im Tabellenblatt „Application-Layer-Gateway“ der „Profilmatrix“ angegeben und werden ggf. im Folgenden erläutert.

Die Anforderungen der Kategorien „Allgemein“, Kommunikation des Application-Layer-Gateways, Unterstützung des Transitverkehrs und Netzwerk-/System-Management entsprechen weitgehend denen, die für Sicherheitskomponenten generell gelten (siehe Abschnitt 4.5.1).

Zusätzlich sollte ein Application-Layer-Gateway in der Lage sein, Packetization Layer Path MTU Discovery nach RFC 4821 (die Ermittlung der maximalen Paketgröße anhand gesendeter Anwendungspakete) durchzuführen.

Für den nicht-transparenten, authentifizierten Zugriff von extern steht das SOCKS5-Protokoll (RFC 1928) zur Verfügung. Dessen Unterstützung – einschließlich sicherer Konfigurationsmöglichkeiten - durch Application-Layer-Gateways wird empfohlen.

Arbeitet ein Gerät mit einer Application-Layer-Gateway-Komponente – wie in der Praxis üblich – gleichzeitig als Router, müssen die im Tabellenblatt „Router“ bzw. in Abschnitt 4.3 geforderten Funktionen für IPv6-Router in gleichem Maße

unterstützt werden. Auch eine Kombination mit einer Paketfilter-Komponente ist nicht unüblich. In diesem Fall müssen die Anforderungen des Tabellenblattes „Paketfilter“ bzw. des Abschnittes 4.5.2 ebenfalls erfüllt sein.

Die eigentliche Application-Layer-Gateway-Funktionalität – das Schützen der ausgangsseitigen, netzinternen Netzkomponenten gegen Angriffe und das Schützen eingangsseitiger, netzinterner Daten gegen unerlaubte Verbreitung – umfasst den Schutz der eigenen Ressourcen gegen Angriffe und die Auswertung und ggf. Änderung ankommender Nutz- und Steuerdaten.

4.5.3.1 Paketanalyse

Bei der *Auswertung ankommender Nutz- und Steuerdaten* unterscheiden wir die folgenden Kategorien:

- Funktionen für alle Nachrichten
- Typische Anwendungen

Bei den *Funktionen für alle Nachrichten* sind folgende Besonderheiten zu beachten:

- Generell müssen sowohl Nutz- als auch Steuerdaten der jeweils betrachteten Protokolle und Ebenen behandelt werden.
- Nachrichten unerwünschter Protokolle müssen vollständig blockierbar sein, d. h., verworfen werden können.
- Konfigurierbare Blockierung oder Änderung von Ports und Adressen, soweit diese explizit mit der IP-Schicht ausgetauscht werden (verpflichtend)
- Asymmetrisches Blockieren (verpflichtend): Es muss möglich sein, die Blockierung auf Basis von Anwendungsprotokollen, einzelnen Protokoll-Funktionen, Ports und/oder Adressen auf eine Initiierungsrichtung (abgehend oder ankommend) zu beschränken. Beispielsweise könnten HTTP-Anfragen generell nur von innen nach außen, entsprechende Antworten nur von außen nach innen zugelassen werden.
- Konfigurierbare Blockierung oder Änderung von Optionen der unteren Schichten, soweit diese explizit mit der IP-Schicht ausgetauscht werden (verpflichtend)
- Erkennung nicht Protokoll-konformer Nachrichten (verpflichtend): Für die unterstützten Protokolle muss eine vollständige Analyse der Nachrichten möglich sein.
- Analyse / Blockierung fragmentierter Nachrichten (verpflichtend): Nachrichten dürfen sich nicht durch Fragmentierung der Analyse durch das Application-Layer-Gateway entziehen können. Ein Application-Layer-Gateway muss Fragmentierung oberhalb der IP-Schicht erkennen und behandeln können.

- Reassemblieren fragmentierter Nachrichten (empfohlen): Ein IPv6-Application-Layer-Gateway sollte fragmentierte, anwendungsorientierte Nachrichten zwecks Analyse reassemblieren. Als unbedenklich eingestufte Fragmente können anschließend ohne erneute Fragmentierung weitergeleitet werden.

- Analyse und Blockierfunktionen für verschlüsselte Nachrichten (verpflichtend): Es muss möglich sein, verschlüsselte Nachrichten zu analysieren und/oder zu verwerfen.

- Analyse- und Blockierfunktionen für getunnelte Nachrichten (verpflichtend): Es muss möglich sein, bestimmte Tunnelungen vollständig zu blockieren.

- Erkennung und Behandlung bekannter Angriffe (empfohlen): Diese Empfehlung selbst ist zwar unspezifisch, stellt aber einen Platzhalter für konkrete bekannte Angriffe dar, die entweder von einem potenziellen Kunden oder einem Anbieter benannt werden können.

Ein Application-Layer-Gateway muss in der Lage sein, alle in der konkreten ÖV üblichen Anwendungen angemessen und entsprechend dem aktuellen Stand bzgl. typischer Nachrichtenfelder und Nachrichtenfolgen zu behandeln.

- Zu den allgemein üblichen Anwendungen gehören insbesondere Webserver-basierte Dienste (HTTP), E-Mail (SMTP/POP/IMAP), Dateitransfer (FTP und in E-Mail-Nachrichten) und Anwendungen für das Netz- und System-Management.

- Angesichts des wachsenden Einsatzes von Voice-over-IP wird empfohlen, eine entsprechende Unterstützung durch Application-Layer-Gateways auch dann vorzusehen, wenn bislang kein Einsatz geplant ist.

4.5.4 VPN-Krypto-Gateway

Ein VPN-Krypto-Gateway stellt gegen „Mithören“ geschützte virtuelle Links über unsichere, insbesondere öffentliche, Netze zur Verfügung. Ein solches Gateway arbeitet anwendungsunabhängig. Die VPN-Krypto-Gateway-Funktionen werden in die folgenden Kategorien gruppiert:

- Allgemein
- Kommunikation des VPN-Krypto-Gateways
- Unterstützung des Transitverkehrs
- Netzwerk-/System-Management
- VPN-Krypto-Funktionalität, bestehend aus:
    - Selbstschutz des VPN-Krypto-Gateway-Gerätes
    - VPN-Krypto-Gateway Tunnelvarianten

Die Anforderungen aus den einzelnen Kategorien sind im Tabellenblatt „VPN-Krypto-Gateway“ der „Profilmatrix“ angegeben und werden ggf. im Folgenden erläutert.

Die Anforderungen der Kategorien „Allgemein“, Kommunikation des VPN-Krypto-Gateways, Unterstützung des Transitverkehrs und Netzwerk-/System-Management entsprechen weitgehend denen, die für Sicherheitskomponenten generell gelten (siehe Abschnitt 4.5.1).

Wenn ein VPN-Krypto-Gateway direkt an einer redundant ausgelegten Schnittstelle betrieben werden soll, die mittels VRRP gesteuert wird, muss es RFC 5798 („Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6“) unterstützen.

Gleiches gilt für die Unterstützung der IPv6-Variante des Hot-Standby-Router-Protokolls (HSRP) für entsprechende Schnittstellen. Für diese Protokollvariante gibt es keinen RFC.

Neben den allgemeinen *Selbstschutz*funktionen für Sicherheitskomponenten muss ein VPN-Krypto-Gateway gegen Angriffe mit langen Ketten von Extension-Headern gewappnet sein. Angriffe mit Optionen in Hop-by-Hop-Extension-Headern sollten ebenfalls erkannt und behandelt werden. Diese Angriffsformen können nur in IPv6-Netzen auftreten.

Ein VPN-Krypto-Gateway muss alle möglichen Kombinationen von IP-Versionen zum Betrieb der virtuellen Links einerseits und für den transportierten Datenverkehr andererseits unterstützen. Insbesondere dann, wenn auf der entfernten Seite virtueller Links ebenfalls ein Dual-Stack-Gateway zu erwarten ist, müssen auch gleichzeitig IPv6- und IPv4-basierte Links möglich sein.

4.6. Infrastruktur-Server

Dieses Profil fasst verschiedene funktionale Netzkomponenten zusammen, die normalerweise für den Betrieb des Netzes benötigt werden. Diese Komponenten können als eigenständige Server realisiert sein und basieren dann auf dem „Endsystem“-Profil, sie können aber auch in einem Router realisiert sein. Die jeweiligen Anforderungen an einen Infrastruktur-Server sind nur dann relevant, wenn der Einsatz der entsprechenden IPv6-Funktionalität geplant ist.

4.6.1 DHCP-Server

Die Eigenschaften eines DHCPv6-Servers sind in RFC 3315 („Dynamic Host Configuration Protocol for IPv6 (DHCPv6)“) festgelegt. Mittels einer Reihe von DHCPv6-Optionen können die Adressen verschiedener (weiterer) Infrastruktur-Server auf den DHCPv6-Klienten konfiguriert werden. Aufgrund der grundsätzlichen Bedeutung für den sicheren Betrieb eines Netzes sind die DHCPv6-Optionen für DNS- und NTP-Server verpflichtend. Die Unterstützung weiterer DHCPv6-Optionen ist, soweit und sobald verfügbar, empfohlen.

4.6.2 DNS-Server

Das Profil sieht aufgrund der Bedeutung von DNS Empfehlungen für den Betrieb eines DNS-Servers vor, auch wenn dieser weitgehend nicht IPv6-spezifisch ist.

Die Nutzung eines rekursiven DNS-Resolvers ist verpflichtend, dieser wird i. d. R. auf DNS-Server des Providers zugreifen.

4.6.3 RADIUS-Server

Wird ein RADIUS-Server [RFC2865] für AAA (Authentifizierung, Autorisierung und Abrechnung) beim Zugang zu IPv6-Netzen verwendet (bspw. zur Authentifizierung beim WLAN-Zugang), so muss dieser mit IPv6-Adressen und -Adressbestandteilen umgehen können. Die dazu nötigen RADIUS-Attribute sind in RFC 3162 („RADIUS and IPv6“) beschrieben. Das RADIUS-Protokoll selbst setzt direkt auf UDP auf und ist somit unabhängig von der IP-Schicht.

4.6.4 Tunnelbroker

Ein Tunnelbroker ermöglicht den automatisierten Aufbau eines Tunnels zur Anbindung eines Teilnetzes oder eines Klienten an eine bestehende IPv6-Infrastruktur. Damit wird wirksam die Migrationsphase zu IPv6 unterstützt, in der noch nicht an allen Standorten ein Internet-Serviceprovider den Zugang zu einem IPv6- oder Dual-Stack-Netz bieten kann.

4.7. Management und Konfiguration

Die meisten IPv6-fähigen Geräte, die in einer ÖV zum Einsatz kommen, besitzen veränderliche Kommunikationseinstellungen und eine oder mehrere Schnittstellen (lokale Bedienschnittstellen, Webserver, dedizierte Anwendungen für den entfernten Zugriff), über die diese Einstellungen konfiguriert und statische Geräteeigenschaften, Einstellungen und aufgezeichnete Daten abgefragt werden können.

Im Weiteren wird nur auf Schnittstellen für den entfernten Zugriff eingegangen. Die Forderungen / Empfehlungen sind unabhängig davon, ob eine physisch separate Kommunikationsschnittstelle für Management und Konfiguration unterstützt wird oder die diesbezügliche Kommunikation „in-band“ erfolgt, d. h. über eine gemeinsame Schnittstelle mit anderen Anwendungen.

Konfigurationseinstellungen und wesentliche lokal aufgezeichnete Ereignisse müssen auch nach einem Stromausfall unverändert erhalten sein. Nur so ist eine lückenlose Nachverfolgung von Konfigurationsvorgängen möglich.

Es wird empfohlen, dass alle Geräte mit mindestens einer Management- und Konfigurationsschnittstelle für den entfernten Zugang ausgestattet sind. Die Möglichkeit zur Konfiguration und Datenabfrage aller Geräte einer administrativen Domäne von einem gemeinsamen Ort aus erhöht nicht nur den Komfort und die Effizienz dieser Arbeiten. Gleichzeitig wird die Gefahr unterlassener Aktualisierungen und nicht bemerkter kritischer Ereignisse reduziert, die beispielsweise durch die zeitweilige Nicht-Zugänglichkeit von Geräten (z. B. in verschlossenen

Mitarbeiterräumen oder in anderweitig belegten gemeinschaftlich genutzten Räumen) entstehen kann.

Eine Management-/Konfigurationsschnittstelle sollte prinzipiell sowohl über IPv4 als auch über IPv6 erreichbar sein. Falls die Verwendung eines der Protokolle (zeitweilig) nicht möglich oder unerwünscht ist, sollte es für diesen Zweck blockierbar sein.

Sowohl statische als auch konfigurierbare und aufgezeichnete Daten müssen gegen unbefugten Zugriff (auch lokal) geschützt werden. Für den entfernten Zugriff müssen angemessene Authentifizierungs- und Authentisierungsmechanismen zur Verfügung stehen.

Ebenso wie die Konfiguration sollten auch Logging-Daten und Alarme sowohl über IPv4 als auch über IPv6 verfügbar gemacht werden können. Wird eines der Protokolle für den tatsächlichen Betrieb (zeitweilig) nicht genutzt, sollte es für diesen Zweck explizit abschaltbar sein.

