Bundesverwaltungsamt
– Bundesstelle für
Informationstechnik –

BIT

# IPv6

## Migrationsleitfaden
## 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 Sicherheit in der Informationstechnik
E-Mail: ipv6@bsi.bund.de


## Autoren


| | |
|---|---|
| **Carsten Schmoll** | Fraunhofer FOKUS |
| **Thomas Günther** | Fraunhofer FOKUS |
| **Tahar Schaa** | Cassini Consulting GmbH |
| **Jens Tiemann** | Fraunhofer FOKUS |
| **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 werden und nur über diese erreichbar sind. Schon heute ist bei den aktuellsten Betriebssystemversionen IPv6 nicht mehr ohne Einschränkungen deaktivierbar. 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 werden durch Profile für verschiedene Geräteklassen 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 und vereinfachen die Überprüfung der Vorgaben. Die Profile können darüber hinaus auch dafür eingesetzt werden, bestehende Infrastrukturelemente für ihren Einsatz in IPv6-Umgebungen zu überprüfen.

Mit diesem Migrationsleitfaden liegt ein Dokument vor, das die schrittweise Einführung von IPv6 beschreibt. Es wird hierin 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

## 2.1. Ausgangssituation

Für Netzinfrastrukturen und Dienste wird die Migration auf das Internet Protocol Version 6 (IPv6) in den nächsten Jahren zwingend. Zur Einführung von IPv6 und zum Betrieb liegen europaweit im Bereich der ÖV bisher kaum praktische Erfahrungen vor, so dass mit der Einführung von IPv6 weitgehend Neuland betreten wird. Insbesondere in der öffentlichen Verwaltung (ÖV) werden Hard- und Softwarekomponenten eingesetzt, deren Kompatibilität mit dem Protokoll IPv6 nicht vollständig geklärt ist. Noch weniger vorhersagbar ist bisher das Verhalten von IPv6 auf die in Bund und Ländern definierten IT-Standardarchitekturen.

Zur Umstellung müssen zahlreiche Netzbereiche um die Unterstützung von IPv6 erweitert werden. Dies betrifft Netze der ÖV, Koppelnetze und Providernetze bis hin zu den Bürgern zu Hause (siehe folgendes Bild).

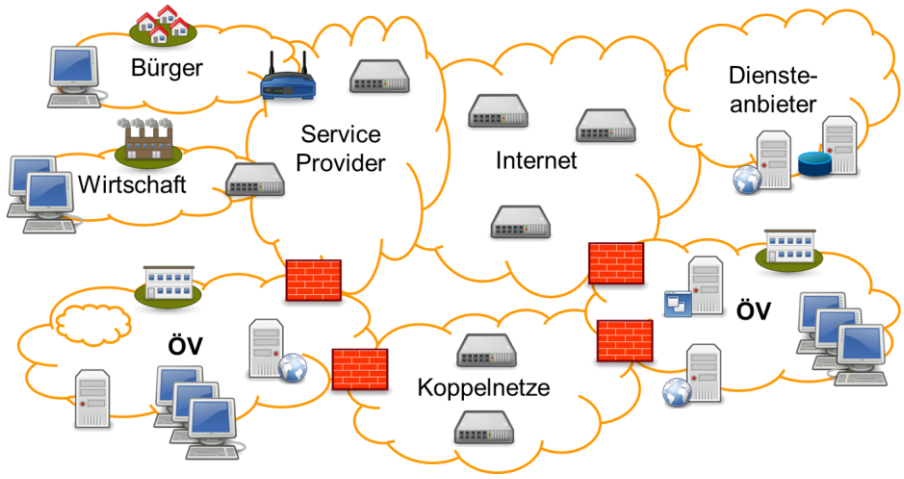


*Abbildung 1: Netzinfrastrukturen und Akteure*

Die Umstellung (Migration) zu IPv6 stellt eine große Herausforderung dar, da IPv6 auf dem Gerätemarkt in verschiedenen Reifegraden verfügbar ist. Zudem muss für die Gewährleistung einer sicheren Nutzung von IPv6 in die Schulung der Mitarbeiter erheblich investiert werden.

In dem Forschungsprojekt „IPv6 Profile und Migration in der Verwaltung“ wurden durch das Fraunhofer-Institut FOKUS der zukünftige Einsatz von IPv6 in der öffentlichen Verwaltung untersucht. Dabei wurde IPv6 sowohl theoretisch betrachtet, als auch praktische Migrationsexperimente durchgeführt. Im Ergebnis wurden diese dokumentiert sowie Empfehlungen abgeleitet, um die mit der IPv6-

Einführung verbundenen Chancen zu nutzen und Risiken für die öffentliche Verwaltung zu minimieren. Im Rahmen dieses Projektes wurde dieser Migrationsleitfaden erstellt und IPv6-Profile für die öffentliche Verwaltung erstellt ([IPv6_PROFILE] und [IPv6_PROFILE-DOK]).

## 2.2. Zweck des Leitfadens

Dieser Migrationsleitfaden soll in erster Linie die Aufstellung eines Migrationskonzepts und den Start eines Migrationsprojekts unterstützen, abgestimmt auf die Anforderungen der jeweiligen Organisation. Als Rahmenbedingungen für die Migration wurden in erster Linie die Gegebenheiten der öffentlichen Verwaltung angenommen. Die dokumentierten Empfehlungen können aber auch für andere IT-Infrastrukturen angewendet werden.

In diesem Migrationsleitfaden steht das praktische Vorgehen bei der Migration im Vordergrund, während das Profildokument [IPv6_PROFIL-DOK] eher abstrakt die Anforderungen an Netz- und IT-Komponenten beschreibt (z. B. zur Unterstützung bei der Beschaffung von neuen Systemen). Querverweise aus dem Migrations-dokument auf das Profildokument erlauben das Vertiefen von einzelnen Aspekten der Anforderungen an IPv6-fähige Komponenten und das Nachschlagen von relevanten Standards. Unterstützt wird von beiden Dokumenten eine möglichst ganzheitliche Sicht auf die Infrastruktur. Dies umfasst sowohl Netzkomponenten als auch Anwendungen.

Dieser Migrationsleitfaden soll bei der Vorbereitung und Durchführung der Migration helfen. Er bietet hierfür „Kochrezepte“ an, u. a. durch die Auflistung der einzelnen Schritte in Checklisten. Diese sind in diesem Dokument in Anhang I – IPv6-Migrations-Checklisten zu finden. Begleitend bieten die Empfehlungen aus Anhang II – IPv6-Migrationsleitlinie wichtige Tipps für die Migration.

Im Einzelfall können Abweichungen vom vorgeschlagenen Vorgehen in den Checklisten und Empfehlungen auf Grund der konkreten Anforderungen sinnvoll sein. Folglich entbindet dieser Leitfaden die IT-Verantwortlichen *nicht* davon, ihre eigenen Anforderungen und Gegebenheiten zu analysieren. Er soll aber eine möglichst realitätsnahe Orientierung zur Migration von IPv4-only zu IPv4/IPv6-Dual-Stack bieten. Für das Fernziel „IPv6-only“ soll zudem der Weg bereitet werden.

## 2.3. Aufbau des Leitfadens

In Kapitel 3 werden die äußeren Rahmenbedingungen beschrieben, welche auch für Behörden eine Migration zu IPv6 bedingen.

In Kapitel 4 werden zunächst aktuelle IPv4-Netzarchitekturen vorgestellt, die typisch für die öffentliche Verwaltung sind. Diese sind angelehnt an reale Netzarchitekturen aus Bund, Ländern und Kommunen. Exemplarisch dargestellt sind die Architekturen „kleinere Verwaltung“ und „größere Verwaltung“. In beiden Strukturen lassen sich die typischen Konfigurationen einer ÖV finden. Im Anschluss werden diese typischen IPv4-Architekturen exemplarisch migriert.

Das Ziel ist nicht nur, die alten IPv4-Architekturen 1:1 in die IPv4/IPv6-Dual-Stack-Welt zu überführen, sondern die besseren IPv6-Protokolleigenschaften auch nutzen zu können.

Im Kapitel 5 „IPv6-Migration“ geht es, ausgehend von der Motivation für eine Migration und möglichen Szenarien der Beteiligten, um die generelle Reihenfolge der Migration und die Schulung von Mitarbeitern.

Vor der eigentlichen Durchführung der Migration steht die Beschäftigung mit dem Adresskonzept und der Netzarchitektur. Im Kapitel 6 „Adresskonzepte und Netzarchitekturen“ werden diese Konzepte vorgestellt und dazu auch Fragen der Sicherheit erläutert.

Übergangstechniken werden in Kapitel 7 vorgestellt. Diese Verfahren sind in die Gruppen Dual-Stack-Techniken, Tunneltechniken und Verfahren zur Protokollumsetzung zwischen IPv4- und IPv6-Netzwerken eingeteilt. Das Kapitel schließt ab mit Empfehlungen zum Einsatz der Techniken ab. Dabei wird auch auf typische Probleme bei der Migration oder dem Dual-Stack-Betrieb eingegangen, sowie kurz der Betrieb in einer reinen IPv6-Umgebung dargestellt.

Kapitel 8 zeigt die mit IPv6 verbundenen Sicherheitsaspekte auf, welche bei der Migration und beim späteren Betrieb beachtet werden müssen, um eine Netzwerksicherheit mindestens auf dem vorhandenen Niveau zu gewährleisten.

Der praktische Schwerpunkt des Dokuments folgt mit der Vorstellung von exemplarischen Migrationsschritten für einzelne IT-Komponenten in Kapitel 9. Ausgehend von den unteren Schichten zu den höheren Schichten des Kommunikationsmodells wird anhand von typischen Komponenten und Funktionsgruppen eine mögliche Vorgehensweise beschrieben.