Verwendet eine Management- und Konfigurationsschnittstelle IPsec und IPv6-Übertragung in einem IPv4-Tunnel, muss auch diese IPv6-Übertragung durch IPsec geschützt werden können. Am Bediengerät ist evtl. gar nicht erkennbar, dass ein Teil der Kommunikationsstrecke in einem Tunnel verläuft, und ein späterer Wegfall des Tunnels (bei durchgängiger Verfügbarkeit von IPv6) darf nicht zu notwendigen Änderungen auf Seiten des Bediengerätes führen.

4.8. Enterprise Switch

Obwohl (Layer-2-)Switches unterhalb der IP-Schicht Daten vermitteln, sollten sie doch bestimmte IPv6-Pakete erkennen und entsprechend behandeln können. Dabei sind zwei Aspekte zu unterscheiden:

- Für Pakete, die bereits auf dem empfangenden Netzwerksegment als kritisch eingestuft werden könnten oder deren Sichtbarkeit aus funktionalen Gründen durch den Switch nicht erweitert werden sollte, sollte die Weiterleitung auf benachbarte Segmente blockierbar sein. Anforderungen aus dieser Gruppe sind im Abschnitt „Datenüberwachung und Filterung“ des Tabellenblattes „Enterprise Switch“ aufgeführt.

- Einige IPv6-Mechanismen sind davon abhängig, dass bestimmte Funktionen in den zwischen Ursprung und Ziel vermittelnden Geräten (insbesondere Switches und Router) implementiert sind. Diese sollten auch dann in diesen Geräten vorhanden sein, wenn der Einsatz der davon abhängigen, höheren Funktionen noch nicht vorgesehen ist. Im entsprechenden Tabellenblatt, hier „Enterprise Switch“, sind solche Anforderungen in den Abschnitten „Dienstgüte (Quality of Service, QoS)“ und „Multicast“ zu finden.

Wird an die Management-Schnittstelle des Switches die Anforderung nach IPv6-Unterstützung gestellt, so gelten die entsprechenden Tabellenblätter, bspw. für Knoten.

5. Anforderungen an Software-Komponenten

Durch die zuvor definierten Geräteprofile für IPv6 wird im Wesentlichen die Konnektivität und Interoperabilität auf Netzwerkebene (Schicht 3) sichergestellt (vgl.

Abbildung 8).

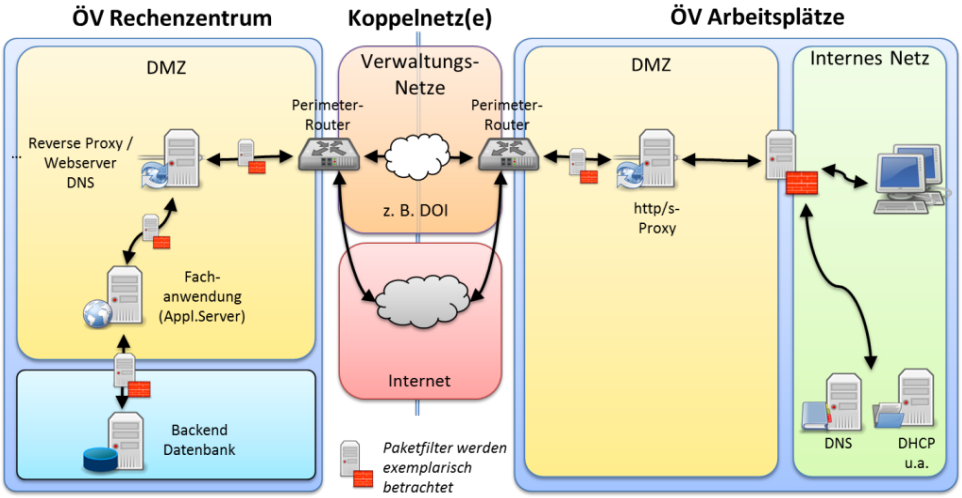


Abbildung 8: Konnektivität auf Netzwerkebene

Das Bild zeigt die Referenzarchitektur der öffentlichen Verwaltung; nähere Details dazu finden sich im Migrationsleitfaden [IPv6_Migration]. Die Referenzarchitektur zeigt die logische Ende-zu-Ende-Kommunikation bestimmter Anwendungen. Die Nutzung solcher Anwendungen kann einen Kommunikationspfad vom Arbeitsplatz über Koppelnetze zu Servern in einem Rechenzentrum umfassen. Der Betrieb einer solchen Anwendung ist damit von den Geräten im Kommunikationspfad und von den dazu notwendigen Netzinfrastrukturdiensten abhängig.

In den folgenden Abschnitten werden diese Abhängigkeiten genauer dargestellt. Abschließend wird ein Verfahren vorgeschlagen, mit dem die Prüfung dieser Abhängigkeiten für verschiedenste Anwendungen systematisch durchgeführt werden kann.

5.1. Komponenten-interne Anforderungen

Ausgangspunkt für die Betrachtung sind die Einbindung und der Betrieb von Systemen in einem IPv6-Netz (Dual-Stack-Betrieb oder IPv6-only). Dazu müssen die Geräte zunächst die grundlegenden Anforderungen des Hardware-Profils erfüllen, wie in Kapitel 4 beschrieben.

Jede in ein IPv6-basiertes Netzwerk eingebundene Anwendungskomponente muss eine Reihe von Basisfunktionen ausführen können:

- Aufbauen ausgehender IPv6-Verbindungen

- Annehmen eingehender IPv6-Verbindungen
- Verarbeitung von IPv6-Adressen bei der DNS-Namensauflösung

Fallweise können weitere Anforderungen hinzukommen:

- Wenn die Software bisher IPv4-Adressen nicht nur zum Adressieren von Kommunikationspartnern benutzt, sondern auch als Anwendungsdaten im engeren Sinne verwendet (etwa für Logging oder als Bestandteil von Sitzungsbezeichnern / SessionIDs), müssen diese Funktionen auch mit IPv6-Adressen umgehen können.
- Auch wenn einzelne Funktionsbereiche der Anwendung (z. B. die Namensauflösung) während der Migrationsphase noch auf IPv4 basieren, sollte schon jetzt die Funktionsfähigkeit auch in reinen IPv6-Netzen geprüft und sichergestellt werden.
- Insbesondere bei Softwarepaketen, die im Quellcode vorliegen, ist darauf zu achten, dass die IPv6-Tauglichkeit auch tatsächlich durch Setzen entsprechender Konfigurationsoptionen einkompiliert wurde.

5.2. Abhängigkeit von anderen (externen) Komponenten

Sodann ist die Abhängigkeit der Anwendung von weiteren Komponenten oder (Sub-)Systemen zu betrachten. Diese Abhängigkeiten sind in

Abbildung 9 schematisch zusammengefasst.

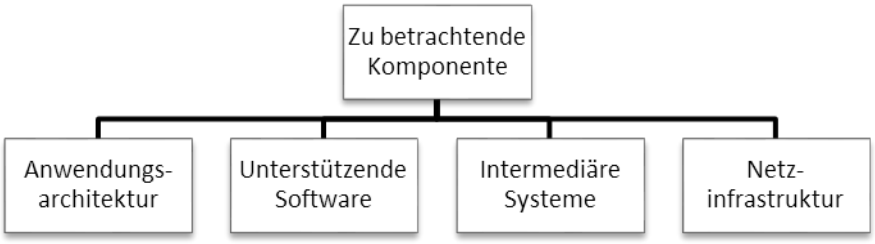


Abbildung 9: Anwendungsvoraussetzungen

Diese Anwendungsvoraussetzungen können weiter verfeinert werden. In Abbildung 10 ist beispielhaft eine Liste von Komponenten dargestellt, wobei die Komponenten thematisch gruppiert sind. Einige dieser Gruppen entsprechen den in

Abbildung 9 aufgeführten Kategorien, andere dienen der weiteren Strukturierung der relativ großen Kategorie „Unterstützende Software“.

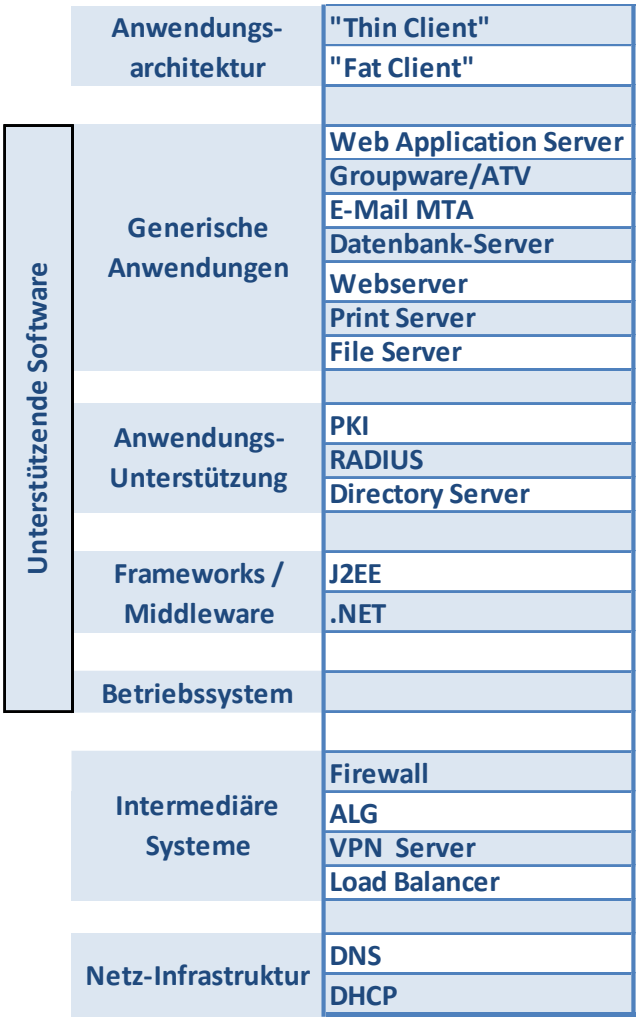


Abbildung 10: Liste möglicher Komponenten (Beispiele)

Einige der Abhängigkeiten werden im Folgenden näher erläutert.

5.2.1 Anwendungsarchitektur

Für die weitere Betrachtung ist es sinnvoll, Anwendungen entsprechend ihrer Grob-Architektur in zwei Klassen einzuteilen. In Literatur und Praxis werden hierfür zahlreiche, unterschiedliche Terminologien verwendet, für unsere Zwecke reicht die eher unscharfe Unterscheidung zwischen den Konzepten „Fat Client“ und „Thin Client“.

5.2.1.1 Fat Client

Anwendungen mit dieser Architektur sind dadurch gekennzeichnet, dass ein nicht unerheblicher Anteil der Gesamtfunktionalität auf dem Endsystem, also dem Rechner des Anwenders implementiert ist.

Damit sind nicht nur Funktionen der eigentlichen Anwendung oder unterstützende Funktionen für Basisdienste gemeint. Auch wenn diese als Dienste auf dedizierten Serversystemen implementiert sind, benötigt ein typischer „Fat Client“

doch zahlreiche, *lokal installierte Bibliotheken*, die die Schnittstelle zu den entsprechenden Serverdiensten implementieren.

Da diese Schnittstellen auf dem jeweils verwendeten Netzwerk aufsetzen, sind die mit dem Fat Client verbundenen Bibliotheken beim Übergang zu IPv6 bei der Migration mit zu betrachten.

5.2.1.2 Thin Client

Die verschiedenen, hier summarisch als „Thin Client“ bezeichneten Konzepte, zeichnen sich dadurch aus, dass auf dem Rechner des Anwenders lediglich anwendungsneutrale Funktionen implementiert sind, die im Wesentlichen die Bildschirmdarstellung sowie die Steuerung verschiedener Ein- und Ausgabegeräte realisieren.

Die eigentliche Anwendung, einschließlich der Schnittstellen zu weiteren im Netzwerk bereitgestellten Diensten, ist auf zentralen Servern implementiert. Diese kommunizieren über vergleichsweise einfache Protokolle mit dem Endsystem. Für diese Protokolle muss dazu eine äquivalente IPv6-Implementierung vorliegen.

Zwar ist die Abhängigkeit der Anwendung von anderen Komponenten sowie den Schnittstellenbibliotheken im Vergleich zu einer Realisierung als Fat Client nicht verschwunden. Allerdings ist die *Zahl der Installationen* erheblich reduziert und auf wenige Serversysteme konzentriert. Dies kann insbesondere bei Betrachtung unterschiedlicher Bibliotheksversionen (oder dem Dual-Stack-Betrieb) den Übergang zu IPv6 erheblich vereinfachen.

In diese Klasse fallen sogenannte Web-Applikationen – deren Klientenseite vollständig in einem Browser abläuft – ebenso wie der Einsatz von Virtualisierungslösungen (für die unterschiedliche Begriffe und Realisierungen gebräuchlich sind, z. B. Terminalserver, Desktop-Virtualisierung oder Virtual Desktop Infrastructure). Hinsichtlich des Einsatzes von IPv6 ergibt sich eine Abhängigkeit der betrachteten Anwendung von der zugrunde liegenden Web- bzw. Virtualisierungsinfrastruktur.

5.2.2 Unterstützende Software

Merkmal der unterstützenden Softwarekomponenten ist es, dass sie anwendungsneutral sind und von verschiedensten Anwendungen benutzt werden können. Darüber hinaus ist zu beachten, dass es durchaus auch Abhängigkeiten einzelner dieser Komponenten untereinander gibt. So kann etwa ein bestimmter Web Application Server vom Funktionieren eines bestimmten Web Servers oder von der Verfügbarkeit bestimmter Print oder File Server abhängig sein.