Kapitel 10 beschreibt die Durchführung und Resultate der Umsetzung mehrerer praktischer Migrationsexperimente. Dafür ausgewählt wurden eine zum einen eine typische Webserverinstallation incl. Proxies und IP-Routern. Zum anderen wurde eine ausgewählte kommunale Anwendung migriert.

Die Kapitel 11 und 12 schließen dieses Dokument mit einem Ausblick auf die mögliche weitere Entwicklung und Nutzung von IPv6 ab. Dabei wird auf neue technische Aspekte von IPv6 und auf bereits vorhandene, bekannte Herausforderungen für den reibungsfreien Betrieb mit IPv6 ein Blick geworfen.

Anschließend finden sich in Anhang I (ab Seite 150) IPv6-Migratsions-Checklisten welche die konkrete, praktische Migration unterstützen, sowie das Literatur-verzeichnis und ein Glossar der in diesem Dokument verwendeten Begriffe. Begleitend zu einer Migration bietet Anhang II wichtige Tipps zur Reihenfolge der Arbeiten und zu wichtigen technischen Entscheidungen in Bezug auf IPv6 in Form einer IPv6-Leitlinie für den praktischen Einsatz.

Zum Einstieg in die Migration wird zunächst die Notwendigkeit der Einführung von IPv6 motiviert. Zudem werden die grundsätzlichen Schritte der Migration aufgelistet.

# 3. Motivation für IPv6 in der öffentlichen Verwaltung

Anfang Februar 2011 wurden die letzten freien IP-Adressblöcke von der IANA an die fünf international tätigen Regional Internet Registries (RIR) verteilt. Im September 2012 hat die auch für Europa zuständige RIPE begonnen ihren letzten IPv4 Adressbereich der Größe /8 nach besonderen Regeln zu vergeben. Somit ist endgültig klar, dass IPv6 eingeführt werden muss.

Der Aufbau von IPv4-basierten Diensten ist zwar noch einige Zeit durch Übergangstechniken wie IPv4-NAT und den Aufkauf frei werdender IPv4-Adressbereiche möglich, dies ist aber mit steigenden Kosten und einer sich verschlechternden Qualität der Nutzerfahrung verbunden.

Geht man diesen Weg, so wählt man hohe Kosten für eine veraltete Netztechnologie mit beschränktem Funktionsumfang. Zudem erhöhen diese Übergangstechniken die Komplexität der Netze zu Lasten der Leistungsfähigkeit und der Sicherheit.

Gleich mehrere Faktoren bedingen mittelfristig die Migration auf IPv6 (mindestens in der Form IPv4/IPv6-Dual-Stack, z. T. auch zu IPv6-only):

- LTE – Mobilfunknetze der dritten Generation (3G) kämpfen bereits heute aufgrund der großen Nutzerzahlen mit der IPv4-Adressknappheit, und teure IPv4-Adresssparmaßnahmen[1] werden installiert. Für Netze der vierten Generation (4G = Long Term Evolution (LTE)) ist daher IPv6 verpflichtend vorgeschrieben.
- Adressknappheit – Auch Internet Service Provider (ISPs) für Festnetzanschlüsse sehen einem Ende ihrer zugeteilten IPv4-Adressen entgegen. Dies betrifft vor allem kleinere, jüngere ISPs und Kabelnetzbetreiber.
- Zwangsmigration – Bürger in Deutschland werden daher in Zukunft z. T. Internetanschlüsse erhalten, welche nur über IPv6 die volle Funktionalität und Dienstqualität wie bisher erreichen.
- IPv6-only im Ausland – Bürger (und Politiker) auf Reisen im Ausland bekommen u. U. bei der Nutzung des (mobilen) Internets vor Ort nur einen IPv6-only-Netzzugang. Damit sind IPv4-only-Dienste i. allg. für sie unerreichbar.
- Renummerierungsaufwände – In der öffentlichen Verwaltung gibt es aufgrund politischer und organisatorischer Veränderungen immer wieder Verwaltungsfusionen. Diese verurachen bei IPv4 enorme Aufwände für eine Renummerierung der IT-Systeme, die mit IPv6 deutlich reduziert werden können.
- Technologiewandel zu IP – In der Automatisierungstechnik gibt es einen Trend zur Nutzung des Internet Protokolls (IP). Auch hier spricht die Vielzahl der eingesetzten Systeme dringend für eine IPv6-Nutzung.

[1] z. B. Carrier-Grade NAT (CGN), siehe dazu Abschnitt 7.4.1

- Logische Ende-zu-Ende Erreichbarkeit – Für die zuverlässige Funktion vieler Server- und Webanwendungen ist eine öffentliche, im Internet eindeutige IP-Adresse notwendig. Diese kann mit IPv4 in Zukunft nicht immer gewährleistet werden.