5.2.3 Intermediäre Systeme („middleboxes“)

Auf dem Kommunikationsweg zwischen dem Arbeitsplatz und entfernten serverbasierten Systemen befinden sich in der Regel verschiedene Zwischenknoten. Diese erfüllen nicht nur die in den Geräteprofilen geforderten Anforderungen auf Netzwerkebene, sondern müssen darüberhinaus eventuell

auch noch bestimmte Eigenschaften auf höheren Protokollschichten haben, um einen zuverlässigen Betrieb zu gewährleisten.

Eine Besonderheit dieser Systeme liegt darin, dass sie in vielen Fällen für die eigentliche Funktion der Anwendung nicht notwendig sind und daher die Wechselwirkungen mit der Anwendung leicht übersehen werden können. Bspw. verhalten sich Paketfilter für die eigentliche Anwendung transparent, eine Fehlkonfiguration des Paketfilters aufgrund unzureichender Informationen über die Anwendung führt in der Regel zur Fehlfunktion der Anwendung.

5.2.4 Netzinfrastruktur

Manche Anwendungen bzw. Komponenten sind zudem direkt auf Informationen aus der Netzinfrastruktur angewiesen (z. B. Namensauflösung, DNS). Auch diese Abhängigkeiten sind zu prüfen.

5.3. Die Software-Matrix

Für die Erfassung und Prüfung abhängiger Komponenten ist folgendes Vorgehen sinnvoll:

In einem ersten Schritt wird eine Liste, wie sie in Abbildung 10 eingeführt wurde, dahingehend erweitert, dass für die zu untersuchende Anwendung alle von ihr genutzten Komponenten namentlich (also Produktname, Version, evtl. weitere Attribute) ersichtlich sind (vgl. Abbildung 11).

			Fachverfahren		
			Produkt	**Version**	**IPv6 ?**
			FV-XXX	*1.0*	*ok*
Unterstützende Software	**Anwendungs-architektur**	**Terminal-Service**			
		Virtualisierung			
	Generische Anwendungen	**Web Application Server**	*Glassfish*	*3.1.2*	*ok*
		Groupware/ATV			
		E-Mail MTA			
		Datenbank-Server			
		Webserver	*Apache*	*2.x*	*ok*
		Print Server			
		File Server			
	Anwendungs-Unterstützung	**PKI**			
		RADIUS			
		Directory Server			
	Frameworks / Middleware	**J2EE**	*Oracle JDK*	*1.7.0_07-b10*	*ok*
		.NET			
	Betriebssystem		*Windows*	*7SP1 x64*	*ok*
	Middle Boxes	**Firewall**	*Cisco xxxx*		*ok*
		ALG			
		VPN Server			
		Load Balancer			
	Netz-Infrastruktur	**DNS**			
		DHCP			

Abbildung 11: Liste konkreter Komponenten

Für jede Teilkomponente ist festzustellen, ob sie für den Betrieb unter IPv6 geeignet ist. Eine Übersichtsliste zum Stand der IPv6-Fähigkeiten von Standardsoftware findet sich im Anhang (Kapitel 10).

Im Falle komplexerer Abhängigkeiten kann dieses Verfahren leicht auf die rekursive Untersuchung von (Sub-)Systemen übertragen werden, sodass sich, gewissermaßen nebenbei, auch wiederverwendbare Abhängigkeits-tabellen ergeben können.

Eine solche komplexere Abhängigkeitsstruktur ist in Abbildung 12 dargestellt:

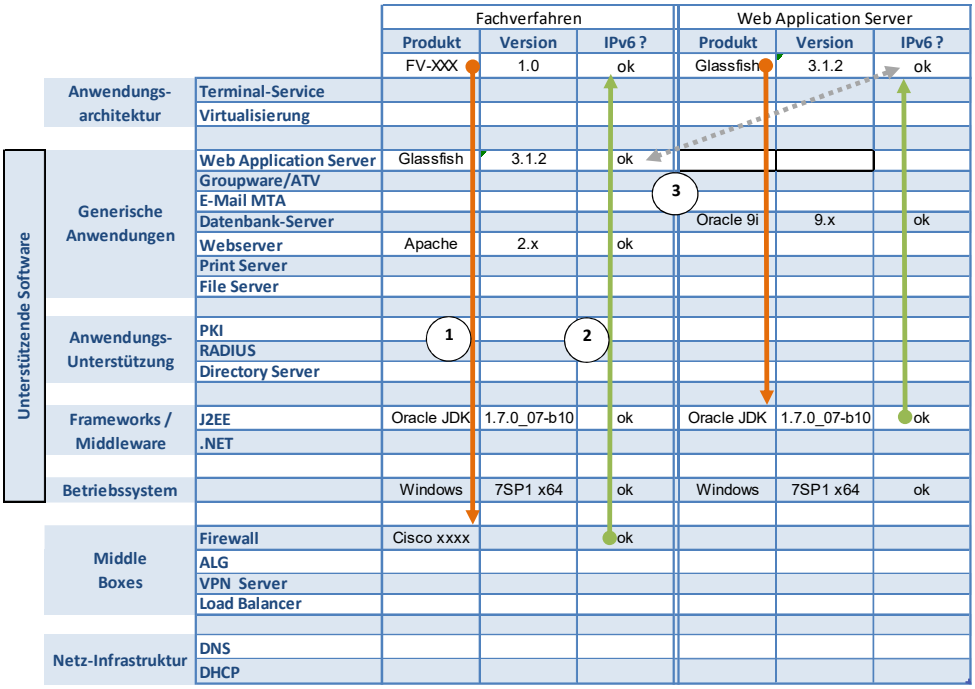


Abbildung 12: Komplexe Abhängigkeitsstruktur

Die abwärtsgerichteten Pfeile (1) geben die (zumindest partielle) Top-Down-Sicht der Anwendung auf die genutzten Komponenten wieder. Die Feststellung der IPv6-Tauglichkeit erscheint hier als komponentenweises Zusammensetzen von nachgeordneten Komponenten in Richtung der eigentlichen Anwendung ((2), von unten nach oben). Die ausgelagerte Betrachtung einer Komponente (hier: „Web Application Server“) ist durch einen grauen Pfeil (3) angedeutet. Eine für eigene Projekte geeignete Vorlage findet sich im Anhang (Kapitel 9, siehe Seite 100).

6. Quellenverzeichnis

Die Dokumente des Quellenverzeichnisses sind eine der Grundlagen für die Projektempfehlungen und die Strukturierung von „Profilmatrix“ und „Profildokument“.

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

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

7. Im Profil referenzierte RFCs

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

RFC2410	Glenn, R. and S. Kent, "The NULL Encryption Algorithm and Its Use With IPsec", RFC 2410, November 1998.
RFC2451	Pereira, R. and R. Adams, "The ESP CBC-Mode Cipher Algorithms", RFC 2451, November 1998.
RFC2460	Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
RFC2464	Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, December 1998.
RFC2467	Crawford, M., "Transmission of IPv6 Packets over FDDI Networks", RFC 2467, December 1998.
RFC2473	Conta, A. and S. Deering, "Generic Packet Tunneling in IPv6 Specification", RFC 2473, December 1998.
RFC2474	Nichols, K., Blake, S., Baker, F., and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998.
RFC2475	Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998.
RFC2491	Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, January 1999.
RFC2492	Armitage, G., Schulter, P., and M. Jork, "IPv6 over ATM Networks", RFC 2492, January 1999.
RFC2507	Degermark, M., Nordgren, B., and S. Pink, "IP Header Compression", RFC 2507, February 1999.
RFC2508	Casner, S. and V. Jacobson, "Compressing IP/UDP/RTP Headers for Low-Speed Serial Links", RFC 2508, February 1999.
RFC2516	Mamakos, L., Lidl, K., Evarts, J., Carrel, D., Simone, D., and R. Wheeler, "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.
RFC2526	Johnson, D. and S. Deering, "Reserved IPv6 Subnet Anycast Addresses", RFC 2526, March 1999.
RFC2545	Marques, P. and F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, March 1999.
RFC2553	Gilligan, R., Thomson, S., Bound, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 2553, March 1999.
RFC2597	Heinanen, J., Baker, F., Weiss, W., and J. Wroclawski, "Assured Forwarding PHB Group", RFC 2597, June 1999.
RFC2637	Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)", RFC 2637, July 1999.

RFC2671	Vixie, P., "Extension Mechanisms for DNS (EDNS0)", RFC 2671, August 1999.
RFC2675	Borman, D., Deering, S., and R. Hinden, "IPv6 Jumbograms", RFC 2675, August 1999.
RFC2710	Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, October 1999.
RFC2711	Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, October 1999.
RFC2746	Terzis, A., Krawczyk, J., Wroclawski, J., and L. Zhang, "RSVP Operation Over IP Tunnels", RFC 2746, January 2000.
RFC2747	Baker, F., Lindell, B., and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.
RFC2750	Herzog, S., "RSVP Extensions for Policy Control", RFC 2750, January 2000.
RFC2766	Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
RFC2784	Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.
RFC2790	Waldbusser, S. and P. Grillo, "Host Resources MIB", RFC 2790, March 2000.
RFC2872	Bernet, Y. and R. Pabbati, "Application and Sub Application Identity Policy Element for Use with RSVP", RFC 2872, June 2000.
RFC2890	Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.
RFC2894	Crawford, M., "Router Renumbering for IPv6", RFC 2894, August 2000.
RFC2918	Chen, E., "Route Refresh Capability for BGP-4", RFC 2918, September 2000.
RFC2961	Berger, L., Gan, D., Swallow, G., Pan, P., Tommasi, F., and S. Molendini, "RSVP Refresh Overhead Reduction Extensions", RFC 2961, April 2001.
RFC2983	Black, D., "Differentiated Services and Tunnels", RFC 2983, October 2000.
RFC2996	Bernet, Y., "Format of the RSVP DCLASS Object", RFC 2996, November 2000.
RFC3031	Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.
RFC3053	Durand, A., Fasano, P., Guardini, I., and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

RFC3095	Bormann, C., Burmeister, C., Degermark, M., Fukushima, H., Hannu, H., Jonsson, L-E., Hakenberg, R., Koren, T., Le, K., Liu, Z., Martensson, A., Miyazaki, A., Svanbro, K., Wiebke, T., Yoshimura, T., and H. Zheng, "RObust Header Compression (ROHC): Framework and four profiles: RTP, UDP, ESP, and uncompressed", RFC 3095, July 2001.
RFC3140	Black, D., Brim, S., Carpenter, B., and F. Le Faucheur, "Per Hop Behavior Identification Codes", RFC 3140, June 2001.
RFC3146	Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", RFC 3146, October 2001.
RFC3162	Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.
RFC3168	Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, September 2001.
RFC3173	Shacham, A., Monsour, B., Pereira, R., and M. Thomas, "IP Payload Compression Protocol (IPComp)", RFC 3173, September 2001.
RFC3175	Baker, F., Iturralde, C., Le Faucheur, F., and B. Davie, "Aggregation of RSVP for IPv4 and IPv6 Reservations", RFC 3175, September 2001.
RFC3181	Herzog, S., "Signaled Preemption Priority Policy Element", RFC 3181, October 2001.
RFC3182	Yadav, S., Yavatkar, R., Pabbati, R., Ford, P., Moore, T., Herzog, S., and R. Hess, "Identity Representation for RSVP", RFC 3182, October 2001.
RFC3226	Gudmundsson, O., "DNSSEC and IPv6 A6 aware server/resolver message size requirements", RFC 3226, December 2001.
RFC3241	Bormann, C., "Robust Header Compression (ROHC) over PPP", RFC 3241, April 2002.
RFC3246	Davie, B., Charny, A., Bennet, J., Benson, K., Le Boudec, J., Courtney, W., Davari, S., Firoiu, V., and D. Stiliadis, "An Expedited Forwarding PHB (Per-Hop Behavior)", RFC 3246, March 2002.
RFC3247	Charny, A., Bennet, J., Benson, K., Boudec, J., Chiu, A., Courtney, W., Davari, S., Firoiu, V., Kalmanek, C., and K. Ramakrishnan, "Supplemental Information for the New Definition of the EF PHB (Expedited Forwarding Per-Hop Behavior)", RFC 3247, March 2002.
RFC3260	Grossman, D., "New Terminology and Clarifications for Diffserv", RFC 3260, April 2002.
RFC3289	Baker, F., Chan, K., and A. Smith, "Management Information Base for the Differentiated Services Architecture", RFC 3289, May 2002.
RFC3306	Haberman, B. and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 3306, August 2002.

RFC3307	Haberman, B., "Allocation Guidelines for IPv6 Multicast Addresses", RFC 3307, August 2002.
RFC3315	Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.
RFC3319	Schulzrinne, H. and B. Volz, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers", RFC 3319, July 2003.
RFC3392	Chandra, R. and J. Scudder, "Capabilities Advertisement with BGP-4", RFC 3392, November 2002.
RFC3410	Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, December 2002.
RFC3411	Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.
RFC3412	Case, J., Harrington, D., Presuhn, R., and B. Wijnen, "Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3412, December 2002.
RFC3413	Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.
RFC3414	Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.
RFC3415	Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.
RFC3416	Presuhn, R., Ed., "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3416, December 2002.
RFC3418	Presuhn, R., Ed., "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3418, December 2002.
RFC3484	Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", RFC 3484, February 2003.
RFC3493	Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, February 2003.
RFC3513	Hinden, R. and S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", RFC 3513, April 2003.