Neben der zentralen Adressknappheit sprechen weitere technische Gründe für die Migration zu IPv6:

- Das Protokolldesign von IPv6 ist einfacher als bei IPv4, was insbesondere das Weiterleiten von IPv6-Paketen gegenüber IPv4 vereinfacht.
- Durch die Menge der Adressen kann weltweit das Ende-zu-Ende-Prinzip wiederhergestellt werden.
- Das Protokolldesign trägt den neueren Anforderungen an Sicherheit, Erweiterbarkeit und Autokonfiguration Rechnung.
- Das Zusammenwachsen der Europäischen Union und die Globalisierung werden zukünftig eine deutlich intensivere internationale, IP-basierte, Sprach- und Datenkommunikation zwingend erfordern.

Eine Übersicht über diese technischen Neuerungen von IPv6 findet sich im Profildokument [IPV6_PROFILE].

Auf Grund dieser Fakten entsteht der Migrationsdruck zu IPv6. Dieser unterscheidet sich, je nach Nutzergruppe, in Stärke und Konsequenzen für die Migrationsstrategien.

Für die Migration zu IPv6 lassen sich Nutzergruppen entsprechend ihrer Rollen einteilen:

- Carrier/Internet Service Provider (ISP)
- Anbieter von Inhalten und Diensten
- Internetnutzer

In der Praxis finden sich natürlich auch Mischformen, z. B. sind Anbieter von Inhalten im Internet selbst auch immer konsumierende Nutzer des Internets. Rechenzentren wiederum bieten ihren Kunden Internetkonnektivität, hosten aber auch Dienste und werden damit selbst zum (technischen) Anbieter von Inhalten.

Entsprechend der Reihenfolge der obigen Aufstellung, staffelt sich die Notwendigkeit die Migration zu anzugehen. Ein Provider muss mit der Migration beginnen oder schon begonnen haben, um die Investitionen in seine umfangreiche Hardwarebasis und sein Geschäftsmodell zu schützen. Eher konsumierende Internetnutzer werden dagegen abwarten und davon ausgehen können, am Markt immer eine Lösung für den Zugriff auf das Internet angeboten

zu bekommen. Sie müssen aber zum Zeitpunkt des Umstiegs die IPv6-Tauglichkeit ihrer IT-Komponenten sicherstellen.

Da die Migration alle Stakeholder in der Nutzungskette von Diensten im Internet betrifft, benötigt diese einen ausreichenden Zeitraum und muss folglich von allen Beteiligten frühzeitig angegangen werden. Dies gilt insbesondere für die öffentliche Verwaltung.

# 4. IT-Infrastrukturen in der öffentlichen Verwaltung

Die Migration zu IPv6 sollte mit der Betrachtung der vorhandenen IT-Strukturen der Behörde oder Organisation gestartet werden. Behörden sollten sich dabei mit ihren konkreten IT-Infrastrukturen in den hier exemplarisch dargestellten wieder finden.

In diesem Kapitel werden daher verschiedene IT-Infrastrukturen betrachtet, welche bei öffentlichen Verwaltungen in Deutschland zu erwarten sind. Die Infrastrukturen sind exemplarisch beschrieben, um von diesen konkrete Migrationsschritte und –Abfolgen abzuleiten.

Es wird davon ausgegangen, dass sich die überwiegende Mehrzahl der aktuell existierenden Netzwerkstrukturen bei öffentlichen Verwaltungen auf einen dieser fünf Fälle abbilden lässt:

| | Einzelplatz Mobil | SoHo ÖV | mittlere ÖV | große ÖV | Kommunales oder Landes Rechenzentrum |
|---|---|---|---|---|---|
| **organisatorische Beispiele** | MA-Ordnungsamt im Außeneinsatz, mobiles Bürgeramt (Koffer) | Schule mit Sekretariat, Beratungsstelle der Polizei | Meldestelle, Ausländerbehörde, Bürgerbüro einer Stadt | Amt mit mehr als 200 Rechnerarbeitsplätzen | |
| **Anz. Rechner-arbeitsplätze** | 1 | bis zu 4 User | 5-200 User | >200 | |
| **Netzanbindung mit Bandbreite** | GPRS/UMTS/ LTE | DSL | symmetrische Anbindung > 2MBit/s | MPLS-Anbindung > 10 MBit/s | redundante Anbindung, >34 MBit/s (min), 1 GBit/s (opt.) |
| **Netztopologie** | VPN | i. d. R. Stichleitungs-anbindung | i. d. R. Stichleitungs-anbindung | i. d. R. angebunden an vollvermaschte Netze | Sternmittelpunkt oder Teil eines vollvermaschten Netzes |
| **Qualität des IT-Supportes** | i. d. R. ohne direkte IT-Betreuung/ keine Vollzeitbetreuung | i. d. R. ohne direkte IT-Betreuung/ keine Vollzeitbetreuung | mit IT-Betreuung aber evtl. zentral | i. d. R. eigene IT-Betreuung | eigene Betriebsmannschaft, evtl. IT-Support als Dienstleistungsangebot |
| **Infrastruktur-komponenten** | **-** | | **interne Server; kaum extern angebotene IT-Dienste** | **lokale interne Server; extern angebotene IT-Dienste** | **Server für kommunales und/ oder landesübergreifendes Dienste-Angebot** |

*Tabelle 1: Klassen von öffentlicher Verwaltung*

Im Folgenden werden diese fünf Fälle weiter detailliert.