RFC3526	Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", RFC 3526, May 2003.
RFC3542	Stevens, W., Thomas, M., Nordmark, E., and T. Jinmei, "Advanced Sockets Application Program Interface (API) for IPv6", RFC 3542, May 2003.
RFC3566	Frankel, S. and H. Herbert, "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec", RFC 3566, September 2003.
RFC3572	Ogura, T., Maruyama, M., and T. Yoshida, "Internet Protocol Version 6 over MAPOS (Multiple Access Protocol Over SONET/SDH)", RFC 3572, July 2003.
RFC3590	Haberman, B., "Source Address Selection for the Multicast Listener Discovery (MLD) Protocol", RFC 3590, September 2003.
RFC3596	Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", RFC 3596, October 2003.
RFC3602	Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.
RFC3633	Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.
RFC3646	Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, December 2003.
RFC3678	Thaler, D., Fenner, B., and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", RFC 3678, January 2004.
RFC3686	Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.
RFC3736	Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.
RFC3775	Johnson, D., Perkins, C., and J. Arkko, "Mobility Support in IPv6", RFC 3775, June 2004.
RFC3776	Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, June 2004.
RFC3810	Vida, R., Ed., and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.
RFC3843	Jonsson, L-E. and G. Pelletier, "RObust Header Compression (ROHC): A Compression Profile for IP", RFC 3843, June 2004.
RFC3879	Huitema, C. and B. Carpenter, "Deprecating Site Local Addresses", RFC 3879, September 2004.

RFC3898	Kalusivalingam, V., "Network Information Service (NIS) Configuration Options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3898, October 2004.
RFC3919	Stephan, E. and J. Palet, "Remote Network Monitoring (RMON) Protocol Identifiers for IPv6 and Multi Protocol Label Switching (MPLS)", RFC 3919, October 2004.
RFC3948	Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.
RFC3956	Savola, P. and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, November 2004.
RFC3963	Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.
RFC3971	Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.
RFC3972	Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.
RFC3973	Adams, A., Nicholas, J., and W. Siadak, "Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)", RFC 3973, January 2005.
RFC3986	Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.
RFC4007	Deering, S., Haberman, B., Jinmei, T., Nordmark, E., and B. Zill, "IPv6 Scoped Address Architecture", RFC 4007, March 2005.
RFC4022	Raghunarayan, R., Ed., "Management Information Base for the Transmission Control Protocol (TCP)", RFC 4022, March 2005.
RFC4033	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.
RFC4034	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, March 2005.
RFC4035	Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.
RFC4038	Shin, M-K., Ed., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "Application Aspects of IPv6 Transition", RFC 4038, March 2005.
RFC4075	Kalusivalingam, V., "Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6", RFC 4075, May 2005.
RFC4087	Thaler, D., "IP Tunnel MIB", RFC 4087, June 2005.
RFC4106	Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

RFC4109	Hoffman, P., "Algorithms for Internet Key Exchange version 1 (IKEv1)", RFC 4109, May 2005.
RFC4113	Fenner, B. and J. Flick, "Management Information Base for the User Datagram Protocol (UDP)", RFC 4113, June 2005.
RFC4191	Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005.
RFC4193	Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.
RFC4213	Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
RFC4241	Shirasaki, Y., Miyakawa, S., Yamasaki, T., and A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service", RFC 4241, December 2005.
RFC4271	Rekhter, Y., Ed., Li, T., Ed., and S. Hares, Ed., "A Border Gateway Protocol 4 (BGP-4)", RFC 4271, January 2006.
RFC4282	Aboba, B., Beadles, M., Arkko, J., and P. Eronen, "The Network Access Identifier", RFC 4282, December 2005.
RFC4283	Patel, A., Leung, K., Khalil, M., Akhtar, H., and K. Chowdhury, "Mobile Node Identifier Option for Mobile IPv6 (MIPv6)", RFC 4283, November 2005.
RFC4291	Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
RFC4292	Haberman, B., "IP Forwarding Table MIB", RFC 4292, April 2006.
RFC4293	Routhier, S., Ed., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.
RFC4294	Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, April 2006.
RFC4295	Keeni, G., Koide, K., Nagami, K., and S. Gundavelli, "Mobile IPv6 Management Information Base", RFC 4295, April 2006.
RFC4301	Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.
RFC4302	Kent, S., "IP Authentication Header", RFC 4302, December 2005.
RFC4303	Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.
RFC4306	Kaufman, C., Ed., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
RFC4307	Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.
RFC4308	Hoffman, P., "Cryptographic Suites for IPsec", RFC 4308, December 2005.

RFC4309	Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.
RFC4311	Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, November 2005.
RFC4338	DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", RFC 4338, January 2006.
RFC4360	Sangli, S., Tappan, D., and Y. Rekhter, "BGP Extended Communities Attribute", RFC 4360, February 2006.
RFC4362	Jonsson, L-E., Pelletier, G., and K. Sandlund, "RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP", RFC 4362, January 2006.
RFC4364	Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.
RFC4380	Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006.
RFC4429	Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, April 2006.
RFC4434	Hoffman, P., "The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)", RFC 4434, February 2006.
RFC4443	Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.
RFC4489	Park, J-S., Shin, M-K., and H-J. Kim, "A Method for Generating Link-Scoped IPv6 Multicast Addresses", RFC 4489, April 2006.
RFC4495	Polk, J. and S. Dhesikan, "A Resource Reservation Protocol (RSVP) Extension for the Reduction of Bandwidth of a Reservation Flow", RFC 4495, May 2006.
RFC4541	Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.
RFC4543	McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.
RFC4552	Gupta, M. and N. Melam, "Authentication/Confidentiality for OSPFv3", RFC 4552, June 2006.
RFC4577	Rosen, E., Psenak, P., and P. Pillay-Esnault, "OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4577, June 2006.

RFC4581	Bagnulo, M. and J. Arkko, "Cryptographically Generated Addresses (CGA) Extension Field Format", RFC 4581, October 2006.
RFC4584	Chakrabarti, S. and E. Nordmark, "Extension to Sockets API for Mobile IPv6", RFC 4584, July 2006.
RFC4594	Babiarz, J., Chan, K., and F. Baker, "Configuration Guidelines for DiffServ Service Classes", RFC 4594, August 2006.
RFC4601	Fenner, B., Handley, M., Holbrook, H., and I. Kouvelas, "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, August 2006.
RFC4604	Holbrook, H., Cain, B., and B. Haberman, "Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast", RFC 4604, August 2006.
RFC4607	Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006.
RFC4609	Savola, P., Lehtonen, R., and D. Meyer, "Protocol Independent Multicast - Sparse Mode (PIM-SM) Multicast Routing Security Issues and Enhancements", RFC 4609, October 2006.
RFC4659	De Clercq, J., Ooms, D., Carugi, M., and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN", RFC 4659, September 2006.
RFC4684	Marques, P., Bonica, R., Fang, L., Martini, L., Raszuk, R., Patel, K., and J. Guichard, "Constrained Route Distribution for Border Gateway Protocol/MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)", RFC 4684, November 2006.
RFC4718	Eronen, P. and P. Hoffman, "IKEv2 Clarifications and Implementation Guidelines", RFC 4718, October 2006.
RFC4760	Bates, T., Chandra, R., Katz, D., and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 4760, January 2007.
RFC4807	Baer, M., Charlet, R., Hardaker, W., Story, R., and C. Wang, "IPsec Security Policy Database Configuration MIB", RFC 4807, March 2007.
RFC4809	Bonatti, C., Ed., Turner, S., Ed., and G. Lebovitz, Ed., "Requirements for an IPsec Certificate Management Profile", RFC 4809, February 2007.
RFC4815	Jonsson, L-E., Sandlund, K., Pelletier, G., and P. Kremer, "RObust Header Compression (ROHC): Corrections and Clarifications to RFC 3095", RFC 4815, February 2007.
RFC4821	Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, March 2007.

RFC4835	Manral, V., "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 4835, April 2007.
RFC4861	Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.
RFC4862	Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.
RFC4864	Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007.
RFC4868	Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.
RFC4869	Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 4869, May 2007.
RFC4877	Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, April 2007.
RFC4884	Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, April 2007.
RFC4890	Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.
RFC4891	Graveman, R., Parthasarathy, M., Savola, P., and H. Tschofenig, "Using IPsec to Secure IPv6-in-IPv4 Tunnels", RFC 4891, May 2007.
RFC4941	Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.
RFC4944	Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.
RFC4945	Korver, B., "The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX", RFC 4945, August 2007.
RFC4966	Aoun, C. and E. Davies, "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007.
RFC4982	Bagnulo, M. and J. Arkko, "Support for Multiple Hash Algorithms in Cryptographically Generated Addresses (CGAs)", RFC 4982, July 2007.
RFC4995	Jonsson, L-E., Pelletier, G., and K. Sandlund, "The RObust Header Compression (ROHC) Framework", RFC 4995, July 2007.
RFC4996	Pelletier, G., Sandlund, K., Jonsson, L-E., and M. West, "RObust Header Compression (ROHC): A Profile for TCP/IP (ROHC-TCP)", RFC 4996, July 2007.

RFC5006	Jeong, J., Ed., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Option for DNS Configuration", RFC 5006, September 2007.
RFC5014	Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, September 2007.
RFC5072	Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, September 2007.
RFC5095	Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.
RFC5114	Lepinski, M. and S. Kent, "Additional Diffie-Hellman Groups for Use with IETF Standards", RFC 5114, January 2008.
RFC5120	Przygienda, T., Shen, N., and N. Sheth, "M-ISIS: Multi Topology (MT) Routing in Intermediate System to Intermediate Systems (IS-ISs)", RFC 5120, February 2008.
RFC5121	Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, February 2008.
RFC5155	Laurie, B., Sisson, G., Arends, R., and D. Blacka, "DNS Security (DNSSEC) Hashed Authenticated Denial of Existence", RFC 5155, March 2008.
RFC5175	Haberman, B., Ed., and R. Hinden, "IPv6 Router Advertisement Flags Option", RFC 5175, March 2008.
RFC5225	Pelletier, G. and K. Sandlund, "RObust Header Compression Version 2 (ROHCv2): Profiles for RTP, UDP, IP, ESP and UDP-Lite", RFC 5225, April 2008.
RFC5304	Li, T. and R. Atkinson, "IS-IS Cryptographic Authentication", RFC 5304, October 2008.
RFC5305	Li, T. and H. Smit, "IS-IS Extensions for Traffic Engineering", RFC 5305, October 2008.
RFC5308	Hopps, C., "Routing IPv6 with IS-IS", RFC 5308, October 2008.
RFC5310	Bhatia, M., Manral, V., Li, T., Atkinson, R., White, R., and M. Fanto, "IS-IS Generic Cryptographic Authentication", RFC 5310, February 2009.
RFC5340	Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.
RFC5453	Krishnan, S., "Reserved IPv6 Interface Identifiers", RFC 5453, February 2009.
RFC5492	Scudder, J. and R. Chandra, "Capabilities Advertisement with BGP-4", RFC 5492, February 2009.
RFC5555	Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, June 2009.

RFC5701	Rekhter, Y., "IPv6 Address Specific BGP Extended Community Attribute", RFC 5701, November 2009.
RFC5722	Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, December 2009.
RFC5790	Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, February 2010.
RFC5795	Sandlund, K., Pelletier, G., and L-E. Jonsson, "The RObust Header Compression (ROHC) Framework", RFC 5795, March 2010.
RFC5798	Nadas, S., Ed., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, March 2010.
RFC5838	Lindem, A., Ed., Mirtorabi, S., Roy, A., Barnes, M., and R. Aggarwal, "Support of Address Families in OSPFv3", RFC 5838, April 2010.
RFC5908	Gayraud, R. and B. Lourdelet, "Network Time Protocol (NTP) Server Option for DHCPv6", RFC 5908, June 2010.
RFC5942	Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, July 2010.
RFC5969	Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.
RFC5996	Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.
RFC6040	Briscoe, B., "Tunnelling of Explicit Congestion Notification", RFC 6040, November 2010.
RFC6071	Frankel, S. and S. Krishnan, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap", RFC 6071, February 2011.
RFC6106	Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.
RFC6141	Camarillo, G., Ed., Holmberg, C., and Y. Gao, "Re-INVITE and Target-Refresh Request Handling in the Session Initiation Protocol (SIP)", RFC 6141, March 2011.
RFC6164	Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", RFC 6164, April 2011.
RFC6204	Singh, H., Beebee, W., Donley, C., Stark, B., and O. Troan, Ed., "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011.
RFC6275	Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

RFC6296	Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011.
RFC6379	Law, L. and J. Solinas, "Suite B Cryptographic Suites for IPsec", RFC 6379, October 2011.
RFC6380	Burgin, K. and M. Peck, "Suite B Profile for Internet Protocol Security (IPsec)", RFC 6380, October 2011.
RFC6398	Le Faucheur, F., Ed., "IP Router Alert Considerations and Usage", BCP 168, RFC 6398, October 2011.
RFC6434	Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.
RFC6437	Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, November 2011.
RFC6540	George, W., Donley, C., Liljenstolpe, C., and L. Howard, "IPv6 Support Required for All IP-Capable Nodes", BCP 177, RFC 6540, April 2012.
RFC6945	Gont, F. „Processing of IPv6 "Atomic" Fragments", RFC6946, May 2013.

8. Glossar

.NET	.NET bezeichnet eine von Microsoft entwickelte Software-Plattform zur Entwicklung und Ausführung von Anwendungsprogrammen. Diese besteht aus einer Laufzeitumgebung, in der die Programme ausgeführt werden, sowie einer Sammlung von Klassenbibliotheken, Programmierschnittstellen und Dienstprogrammen (Services).
6in4	Ein Transitionsverfahren zur Migration von IPv4 zu IPv6, bei dem der IPv6-Verkehr über IPv4-Tunnel übertragen wird, wobei eine feste, vorkonfigurierte Zuordnung zwischen IPv6- und IPv4-Zieladressen besteht (siehe [RFC4213]).
6over4	Ein Transitionsverfahren zur Migration von IPv4 zu IPv6, bei dem der IPv6-Verkehr zwischen Dual-Stack-Knoten über einen IPv4-Multicast-Tunnel übertragen wird. Die IPv6-Seite jedes empfangenden Knotens entscheidet unabhängig über das weitere Vorgehen (lokale Zustellung und/oder Weiterleitung).
6to4	Ein Transitionsverfahren zur Migration von IPv4 zu IPv6, bei dem der IPv6-Verkehr über IPv4-Tunnel übertragen wird, wobei auf jede IPv4-Adresse ein /48 großes IPv6-Netz abgebildet. Die IPv6-Adresse setzt sich aus dem Präfix 2002::/16 und der hexadezimal notierten IPv4-Adresse zusammen.
Active Directory	Ein auf LDAP basierender Verzeichnisdienst der Firma Microsoft.
AD	(siehe Active Directory)
ALG	(siehe Application Level Gateway)

Anforderungsgrad (Migrationsleitlinie)	In den IPv6-Profilen und in den IPv6-Migrationsleitlinien werden definierte Anforderungsgrade verwendet, um die Empfehlungen eindeutig zu kennzeichnen. verpflichtend / muss: Die beschriebene Eigenschaft muss in dieser Form aus technischen oder aus administrativen Gründen umgesetzt werden, da anders das gewollte Verhalten nicht erreicht werden kann. empfohlen / sollte: Die Nutzung der Funktion wird als sinnvoll angesehen. Abhängig von den Gegebenheiten und Anforderungen im Einzelfall kann hiervon auch abgewichen werden. optional / darf: Die beschriebene Funktion ist optional und muss nicht bereitgestellt werden.
Anycast	Anycast ist eine Adressierungsart in Computernetzen, bei der man über eine einzelne IP-Adresse genau einen Rechner aus einer Gruppe von Rechnern ansprechen kann, welche mit dieser Adresse konfiguriert sind. Es antwortet derjenige Rechner, welcher über die kürzeste Route erreichbar ist bzw. auf eine andere, festgelegte Art topologisch „am nächsten“ ist.
Application Level Gateway	Filterfunktionen oberhalb der Transportschicht werden von einem sogenannten Application-Level Gateway, auch Sicherheits-Proxy genannt, übernommen. Mittels eines Proxys lassen sich Datenströme auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten. Das ALG kann zudem die strikte Einhaltung von Anwendungsprotokollen erzwingen, unerwünschte Anwendungsdaten aus den Datenpaketen entfernen (bzw. austauschen) oder Verbindungen anwendungsspezifisch protokollieren.
AS	(siehe Autonomes System)
Autonomes System (engl. Autonomous System)	Ein autonomes System (AS) ist eine Ansammlung von IP-Netzen, welche als Einheit verwaltet werden und über ein (oder auch mehrere) gemeinsames internes Routing-Protokoll (IGP) verbunden sind. Diese Definition ist insbesondere für den Einsatz des Internet-Routing-Protokolls oder Exterior-Gateway-Protokolls BGP notwendig, welches die Verbindungswege zwischen mehreren autonomen Systemen weitergibt.

Backend	Das Backend ist im Gegensatz zum Frontend der Teil eines Serververbundes oder eines Computersystems, der sich weiter entfernt vom Nutzer befindet, z. B. in einem Rechenzentrum. Es wird benutzt, um interne Dienste bereitzustellen oder miteinander zu verbinden. Ein Backend-Netzwerk benötigt typischerweise eine hohe Bandbreite und wird nicht direkt von Nutzern angesprochen, sondern nur durch vorgeschaltete Server.
BGP	(siehe Border Gateway Protocol)
Border Gateway Protocol	Das Border Gateway Protocol ist das verwendete Routing-Protokoll des Internets und gehört zu den Exterior-Gateway-Protokollen (EGP), de facto ist es das einzige EGP. Über BGP ist es nicht nur möglich, die Kommunikation innerhalb eines Autonomen Systems zu gewährleisten, sondern auch Provider-übergreifend. Es beschreibt, wie Router untereinander Informationen über die Verfügbarkeit von Verbindungswegen zwischen den Netzen unterschiedlicher autonomer Systeme (AS) weitergeben. BGP liegt aktuell in der Version 4 vor und ist in [RFC4271] beschrieben.
CGA	(siehe Cryptographically Generated Adresses)
Client	Als Client werden Software und Hardware bezeichnet, die bestimmte Dienste von einem entfernten Server in Anspruch nehmen können. Häufig steht der Begriff Client für einen Arbeitsplatzrechner (siehe Klientensystem), der in einem Netz auf Daten und Programme eines Servers zugreift.
CMS	(siehe Content Management System)
Content Management System	Ein Content-Management-System (CMS) dient der gemeinschaftlichen Erstellung, Bearbeitung und Organisation von Web-Inhalten. Diese können aus Text- und Multimedia-Dokumenten bestehen. Ein Autor kann ein solches System in den meisten Fällen ohne Programmier- oder HTML-Kenntnisse bedienen.
Cryptographically Generated Adresses	Eine Cryptographically Generated Address (CGA) ist eine IPv6-Adresse, deren Host Indentifier (Schnittstellenadresse, untere 64 Bits der IPv6-Adresse) über eine Einweg-Hashfunktion erzeugt wurde. Mittels der CGA kann bei SEND (Secure Neighbor Discovery Protocol) ein Public Key (siehe Signatur) an eine IPv6-Adresse gebunden werden.

Datenbanksystem	Ein Datenbanksystem (DBS) ist ein System zur elektronischen Datenverwaltung. Die wesentliche Aufgabe eines DBS ist es, große Datenmengen effizient, widerspruchsfrei und dauerhaft zu speichern und benötigte Teilmengen in unterschiedlichen, bedarfsgerechten Darstellungsformen für Benutzer und Anwendungsprogramme bereitzustellen. Ein DBS besteht aus zwei Teilen: der Verwaltungssoftware, genannt Datenbankmanagementsystem (DBMS) und der Menge der zu verwaltenden Daten, der eigentlichen Datenbank.
Demilitarisierte Zone	Eine Demilitarisierte Zone (DMZ) ist ein Zwischennetz, das an Netzübergängen gebildet wird und ein eigenes Netz darstellt, welches nicht so stark gesichert ist wie das eigentlich zu schützende, interne Netz. Eine DMZ wird oft verwendet, um darin Server zu betreiben, die von außen erreichbar sein sollen (z. B. der öffentliche Webserver einer Institution).
DHCP	(siehe Dynamic Host Configuration Protocol)
Dienst (engl. Service)	Der Begriff Dienst (auch Service) beschreibt in der Informatik allgemein eine technische, autarke Einheit, die zusammenhängende Funktionalitäten zu einem Themenkomplex bündelt und über eine klar definierte Schnittstelle zur Verfügung stellt. Typische Beispiele sind z. B. Webservices, die Funktionalitäten für Dritte über das Inter- bzw. Intranet verfügbar machen, Netzwerkdienste, Systemdienste oder auch Telekommunikationsdienste.
Directory	(vgl. Verzeichnisdienst)
DMZ	(siehe Demilitarisierte Zone)
DNS	(siehe Domain Name System)
Domain Name System	Das Domain Name System übersetzt alphanumerische Adressnamen (z. B. www.bsi.bund.de) in numerische Adressen (z. B. 194.95.177.86). Auch eine Übersetzung in die umgekehrte Richtung ist mit einem DNS-Server möglich (sog. Reverse DNS).
Dual-Stack	Das Gerät oder die Softwarekomponente ist sowohl über IPv4 als auch über IPv6 direkt erreichbar und verfügt dafür über entsprechende IPv4- und IPv6-Adressen, es ist über die Adressen in die entsprechenden Netze eingebunden und kann über beide Protokolle unabhängig kommunizieren.

Dynamic Host Configuration Protocol	Das Dynamic Host Configuration Protocol (DHCP) ermöglicht die Zuweisung der Netzwerkkonfiguration an Clients durch einen Server. Durch DHCP ist die automatische Einbindung eines Computers in ein bestehendes Netzwerk ohne manuelle Konfiguration möglich.
EGP	(siehe Exterior Gateway Protocol)
EIGRP	(siehe Enhanced Interior Gateway Routing Protocol)
Ende-zu-Ende-Kommunikation	Ende-zu-Ende-Kommunikation bezieht sich eine durchgängige, transparente Kommunikation oberhalb der Netzwerkschicht. Zur Nutzung eines Dienstes oder einer Anwendung wird der gesamte logische Kommunikationspfad zwischen Client und Server betrachtet, was z. B. Sicherheitskomponenten auf dem Übertragungsweg einschließen kann. Aufgrund des großen Adressumfangs erlaubt IPv6 wieder eine Umsetzung der Ende-zu-Ende-Kommunikation ohne einen Eingriff in der Transportschicht. Dies kann in einigen Anwendungsfällen aufgrund von Sicherheitsanforderungen nicht erwünscht sein.
Endsystem	Ein Endsystem ist ein Knoten, der Anwendungsfunktionen enthält, ausschließlich die von ihm selbst erzeugten Pakete versendet und nur für ihn selbst bestimmte ankommende Pakete bearbeitet.
Enhanced Interior Gateway Routing Protocol (EIGRP)	EIGRP ist ein 1992 von Cisco veröffentlichtes proprietäres Routing-Protokoll. Bei EIGRP handelt es sich um eine verbesserte Version des früheren IGRP, zu welchem weiterhin Kompatibilität besteht. EIGRP ist ein erweitertes Distance-Vector-Routingprotokoll, welches sich beim Austausch mit benachbarten Geräten sowie bei der Speicherung von Routing-Informationen wie ein Link-State-Routingprotokoll verhält. Mit Hilfe dieser Link-State-Eigenschaften erreicht EIGRP im Verhältnis zu konventionellen Distance-Vector-Routingprotokollen eine sehr schnelle Konvergenz und ist immun gegenüber Routing-Schleifen.

Exterior Gateway Protocol	Ein Exterior-Gateway-Protokoll (EGP) dient dazu, Erreichbarkeitsinformationen zwischen Autonomen Systemen (AS) auszutauschen, d. h. Informationen darüber, welche Netze untereinander erreichbar sind. Diese Daten setzen dann die Router der autonomen Systeme in interne Routing-Informationen für Intradomain-Routingprotokolle wie z. B. OSPF oder das Routing Information Protocol (RIP) um. Das einzige derzeitige EGP ist das Border Gateway Protokoll (BGP).
Extranet	Das Extranet (nach ISO/IEC 2382) ist eine Erweiterung des Intranets um eine Komponente, die nur von einer festgelegten Gruppe externer Benutzer verwendet werden kann. Extranets dienen der Bereitstellung von Informationen, die zum Beispiel Unternehmen, Kunden oder Partnern zugänglich gemacht werden, nicht aber der Öffentlichkeit.
Fachanwendung, Fachverfahren	Die Fachanwendung (oder Fachverfahren) ist ein Begriff der Informationstechnik und bezeichnet eine für einen Kunden oder eine Branche angefertigte Anwendungssoftware. Aktuelle Fachverfahren basieren oft auf Standardkomponenten und –Diensten und sind z. B. auf einem Applikationsserver implementiert (siehe auch Querschnittsdienste).
Fat Client	Ein Fat Client (oder Rich Client) bezeichnet innerhalb der elektronischen Datenverarbeitung ein Klientensystem, bei dem die eigentliche Verarbeitung der Daten lokal auf dem Client vollzogen wird. Meistens wird auch eine grafische Benutzeroberfläche zur Verfügung gestellt. Der Gegensatz dazu ist der Thin Client.
Firewall	Eine Firewall ist ein Transitsystem, das nur die zugelassenen Pakete weiterleitet. Eine Firewall (auch als Sicherheits-Gateway bezeichnet) bildet dabei ein System aus Soft- und Hardware-Komponenten, um IP-Netze sicher zu koppeln. Die Firewall filtert dazu eingehende Datenpakete anhand von Regelwerken auf Basis von Adressdaten, Protokolltypen und/oder Eigenschaften der OSI-Schichten 2 bis 4. Dazu kann auch eine Reassemblierung der paketbasierten Datenströme erforderlich sein.