### 3.1. Infrastruktur „Mobiler Arbeitsplatz“

Typische Merkmale:

- Im allgemeinen wird der Internetzugang Dritter genutzt
- Mobilfunk (3G, LTE), öffentlicher WiFi-Hotspot oder privater Internetzugang
- Vom Arbeitgeber gestelltes Smartphone/Laptop mit Netzzugang
- Bei großen Behörden z. T. auch direkter Netzzugang zum Verwaltungsnetz

### 3.2. Infrastruktur „SoHo“

Typische Merkmale:

- feste Installation incl. dediziertem Gateway-Router
- Internetzugang über lokal verfügbaren ISP, z. B. über privaten DSL-Internetzugang
- Zugang zu „seiner“ ÖV via sicherem Tunnel vom Arbeitsplatzrechner aus (empfohlen: VPN mit IPv4 und IPv6 getunnelt)

### 3.3. Infrastruktur „Mittlere Verwaltung“

Typische Merkmale:

- Permanente Infrastruktur incl. ÖV-Gateway-Router
- Mehrere Arbeitsplätze an einem Standort
- DMZ ist optional: öffentlicher Webserver kann vorhanden sein
- Mehrere interne Server (Dateiserver, DNS, DHCP, „kleinere“ Fachverfahren)
- Zumeist kein technischer IT-Verantwortlicher vor Ort

### 3.4. Infrastruktur „Große Verwaltung“

Typische Merkmale:

- Wie mittlere ÖV, aber mehrere Server/Dienste sind extern sichtbar/zugreifbar

- Große Anzahl von Arbeitsplätzen
- Server/Services sind oft komplexere Dienste (Fachverfahren), die auch für angrenzende Verwaltungsbereiche angeboten werden
- Komplexere Serverarchitekturen in der DMZ als bei mittlerer ÖV, z. B. mit dedizierten Datenbank- und Applikationsservern
- Technischer IT-Verantwortlicher vor Ort

### 3.5. Infrastruktur „Rechenzentrum“

Typische Merkmale:

- Oft mit Virtualisierungsumgebungen / Blade-Systemen (z. T. mandantenfähig)
- In der Regel weniger Arbeitsplätze/Klienten als mittlere Verwaltung
- Betreibt auch Server/Services für andere öffentliche Verwaltungen
- Kann Tunnelendpunkte (Tunnelserver) und IPv6-Tunnelbroker anbieten
- Technisches IT-Team vor Ort
- IT-System-Management (Monitoring, Alarmierung) vorhanden

### 3.6. IPv6-Migrationsreferenzarchitektur

Die oben aufgeführten typischen IT-Infrastrukturen und ihre Architektur in der öffentlichen Verwaltung haben sich im Laufe der Zeit weiter entwickelt. Diese Entwicklung wurde getrieben durch den Wandel der Anforderungen, neue Sicherheitsmechanismen und die Weiterentwicklung genutzter Software- und Hardwarekomponenten.

Es ist das Ziel der Einführung von IPv6 in der ÖV, für Netze und Dienste ein einheitliches und strukturiertes Adressschema zu etablieren und grundsätzlich eine Ressort-übergreifende Kommunikation mit eindeutiger Adressierung zu ermöglichen. Nur so kann die Kommunikationsinfrastruktur der ÖV in Deutschland für die zukünftigen Anforderungen vorbereitet werden, welche eine engere und direktere Kommunikation zwischen den Behörden erfordern können.

Hier wird beispielhaft die Nutzung einer Fachanwendung und ihr logischer Kommunikationsweg vom Endsystem zum Server als Ausgangspunkt betrachtet. Die problemlose, transparente Nutzung des gesamten Kommunikationspfades mit IPv6 soll dabei sichergestellt werden. Dazu müssen sowohl die einzelnen Verwaltungen, als auch die Koppelnetze und die Übergänge zwischen diesen Netzen durchgängig mit IPv6 funktionieren.

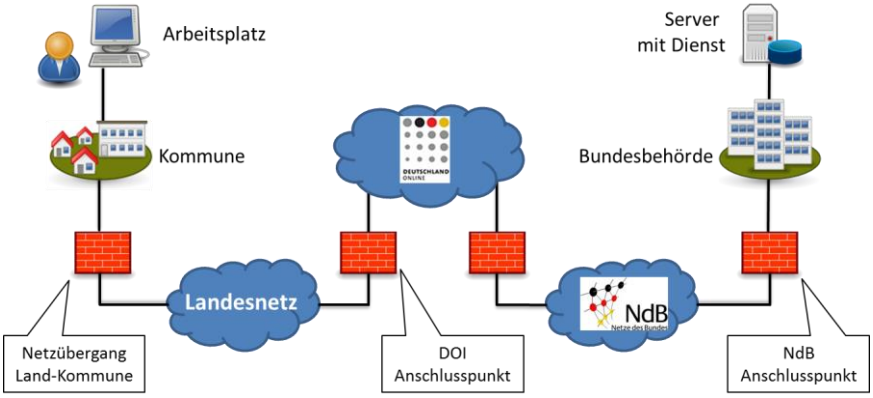


*Abbildung 2: Kommunikation in der ÖV*

Die gewachsenen Infrastrukturen der einzelnen Einrichtungen werden zwangsläufig mit der Einführung von IPv6 konfrontiert. Da diese mit neuen Funktionen und Möglichkeiten einen tiefgehenden Eingriff in die Architektur der Infrastruktur darstellt, sollte die Umstellung zu einer grundlegenden Prüfung der Netzkonzeption genutzt werden.