Frontend (engl.)	Ein Frontend ist die Kommunikationsschnittstelle zwischen einem IT-System und dem Nutzer. Ein einfaches Frontend kann z. B. aus einer Eingabemaske bestehen, in die der Benutzer Daten eingibt, welche über die Middleware an das Backend weitergeleitet werden.
Host	Als Host wird ein in einem Rechnernetz eingebundenes Rechnersystem mit zugehörigem Betriebssystem bezeichnet,
ICMP	(siehe Internet Control Message Protocol)
IDS	(siehe Intrusion Detection System)
IDS	(siehe Intrusion Detection System)
IGP	(siehe Interior Gateway Protocol)
Infrastruktur-Router	(siehe Router)
Interface Identifier	Niederwertiger Teil einer IPv6-Adresse, bestehend aus den unteren 64 Bits der 128 Bits großen IPv6-Adresse.
Interior Gateway Protocol	Als Interior Gateway Protocol (IGP) werden Routing-protokolle bezeichnet, die innerhalb von Autonomen Systemen eingesetzt werden. Im Gegensatz zu Exterior-Gateway-Protokollen (EGP) zeichnen sie sich durch besondere Fähigkeiten im Umgang mit komplizierten Netzwerktopologien aus. Zu den IGPs gehören OSPF, RIP(ng), IS-IS und EIGRP.
Intermediate System to Intermediate System	Das IS-IS-Protokoll (IS-IS) ist ein Router-Protokoll im OSI-Umfeld, das Router untereinander benutzen, um Routing-Informationen, Fehlermeldungen, Statusmeldungen etc. auszutauschen. Das IS-IS-Protokoll arbeitet nach einem ähnlichen Konzept wie das OSPF-Protokoll. IS-IS für IPv4 ist in [RFC1142] beschrieben. In [RFC5308] ist IS-IS für IPv6 definiert.

Internet Control Message Protocol [engl.]	Das Internet Control Message Protocol (ICMP) transportiert Fehler- und Diagnoseinformationen, wobei sich die Standards für IPv4 und IPv6 unterscheiden. Es wird intern von TCP, UDP und den beiden IP-Protokoll-Versionen genutzt und kommt z. B. zum Einsatz, wenn Datenpakete nicht ausgeliefert werden können, ein Gateway Datenverkehr über eine kürzere Route leiten möchte oder ein Gateway nicht genug Pufferkapazität für die zu verarbeitenden Daten besitzt und dafür eine Fehlermeldung signalisieren will.
Internet Protocol Security	Internet Protocol Security (IPsec) ist eine Sicherheitsprotokoll-Suite, die für die Kommunikation über IP-Netze die Schutzziele Vertraulichkeit, Authentizität und Integrität gewährleisten soll. Im Gegensatz zu anderen Verschlüsselungsprotokollen wie etwa SSL arbeitet IPsec direkt auf der Vermittlungsschicht (network layer) des TCP/IP-Protokollstapels (entspricht Schicht 3 des OSI-Modells).
Interoperabilität	Eigenschaft von IT-Systemen und -Anwendungen, miteinander kommunizieren zu können. Interoperabilität bezieht sich immer auf eine oder mehrere Ebenen des OSI-Referenzmodells oder spezielle Kommunikationsaspekte. Die Art der Interoperabilität muss deshalb stets genauer beschrieben werden.
Intranet (engl. intranet)	Ein Intranet ist ein terminales Netz, das sich unter vollständiger Kontrolle genau eines Netzbetreibers (also der jeweiligen Behörde oder des Unternehmens) befindet. Meist werden Zugriffe aus anderen Netzen (wie dem Internet) durch ein Sicherheits-Gateway verhindert oder nur mit speziellen Regeln zugelassen.
Intrusion Detection System	Ein Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen auf ein Rechnersystem oder Rechnernetz. Es beobachtet die Kommunikation innerhalb eines Netzes und erkennt Einbrüche anhand verschiedener Metriken (beispielsweise anhand ungewöhnlicher Kommunikationsmuster). Einbrüche werden aufgezeichnet und gemeldet.
Intrusion Detection System [engl.]	Ein Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen auf ein Rechnersystem oder Rechnernetz.

Intrusion Prevention System	Ein Intrusion Prevention System (IPS) ist eine Erweiterung eines IDS. Ein IPS erkennt und meldet Angriffe nicht nur, sondern kann Angriffe aktiv abwehren. Mögliche Aktionen sind dabei das Verwerfen der zu einem erkannten Angriff gehörenden IP-Pakete oder das dynamische Ändern von Filtereinstellung am Sicherheits-Gateway.
IPS	(siehe Intrusion Prevention System)
IPsec	(siehe Internet Protocol Security)
IPv4 (Internet Protocol Version 4)	Das Internet Protocol Version 4 ist ein verbindungsloses Protokoll der Vermittlungsschicht (network layer) und erlaubt den Austausch von Daten zwischen zwei Rechnern ohne vorherigen Verbindungsaufbau. IPv4 setzt nicht voraus, dass das darunterliegende Netzwerk eine Fehlererkennung durchführt. Ferner verfügt es über keine Verlässlichkeits- oder Flusssteuerungsmechanismen. Die meisten dieser Anforderungen gibt IPv4 an die nächsthöhere Schicht – die Transportschicht – weiter.
IPv4-only	Mit IPv4-only werden Netzwerke bezeichnet, die ausschließlich IPv4 unterstützen, d. h., alle Geräte oder Softwarekomponenten im Netzwerk sind nur über das IPv4-Protokoll erreichbar.
IPv6 (Internet Protocol Version 6)	Das Internet Protocol Version 6 (IPv6) ist die Nachfolgeversion von IPv4 und soll dieses langfristig ablösen, da es u. a. die Zahl der verfügbaren Rechner-adressen stark erweitert und zusätzliche Funktionen zur Unterstützung von Autokonfiguration und Sicherheit bereitstellt. IPv4 und IPv6 sind nicht direkt kompatibel, sodass für die Kommunikation zwischen Systemen, die IPv4 nutzen und solchen, die IPv6 nutzen, eine Protokollumsetzung stattfinden muss oder die Systeme für den Dual-Stack-Betrieb konfiguriert werden müssen.
IPv6-only	IPv6-only sind Netzwerke, die nur IPv6 unterstützen, das heißt, alle Geräte und Softwarekomponenten im Netzwerk sind nur über das IPv6-Protokoll erreichbar.
IS-IS	(siehe Intermediate System To Intermediate System)
ISPs der ÖV	Internet-Serviceprovider zur Anbindung der deutschen öffentlichen Verwaltungen an das Internet

Java	Eine objektorientierte Programmiersprache und ein Bestandteil der von SUN entwickelten Java-Technologie – diese besteht grundsätzlich aus Entwicklungswerkzeug zum Erstellen von Programmen und der Laufzeitumgebung zu deren Ausführung.
Klientensystem	Ein Klientensystem ist ein Endsystem, das Anwendungsfunktionen und Nutzerschnittstellen für den Zugang zu und die lokale Verarbeitung von lokal oder entfernt gespeicherten, erfassten oder produzierten Daten enthält. Gleichzeitig oder alternativ kann auch der Zugang zu entfernten Anwendungsfunktionen ermöglicht werden.
Knoten	Als Knoten wird (in diesem Kontext) jedes Netzelement bezeichnet, das eine oder mehrere IP-basierte Nutzdaten-Schnittstellen besitzt. Über die Nutzdaten-Schnittstellen können auch Management-Protokolle abgewickelt werden.
Konformität	In diesem Zusammenhang die Eigenschaft eines Kommunikationssystems, den für diesen Systemtyp festgelegten Anforderungen und Protokollspezifikationen zu entsprechen (siehe auch Interoperabilität).
Konnektivität	Die Kommunikationsfähigkeit eines Knotens mit einem (oder mehreren) Netzwerk(en) oder anderen Knoten. Sie bezieht sich immer auf eine oder mehrere Ebenen des OSI-Referenzmodells oder spezielle Kommunikationsaspekte. Die Art der Konnektivität muss deshalb stets genauer beschrieben werden. Typische Beispiele sind Konnektivität bzgl. Adressierung und Routing.
LAMP (Linux, Apache, MySQL, PHP)	Abkürzung für eine Webserver-Umgebung bestehend aus dem Betriebssystem *Linux* sowie den Software-Produkten *Apache*, *MySQL* und *PHP* (teilweise auch zzgl. Perl oder Python, dann LAMPP genannt).
LDAP	(siehe Lightweight Directory Access Protocol)
Lightweight Directory Access Protocol	Ein Anwendungsprotokoll, das die Abfrage und Modifikation von Informationen eines Verzeichnisdienstes über ein IP-Netzwerk erlaubt. Die aktuelle Version ist in RFC4510 und RFC4511 spezifiziert.
LIR	(siehe Local Internet Registry)

Local Internet Registry	Eine Organisation, der von einer Regional Internet Registry (RIR) ein Block von IP-Adressen zugeteilt wurde und die damit ihre Endkunden bedient. Die meisten LIRs sind Internet-Serviceprovider, Unternehmen oder akademische Institutionen.
Middlebox (engl.)	Eine Middlebox kann Pakete ändern und blockieren, muss aber nicht am Routing teilnehmen. Dieser Oberbegriff bezeichnet verschiedene Komponenten im Datenpfad, bspw. Firewall oder NAT.
Middleware	In der Informatik: anwendungsneutrale Programme, die so zwischen Anwendungen vermitteln, dass die Komplexität dieser Applikationen und ihre Infrastruktur verborgen werden. Im Gegensatz zu niveautieferen Netzwerkdiensten, welche die einfache Kommunikation zwischen Rechnern handhaben, unterstützt Middleware die Kommunikation zwischen Prozessen.
MLD	(siehe Multicast Listener Discovery)
Mobiler Arbeitsplatz	(siehe Klientensystem)
Mobiltelefon	(siehe Klientensystem)
Multicast	Eine Übertragungsart von einem Punkt, resp. einem Sender, zu einer definierten Gruppe von Empfängern. Das können auch festgelegte Netzwerkknoten sein. Man spricht bei Multicast auch von Punkt-zu-Mehrpunkt-Verbindung (P2MP). Der Vorteil des Multicasting liegt darin, dass Nachrichten über eine Adresse gleichzeitig an mehrere Teilnehmer übertragen werden können, ohne dass sich dabei protokollbedingt die benötigte Bandbreite mit der Anzahl der Empfangseinrichtungen vervielfältigt. Bei IPv6 wird Multicast als eine grundlegende Übertragungsart genutzt, auch zur Konfiguration der beteiligten Knoten.
NAT	(siehe Network Address Translation)
NAT-PT	Der Network Address Translator, Protocol Translator (NAT-PT) ist eine Netzkomponente, die als Übersetzungskomponente für die Datenpakete der IP-Protokolle in den Versionen IPv4 in IPv6 fungiert. Solche Komponenten, die sich in der Regel in Routern befinden, dienen der Migration zwischen IPv4- und IPv6-Netzen.
ND / NDP	(siehe Neighbor Discovery Protocol)

Neighbor Discovery Protocol	Das Neighbor Discovery Protocol (NDP) wird von den Knoten eines IPv6-Netzwerkes benutzt, um die Link-Layer-Adresse von anderen Knoten desselben Netzwerkes zu ermitteln. Für alle Knoten außerhalb des eigenen Netzwerkes wird NDP benutzt, um einen Router zu finden, der die Pakete weiterleiten kann. Damit ist NDP ein Ersatz für das Address Resolution Protocol (ARP) von IPv4.
Network Address Translator – Protocol Translator	Eine Netzkomponente, die als Übersetzungskomponente für die Datenpakete der IP-Protokolle in den Versionen IPv4 in IPv6 fungiert. Solche Komponenten, die sich in der Regel in Routern befinden, dienen der Kommunikation zwischen IPv4- und IPv6-Netzen. NAT-PT setzt nicht nur die Adressen, sondern die gesamten Pakete um.
Netzinfrastrukturdienste	Unter Netzinfrastrukturdiensten werden in diesem Dokument zusammenfassend Dienste bezeichnet, die für den Betrieb des Netzes selbst wichtig oder in der gewählten Konfiguration notwendig sind. Normalerweise sind dies mindestens DHCP und DNS (siehe auch Querschnittsdienste).
Netzübergang	Die Schnittstelle zwischen zwei unterschiedlichen Netzwerken. Einer solchen Schnittstelle obliegt die Anpassung der physikalischen Übertragungsmedien sowie der Netzwerk-, Transport- und Anwendungsprotokolle. In der Regel wird ein solcher Netzübergang von einem Gateway gebildet. Die Anpassung betrifft die in der Vermittlungsschicht realisierte Datenvermittlungstechnik mit den Netzwerkprotokollen, die Transportschicht mit der Anpassung der Transportprotokolle und nicht zuletzt die Anwendungsschicht mit der Transcodierung der Anwendungsdaten.
Node	(siehe auch Knoten)
Online Services Computer Interface	Ein Protokollstandard für die deutsche öffentliche Verwaltung. Er steht für mehrere Protokolle, deren gemeinsames Merkmal die besondere Eignung für das E-Government ist. OSCI-Transport dient der sicheren, vertraulichen und rechtsverbindlichen Übertragung digitaler Daten über das Internet mittels einer Reihe verschiedener Protokolle (OSCI-XÖV-Standards) für den Austausch fachlicher Inhaltsdaten auf XML-Basis zwischen Kunden und Behörden bzw. Behörden untereinander.