In dieser IPv6-Migrationsmusterarchitektur wird von einer gewachsenen IPv4-only IT-Infrastruktur ausgegangen. Letztere dient als Ausgangpunkt für die beispielhafte Migration zu einer IPv4/IPv6-Dual-Stack-Infrastruktur, mit dem Ziel, alte, aus IPv4 resultierende Einschränkungen abzulösen. IPv6 verbessert durch den größeren Adressraum und den Wegfall von Network Address Translation (NAT) die technischen Grundlagen der Behördenkommunikation.

Ferner bietet IPv6 auch technische Möglichkeiten, die das IPv4-Protokoll so nicht unterstützt, wie z. B. direkten Support für Multihoming und verbesserte mobile Datenübertragung durch Mobile IPv6.

Die Ausgangssituation ist in der folgenden Abbildung dargestellt: Zwei Einrichtungen (ÖV1 und ÖV2) sind über verschiedene Koppelnetze miteinander verbunden, z. B. Landesnetze oder auch das Internet. Innerhalb einer ÖV finden sich zudem verschiedene Teilnetze zur Strukturierung des Netzes, die verschiedenen Sicherheitszonen zugeordnet sind. Den Koppelnetzen zugewandt ist die DMZ mit dem Sicherheits-Gateway. Dahinter befinden sich die Arbeitsplatznetze, interne Server und Backend-Server für die angebotenen Dienste.

In dieser Übersichtsdarstellung wird exemplarisch davon ausgegangen, dass jede ÖV ein Fachverfahren anbietet (FA1, FA2), das von der jeweils anderen ÖV und ihr selbst genutzt wird.

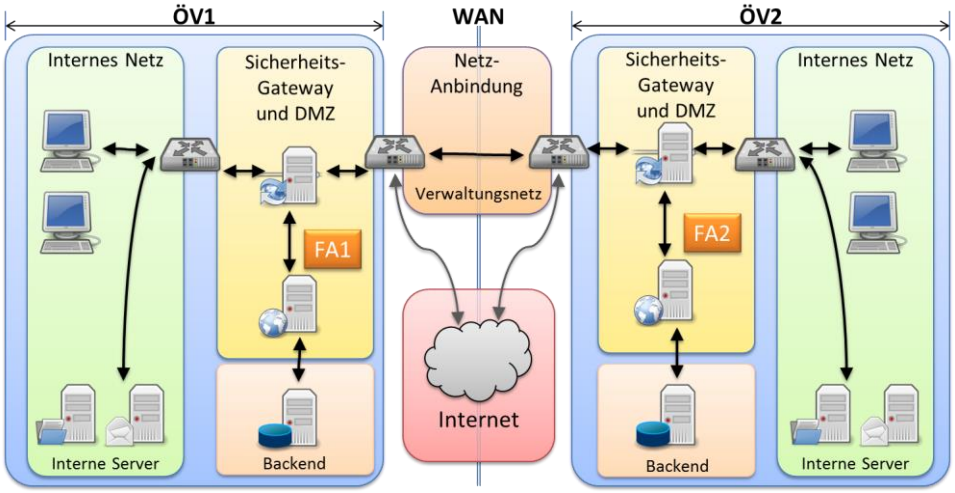


*Abbildung 3: ÖV-Netzarchitektur*

Bei der Betrachtung einer Migration spielen weitere Komponenten eine Rolle, wie z. B. die Firewalls oder ein Reverse-Proxy zur technischen Realisierung eines Dienstes. Um die Darstellung nicht zu komplex werden zu lassen, wird im Folgenden nur die exemplarische Nutzung eines Fachverfahrens (FA) dargestellt – eine ÖV ist dann nur Anbieter und die andere nur Nutzer des FA. Daraus ergibt sich die Darstellung der folgenden Referenzarchitektur für die öffentliche Verwaltung, welche die Grundlage für diesen Migrationsleitfaden bildet.

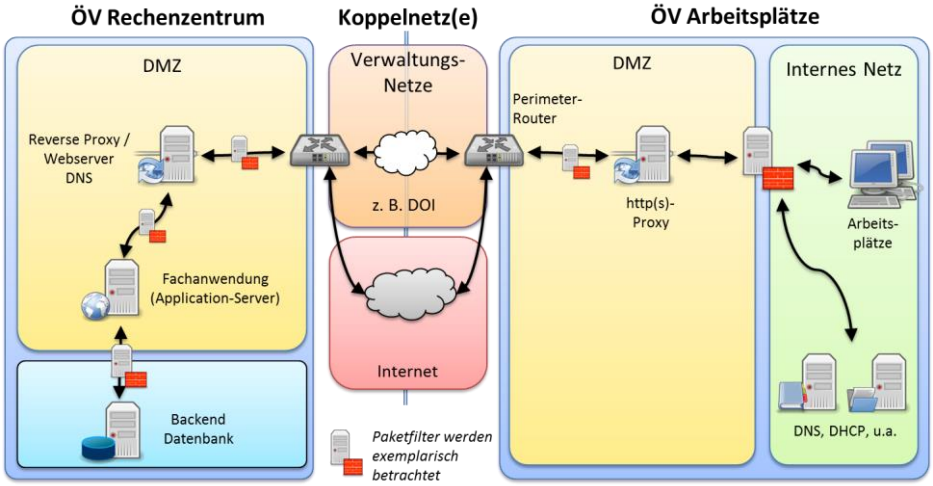


*Abbildung 4: ÖV-Migrationsreferenzarchitektur*

Auf der linken Seite ist die technische Realisierung der FA dargestellt. Die rechte Seite stellt beispielhaft die verschiedenen Möglichkeiten zur Anbindung von Arbeitsplätzen in der ÖV dar. Die logischen Komponenten einer typischen Konfiguration sind:

- Arbeitsplätze
- Interne Server in einem separaten Netzbereich
- PAP-Struktur (Paketfilter – Application Level Gateway – Paketfilter) zur Anbindung

Auf der linken Seite ist die FA auf einem Applikationsserver installiert. Auf diesen kann nur über ein Reverse-Proxy oder einen Webserver zugegriffen werden. Die Anwendungsdaten liegen davon getrennt auf einem Datenbank-Backend, welches wiederum von dem Applikationsserver über einen Paketfilter getrennt ist.

Ausgehend von der IPv4-only Infrastruktur sind abgestufte Teilmigrationen möglich. Diese orientieren sich an den vorhandenen Teilnetzen. In Kapitel 5 wird beschrieben, wie solche Teilmigrationen vorbereitet werden sollten.

Die Migration zu IPv6-only Netzen ist das langfristige Ziel. Dies ist zurzeit jedoch nur sinnvoll für Teilnetze mit dedizierten neuen Anwendungen, wie z. B. Voice-over-IP (VoIP) Telefonie. Einen Ausblick darauf gibt Abschnitt 7.6 in diesem Dokument.

# 5. IPv6-Migration

Die Migration einer vorhandenen Infrastruktur zu IPv4/IPv6-Dual-Stack stellt in jedem Fall ein eigenes Projekt dar. Dieses benötigt neben dem Regelbetrieb eigenständige Ressourcen (Personal, Budget, Planung). Zudem muss die eigentliche Durchführung der Migration neben dem Tagesgeschäft in laufenden Betrieb eingepasst werden.

Das Migrationsprojekt muss sorgfältig geplant werden. Für den Betrieb und die Migration von komplexen Systemen, wie z. B. Kommunikationsnetzwerken und Rechenzentren, gelten die allgemein bekannten „Weisheiten“ und Prinzipien:

- „Planung ist das halbe Leben.”
- Eine gute Dokumentation ist die andere Hälfte.
- Ein komplett neues System baut man am besten ohne Altlasten auf (z. B. IPv6-only-Telefonie).
- Notwendige Umbauten nutzt man effektiv, indem dabei gewachsene Strukturen aufgeräumt werden (Konsolidierung).
- Ein schrittweises Vorgehen („chicken little“-Strategie) ermöglicht ein kontrolliertes Zurückgehen („rollback“) im Fehlerfall und ausführliche, systematische Tests.
- Migration „von außen nach innen“ (bzgl. Topologie der Netze)
- Migration „von unten nach oben“ (bzgl. OSI-Kommunikationsmodell)

Aus diesen Prinzipien lassen sich zwei sinnvolle Vorgehensweisen für die Migration von IPv4-only- zu Dual-Stack-Umgebungen ableiten, die ab Abschnitt 5.1.1 dargestellt werden. In der Praxis werden sich Mischformen finden.

Generell ist es wichtig, ein klares Projektziel, ausgerichtet an den originären Aufgaben der Behörde zu definieren (IT-Alignment).