Open Shortest Path First	Ein dynamisches Routing-Protokoll innerhalb eines autonomen Systems. Es hat das Routing Information Protocol (RIP) als Standard-Interior Gateway Protocol (IGP) insbesondere bei großen Netzen abgelöst. Es ist ein Link-State-Routing-Protokoll, das auf dem von Edsger Wybe Dijkstra entwickelten Algorithmus „Shortest Path First“ basiert. Ein großer Vorteil gegenüber dem Routing Information Protocol (RIP) ist, dass jeder Router die vollständige Netztopologie kennt. Unter IPv4 wird OSPF in Version 2 verwendet, welche in [RFC2328] spezifiziert ist. Unter IPv6 wird die Version 3 verwendet, welche in [RFC5340] spezifiziert ist.
OSCI	(siehe Online Services Computer Interface)
OSPF	(siehe Open Shortest Path First)
Paketfilter	IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiter zu leiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.
Perimeter-Router	Ein Router an einer administrativen Grenze, auch Edge Router oder Border-Router genannt.
PKI	(siehe Public Key Infrastructure)
Präfix	Oberer, höherwertiger Teil einer IPv6-Adresse
Proxy	Eine Art Stellvertreter in bzw. Insbesondere zwischen Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.
Public Key Infrastructure	Sicherheitsinfrastruktur, die es ermöglicht, in nicht gesicherten Netzen (z. B. im Internet) auf der Basis eines von einer vertrauenswürdigen Stelle ausgegebenen Schlüsselpaares verschlüsselt Daten auszutauschen bzw. Signaturen zu erzeugen und zu prüfen.

Querschnittsdienste	Als Querschnittsdienste werden in diesem Dokument zusammenfassend grundlegende, netzbasierte Anwendungen bezeichnet (z. B. LDAP-Server, Fileserver, Mail- und Webserver, Datenbanksystem), die auf einer betriebsbereiten Netzinfrastruktur aufsetzen (siehe auch Netzinfrastrukturdienste) und auf denen Fachanwendungen aufsetzen können.
Regional Internet Registry	Eine regional mit der Verwaltung und Zuteilung von Internet-Ressourcen betraute Organisation. Die Zuständigkeit umfasst die Verwaltung von IP-Adressen (IPv4 und IPv6) sowie AS-Nummern. Es gibt weltweit derzeit fünf RIRs, grob entsprechend den Kontinenten der Erde.
Remote Desktop	Unter Remote-Desktop wird meistens der Fernwartungszugriff auf ein Klientensystem über ein lokales Netz oder das Internet verstanden.
Request for Comments	In Request for Comments (RFC) werden wichtige Internet-Standards festgelegt. RFCs können bei der Internet Engineering Task Force (IETF) eingereicht werden, die die Entscheidung trifft, ob der Vorschlag zum Standard erhoben wird. RFCs werden nummeriert und nicht mehr verändert. Sollen bestehende RFCs verändert oder erweitert werden, so geschieht dies, indem ein neuer RFC mit einer neuen Nummer und mit den entsprechenden Neuerungen geschaffen wird.
Reverse DNS	(siehe Domain Name System)
RFC	(siehe Request for Comments)
Rich Client	(siehe Fat Client)
RIP	(siehe Routing Information Protocol)
RIR	(siehe Regional Internet Registry)
Router	Ein Knoten, der IP-Pakete auf Basis komplexer Regeln zwischen verschiedenen Nutzdaten-Schnittstellen vermittelt und weiterleitet. Die Regeln können manuell und/oder über Internet- oder proprietäre Protokolle konfiguriert werden. Router verbinden IP-Netze auf der Vermittlungsschicht und begrenzen die Broadcast-Domäne eines Ethernets.

Routing Information Protocol	Das Routing Information Protocol (RIP) ist ein Routing-Protokoll auf Basis des Distanzvektoralgorithmus, das innerhalb eines autonomen Systems (z. B. LAN) eingesetzt wird, um die Routingtabellen von Routern automatisch zu erstellen. Es gehört zur Klasse der Interior Gateway Protocols (IGP). RIP liegt für IPv4 in der Version 2 [RFC2453] vor. Unter dem Namen RIPng (RIP next generation) wurde es erweitert, um IPv6 zu unterstützen.
Secure Neighbor Discovery	Das SEcure Neighbor Discovery (SEND) Protokoll (siehe [RFC3971]) ist eine Sicherheitserweiterung für das Neighbor Discovery Protocol (NDP).
SEND	(siehe Secure Neighbor Discovery)
Server	Ein Serversystem oder kurz Server ist ein Endsystem, das Klientensystemen Daten oder Anwendungsfunktionen zur entfernten Nutzung bereitstellt und typischerweise im Backend zu finden ist. Ein Server kann sich dazu weiterer Server bedienen, denen gegenüber er sich dabei in der Rolle eines (speziellen) Klientensystems befindet. Beispiele sind Applikations-, Daten-, Web-, Print oder E-Mail-Server.
Service	(siehe Dienst)
Service Level Agreement	Der Begriff Service-Level-Agreement (SLA) oder Dienstgütevereinbarung (DGV) bezeichnet einen Vertrag zwischen Auftraggeber und Dienstleister, der Leistungseigenschaften für Dienste beschreibt, bspw. Dienstgüte oder Reaktionszeit.
Sicherheits-Gateway	Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen Kommunikation auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

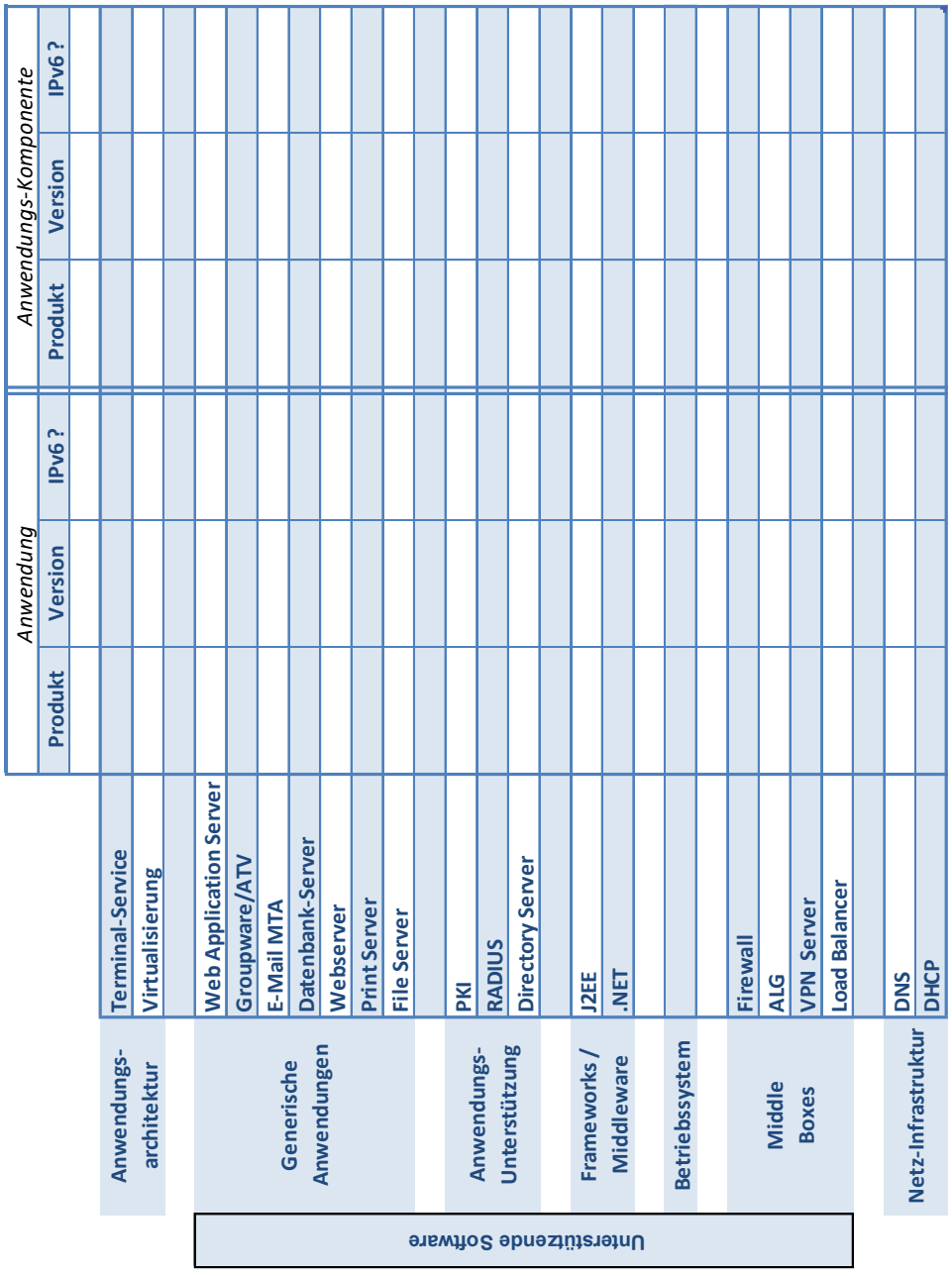
Sicherheitskomponente	Unter dem Begriff Sicherheitskomponente sind alle Komponenten zusammengefasst, deren Aufgabe es ist, den Netzbetrieb und die transportierten Nutzdaten gegen Angriffe zu schützen. Sicherheitskomponenten sind, abhängig von ihrer Aufgabe, Transitsysteme, Endsysteme oder auf Endsystemen installiert.
Sicherheits-Proxy	(siehe Applikation Level Gateway)
Signatur	Zeichenfolge, die über eine Datei oder eine andere Zeichenfolge mittels einer mathematischen Funktion gebildet wird. Sie dient z. B. zur Authentifizierung eines Nutzers, einer E-Mail oder einer IPv6-Adresse.
SLA	(siehe Service Level Agreement)
SLAAC	(siehe Stateless Address Autoconfiguration)
SmartPhone	(siehe Klientensystem)
SOHO-Router	Router für die speziellen Bedürfnisse in einer kleinen Verwaltung (Small Office / Home Office (SOHO)), beispielsweise durch die Integration einer DSL-WAN-Schnittstelle (dann auch DSL-Router genannt). (Siehe auch Router.)
Stateless Address Autoconfiguration	Mittels Stateless Address Autoconfiguration (SLAAC, zustandslose Adressenautokonfiguration) kann ein Host vollautomatisch eine funktionsfähige Internetverbindung aufbauen. Dazu wird eine link-lokale Adresse auf dem Host erzeugt. Anschließend kommuniziert der Host über das Neighbor Discovery Protocols (NDP) mit den für sein Netzwerksegment zuständigen Routern, um die notwendige Konfiguration zu ermitteln.
Switch	Ein Switch ist eine Netz-Komponente zur Verbindung mehrerer Netz-Segmente in einem lokalen Netz, dz.ie Weiterleitung von Paketen erfolgt ausschließlich auf der Basis von Schicht-2-Adressdaten (Schicht-2-Switch). Werden IP-Adressdaten berücksichtigt, so spricht man von einem Schicht-3-Switch, der auch Routing-Protokolle unterstützen kann. Beide Typen können eine IP-basierte Management-Schnittstelle besitzen.
Tablet	(siehe Klientensystem)

Thin Client	Eine Anwendung oder ein Computer als Endgerät (Terminal) eines Netzwerkes, in dem im Gegensatz zum Fat Client keine lokale Datenverarbeitung stattfindet.
Traffic Shaping	Eine Funktion eines Rechnernetzes zur Steuerung des Datenflusses von IP-Paketen nach definierten Kriterien. Diese Funktion ist unidirektional, das heißt sie arbeitet im Gegensatz zur Datenflusskontrolle ohne Steuerinformationen der Gegenseite. Kriterien können z. B. Prioritäten sein oder auch die Variation der Paketverzögerungen.
Transitsystem	Ein Transitsystem ist ein Knoten, der – auch nicht an ihn adressierte – ankommende Pakete auswertet, ggf. bearbeitet und in der Regel weiterleitet. Die Auswertung kann auf unterschiedlichen Schichten erfolgen.
Tunnel-Broker	Ein Tunnel-Broker-Dienst stellt Netzwerk-Tunnel zur Verfügung um Konnektivität zwischen Netzen über eine bestehende (Internet-)Infrastruktur zu ermöglichen, welche ein anderes Netzwerkprotokoll verwendet. Der Tunnel Broker im engeren Sinne handelt mit dem Nutzer bzw. einem Netzknoten des Nutzers die Tunnelendpunkte aus und konfiguriert üblicherweise einen IP-in-IP-Tunnel, der einen Dual-Stack-Netzknoten des Nutzers mit dem Tunnelserver des Dienstanbieters verbindet. Das Konzept ist beschrieben in RFC3053 - IPv6 Tunnel Broker.
Tunneling	Tunneling bezeichnet in einem Netzwerk die Einbettung und Übertragung der PDUs eines Kommunikationsprotokolls in einem (insbesondere anderen) Kommunikationsprotokoll derselben oder einer höheren Protokollschicht. Vor und hinter den Tunnelpartnern wird somit das ursprüngliche Protokoll „gesprochen“, während zwischen den Tunnelpartnern ein anderes Protokoll verwendet wird, das die Daten des ursprünglichen Protokolls transportiert.
Unicast	Unicast ist eine Kommunikationsform, bei der ein Sender mit genau einem Empfänger kommuniziert. Unicast sagt nichts aus über den Richtungsbetrieb, ob unidirektional oder bidirektional, sondern zeigt lediglich an, dass genau zwei Kommunikationspartner direkt oder über ein Netzwerk miteinander kommunizieren. Unicast entspricht einer Punkt-zu-Punkt-Verbindung (P2P). Ein typisches Beispiel für Unicast ist das Telefonieren mit einem anderen Teilnehmer.

Verschlüsselung	Verschlüsselung dient der Geheimhaltung von Daten vor unberechtigten Dritten. Verschlüsselung erfolgt durch deterministisch reversible Kodierung der Daten. Für die Entschlüsselung ist die Kenntnis eines Geheimnisses erforderlich, das nur Berechtigten bekannt sein darf.
Verzeichnisdienst	Ein Verzeichnisdienst ist ein Dienst, der eine Abbildungsfunktion (i) zwischen verschiedenen Darstellungsformen bestimmter Daten (beispielsweise zwischen Rechnernamen und numerischen IP-Adressen) und/oder (ii) zwischen konkreten Diensten und generischen Namen oder Beschreibungen bereitstellt.
Virtual Local Area Network	Virtuelle lokale Netze (Virtual LANs, VLANs) werden zur logischen Strukturierung von Netzen verwendet. Dabei wird innerhalb eines physischen Netzes eine logische Netzstruktur abgebildet, indem funktional zusammengehörende Arbeitsstationen und Server durch Managementeinstellungen zu einem virtuellen Netz verbunden werden.
Virtual Private Network	Ein Netz, das physisch innerhalb eines anderen Netzes (oft dem Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind.
Virtualisierung	Virtualisierung bezeichnet in der Informatik Methoden, die es erlauben, Ressourcen (eines Computers oder Netzwerks) zusammenzufassen oder aufzuteilen. Es gibt viele Konzepte und Technologien im Bereich der Hardware und Software, die diesen Begriff verwenden, u. a. die Server-Virtualisierung oder Virtual Private Networks (siehe Virtual Private Network).
VLAN	(siehe Virtual Local Area Network)

Voice over IP	Voice over IP (VoIP) oder Internet-Telefonie bezeichnet die Nutzung von Sprachdiensten über Computernetzwerke, welche nach Internet-Standards aufgebaut sind. Dabei werden Sprache und Steuerinformationen (z. B. für den Verbindungsaufbau) über ein auch für Datenübertragung nutzbares Netz übertragen. Bei den Gesprächsteilnehmern können sowohl Computer als auch auf IP-Telefonie spezialisierte Telefonendgeräte eingesetzt werden.
VoIP	(siehe Voice over IP)
VPN	(siehe Virtual Private Network)
VPN-Krypto-Gateway	Ein Transitsystem, das die Nachrichten zu bzw. von bestimmten externen Netzen oder Knoten ver- bzw. entschlüsselt.
WebCam	Eine WebCam ist eine Kamera, die einen Web-geeigneten Videostrom oder entsprechende Einzelbilder erzeugt. Diese können je nach Ausstattung mittels eines integrierten oder externen Webservers über das Internet abgerufen werden.
Webclient	Ein Webclient ist eine Instanz, die über das Web angebotene Dienste nutzt. Dazu werden in der Regel standardisierte Protokolle wie HTTP, HTTPS und SOAP benutzt.
Zertifikat	Ein Datensatz, der einem darin genannten Objekt (Rechner, Person, …), bestimmte, im Zertifikat beschriebene, Eigenschaften bestätigt. [Die Identität eines Objektes mit einem im Zertifikat genannten wird üblicherweise durch eine Verschlüsselung und/oder Signatur eines Datensatzes bewiesen, die durch einen im Zertifikat enthaltenen (oder von diesem referenzierten) Schlüssel rückgängig gemacht bzw. verifiziert werden kann.]

9. Anhang: Vorlage für die Erfassung von Software-Abhängigkeiten



10. Anhang: Software in der Öffentlichen Verwaltung

In der ÖV ist aktuell ein breites Portfolio an Softwareprodukten aufgrund langfristig gewachsener Strukturen im Einsatz. Im Folgenden werden die wesentlichen Produkte aufgeführt und in Softwareklassen eingeteilt. Da die Betrachtung der IPv6-Migration für jedes einzelne dieser Produkte zu viel Aufwand bedeutet, ist hier nur deren grundsätzlich Eignung für IPv6 erfasst.

Es wird empfohlen, alle vorhandenen Systeme vor einer Migration auf die aktuellste stabile Version zu aktualisieren.

Nützliche Links:

http://ipv6int.net/systems/index.html
http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems
http://en.wikipedia.org/wiki/Comparison_of_IPv6_application_support
http://www.deepspace6.net/docs/ipv6_status_page_apps.html

Stand der Tabellen: Juni 2013

10.1. Betriebssysteme

Software	Kategorie	IPv6 Unterstützung
MS Windows NT/2000	Betriebssystem	nein
MS Windows XP	Betriebssystem	ab Version SP2
MS Windows Vista	Betriebssystem	ja
MS Windows 7	Betriebssystem	ja
MS Windows 8	Betriebssystem	ja
MS Windows SRV 2003	Betriebssystem	ja
MS Windows SRV 2008	Betriebssystem	ja
MS Windows SRV 2012	Betriebssystem	ja
LINUX Kernel Versionen	Betriebssystem	ab Version 2.6.x, empfohlen ab Version 2.6.20
LINUX Distribution Suse /SLES	Betriebssystem	ab Version 9.1
LINUX Distribution Red Hat / Fedora	Betriebssystem	RedHat: ab Version 4.1 Fedora: ab Version 2
LINUX Distribution DEBIAN	Betriebssystem	ab Version 3.1
LINUX Distribution Ubuntu	Betriebssystem	ab Version 4.10
LINUX Distribution CentOS	Betriebssystem	ab Version 4.1
LINUX Distribution Gentoo	Betriebssystem	ab Version 2004.0
FreeBSD	Betriebssystem	ab Version 4.0
HP-UX	Betriebssystem	ab Version 11i v2
IBM-AIX	Betriebssystem	ab Version 4.3
Z-OS	Betriebssystem	ab Version V1R4.0
Siemens BS2000/OSD	Betriebssystem	ab Version 2002
Mac OS X	Betriebssystem	ab Version 10.6
Solaris	Betriebssystem	ab Version 8
SUN-OS	Betriebssystem	ab Version 8
OpenBSD	Betriebssystem	ab Version 2.7
NetBSD	Betriebssystem	ab Version 1.5

IPv6-Matrix für ältere Windows-Systeme:
https://wikispaces.psu.edu/display/ipv6/Windows+IPv6+support+matrix

10.2. Webdienste, -server und Proxies

Software	Kategorie	IPv6-Unterstützung
Java auf Client Site	Framework	ab Version 1.4.2
Java Servlets auf Serverseite	Framework	ab Version 1.5
.Net	Framework	ab Version 1.1
MS-IIS	Webserver	ab Version 6.0
Apache	Webserver	ab Version 2.0.14
Nginx	Webserver / Proxy	ab Version 0.7.36
Lighttpd	Webserver / Proxy	ja, (ab Version 1.4.27)
Squid	Proxyserver	ab Version 3.1
Privoxy	Proxyserver	ab Version 3.0.16

10.3. Middleware, Applikationsserver

Software	Kategorie	IPv6-Unterstützung
Oracle Application Server	Applikationsserver	s. DB
Oracle Application Server 2 (ex BEA)	Applikationsserver	s. DB
Tomcat	Applikationsserver	ab Version 5.5
JBOSS	Applikationsserver	ab Version 6.0
Glassfish	Applikationsserver	ab Version 2.1.1
IBM Websphere	Applikationsserver	ab Version 6.0
SAP Netweaver	Applikationsserver	ab Version 7.0 Enhancement Package 2
SAP ERP	Applikationsserver	AS ABAP mit SAP ab Kernel 7.10, Patchlevel 150

Ein guter Vergleich von Webservern findet sich unter:
http://socialcompare.com/en/comparison/comparison-of-web-servers

10.4. DNS / Directory Dienste / LDAP / X.500 DAP

Software	Kategorie	IPv6-Unterstützung
MS - ADS inkl. Clustering	Verzeichnisdienst	ab Version 2008
Novell - NDS	Verzeichnisdienst	ab Version 6.5
LINUX - Samba	SMB-Server und -Klient	ab Version 3.2
BIND	DNS-Server	ab Version 9.3.2
OpenLDAP	Verzeichnisdienst	ab Version 2.0.0
DIRX	Verzeichnisdienst	ab Version V8.1

10.5. Groupware

Software	Kategorie	IPv6-Unterstützung
MS-Exchange	Groupware	ab Version 2007 SP1 (mit WS2008)
MS-Lotus Notes	Groupware	ab Version 7.0
Novell Groupwise	Groupware	ab Version 7
OSS-Lösungen (OpenXChange, Zarafa)	Groupware	Zarafa: imap, pop IPv4 only
Biztalk	Groupware	ab Version 2010
MS Sharepoint	Groupware	ab Version 2007

10.6. E-Mail

Software	Kategorie	IPv6 Unterstützung
Postfix	Mailserver	ab Version 2.2.0
Courier Mail Server	Mailserver	ab Version 0.42.2
CyrusImap	Mailserver	ab Version 2.2.3
exim	Mailserver	ab Version 4.20
QMail	Mailserver	ab Version 1.03
SendMail	Mailserver	ab Version 8.12.9
Dovecot	Mailserver	ab Version 2.1.1
ZMailer	Mailserver	ab Version 2.99.55
Outlook 2007	Mailclient	ja
Thunderbird	Mailclient	ab Version 1.5
Entourage	Mailclient	nein
Evolution	Mailclient	ab Version 1.4.5

10.7. Datenbanken

Software	Kategorie	IPv6-Unterstützung
MS Access	Datenbankserver	ab Version 2003
MS SQL	Datenbankserver	ab Version 2005
MySQL	Datenbankserver	ab Version 5.5
Oracle	Datenbankserver	ab Version 11g, Release 1
PostgresSQL	Datenbankserver	ab Version 9.0
IBM-DB2	Datenbankserver	ab Version 10
Berkeley DB	Datenbankserver	ab Version 4.5
DB Connectoren / ODBC / JDBC	Datenbankadapter	abhängig von der verwendeten Datenbank, Treiber werden in der Regel mit der Datenbank ausgeliefert.

10.8. Terminal-Systeme / VM / Application-Streaming

Software	Kategorie	IPv6 Unterstützung
Windows Terminalserver	Client- / Server-Implementierung	ab Vista und Server 2008
Linux Terminalserver	Client- / Server-Implementierung	(ja)
VNC	Client- / Server-Implementierung	ab Version 4.1.2 (Pers), 4.1.7 (Enterprise)
NX Free Edition	Client- / Server-implementierung	Version 3.5.0,
Citrix XEN	Client-Server-Implementierung	nein
Citrix XEN Desktop	Client-Implementierung	nein
VMware GSX/Server	Client-Server-Implementierung	ab Version 3.5
VMware VDI	Server-Implementierung	(vSphere: ab Version 4.0)
V-Box (Grundlage für SINA VW)	Server-Implementierung	(basiert auf VirtualBox)
VirtualBox	Client-Implementierung	ja
MS Virtual PC	Client-Implementierung	ja, Virtual PC 2004
MS Hyper-V + 2008R2	Server-Implementierung	ja
VMware Workstation	Client-Implementierung	ja, ab Version 7
ThinApp (VMware)	Server-Implementierung	ab 2010 NIST Host Compliance
XENApp (Citrix)	Client-Server-Implementierung	ab Version 5
Parallels Desktop	Client-Implementierung	ab Version 6

10.9. System Management und Monitoring

Bei Management- und Monitoring-Systemen muss zwischen der Kommunikationsschnittstelle des Systems (z. B. Abfragen von Werten über IPv4 oder IPv6) sowie den Informationselementen selbst (z. B. Zähler für IPv6-Pakete) unterschieden werden. Beide Eigenschaften können in der Praxis normalerweise unabhängig voneinander genutzt werden (bspw. Abfrage von IPv6-Paketzählern über eine IPv4-Management-Schnittstelle).

Software	Kategorie	IPv6-Unterstützung
Nagios	Client-Server-Implementierung	ab Version 3.2.3 (Patch)
MOM	Server-Implementierung	http://support.microsoft.com/kb/972052/de
HP-Open View	Server-Implementierung	ja
IBM-Tivoli	Server-Implementierung	ja
BMC ProactiveNet (ehemals Patrol)	Server-Implementierung	Unterstützung geplant
Munin	Server-Implementierung	ja, ab Version 1.4 http://munin-monitoring.org/wiki/IPv6
OpenITCockpit	Server-Implementierung	basiert auf NAGIOS

10.10. Softwareverteilung

Software	Kategorie	IPv6 Unterstützung
MS WSUS	Server-Implementierung	3.0 SP2
Opsi	Server-Implementierung	abhängig vom Server: Betriebssystem, DNS und ggf. Software-Bibliotheken
DSM 7.0 (ehem. ENTEO)	Client-Server-implementierung	ja
CASPER	Server-Implementierung	nein

10.11. Router-Betriebssysteme

Software	Kategorie	IPv6 Unterstützung
Cisco iOS	Embedded System	ab 12.2T
OpenWRT	Embedded System	ja (opkg install ipv6-support)
DDWRT	Embedded System	ja
Juniper	Embedded System	ja
F5	Embedded System	ja

10.12. Mobile Plattformen

Software	Kategorie	IPv6 Unterstützung
Android	Betriebssystem	ab Version 2.2 (nur WLAN)
Apple iOS	Betriebssystem	ab Version 4
Windows Mobile / CE / 7	Betriebssystem	ja (6.5) Nein (7)
RIM - Blackberry	Betriebssystem	IPv6 im WLAN unterstützt durch Playbook Tablet 2.0 und Z10 Smartphone, keine IPv6-Unterstützung für Blackberry Enterprise Server
Web OS	Betriebssystem	ab Version 2.1.0

11. Abbildungsverzeichnis

12. Tabellenverzeichnis