## 5.1. Reihenfolge der Migration

**Vorbereitung:**

- Zieldefinition
  - An welchen Stellen ist IPv6 relevant für die behördliche Aufgabe?
  - Ist eine Voll- oder Teilmigration sinnvoll?
  - Welche Meilensteine sind gefordert (Zeitplanung)?
- Bestandsaufnahme

  *(siehe hierfür auch Checkliste "Migrationsplanung", Seite 150 ff.)*
  - Netzaufteilung
  - Angebotene Dienste (und deren Life Cycles)
  - Netzübergänge
  - Betreiber
- Verträge
  - inklusive Kontakte, Laufzeiten, Abschreibungszeiträume und Service-Level Agreements (SLAs)

**Allgemeine Migrationsschritte:**

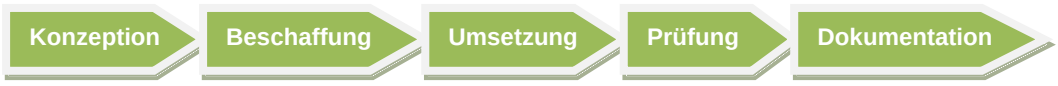


*Abbildung 5: Migrationsschritte*

In Anhang II im Abschnitt 14.1 (ab Seite 187) und in Abschnitt 9.2.1.2 sind die sinnvollen technischen Migrationsschritte aufgeführt. Diese beachten auch die Abhängigkeiten zwischen den IT-Komponenten, so dass es zu möglichst wenigen Betriebsunterbrechungen oder Störungen kommt.

### 5.1.1 Migration „von unten nach oben“

Dieses Vorgehen bei der Migration orientiert sich am Schichtenmodell der Kommunikation. Es werden zunächst die Netzinfrastrukturkomponenten (unten) wie Switche und Router IPv6-fähig gemacht, um diese Infrastruktur in Richtung Dual-Stack-Betrieb zu migrieren, selbst wenn diese zunächst nur mit IPv4 genutzt wird. Damit werden die Grundlagen für IPv6 geschaffen.

Zunächst wird mit der Sicherungsschicht (OSI-Layer 2, Switches) begonnen, danach werden die Vermittlungsschicht (Layer 3, IP-Router und Klienten) und die Infrastrukturdienste (u. a. DNS, DHCP, NTP) migriert. Abgeschlossen wird das Projekt mit der Migration der Anwendungen. Dieses Migrationsmodell wird in den folgenden Kapiteln ausführlich beschrieben. Die verschiedenen Migrationsschritte der jeweiligen Schichten werden in Kapitel 9 exemplarisch dargestellt.

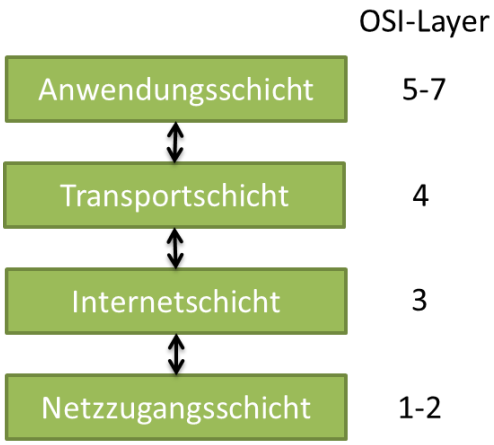


*Abbildung 6: Schichtenmodell der Kommunikation (TCP/IP)*

Werkzeuge für das Netzwerkmanagement und das Monitoring müssen vor Verwendung von IPv6-Diensten migriert werden, damit die neuen IPv6-Eigenschaften der Komponenten überwacht und gesteuert werden können. Schrittweise werden dabei neue Dienste integriert und der erreichte Stand getestet und dokumentiert.

Aus Sicherheitsgründen ist bei der Inbetriebnahme von IPv6-Funktionen auf den Komponenten darauf zu achten, dass diese nicht ungewollt mit einer unkontrollierten Konfiguration aktiv werden. Beispielsweise könnte das Betriebssystem auf einem Arbeitsplatzrechner in der Standard-Konfiguration versuchen, über ein verfügbares IPv6-Netz bereits unkontrolliert Verbindungen aufzubauen.

Zwingende Voraussetzung für dieses Vorgehen ist die gründliche Planung des Migrationsprozesses mit der Aufstellung eines Adresskonzepts und einer Netzarchitektur, die an IPv6 angepasst wird, sowie eines Zeitplans („Roadmap“).

Mit dem hier beschriebenen Vorgehen wird die Grundlage für eine erfolgreiche (Teil-)Migration sichergestellt.

### 5.1.2 Migration „von außen nach innen“

Die Idee hierbei ist, dass man kurzfristig eine IPv6-Kommunikation nach außen ermöglicht, während man mit einem entspannten Zeitplan die interne und in der Regel aufwändigere Migration der internen IT nachzieht.

Es sollten deshalb zuerst Subnetze und Dienste migriert werden, die eine Schnittstelle zwischen der Organisation und der Außenwelt darstellen. Dies kann z. B. ein Informationsangebot über ein Webportal (Fachverfahren), eine extern nutzbare Datenschnittstelle (z. B. EDI, OSCI) oder auch ein Zugang zur Infrastruktur mittels VPN sein.

Die interne Infrastruktur bleibt so vorerst unverändert, und wird anschließend in einem Folgeprojekt migriert. Wie schon in Kapitel 3 dargestellt, reflektiert dieses Vorgehen die Anforderung an die Rolle als Dienstleister, Angebote so zur Verfügung zu stellen, dass möglichst alle Kunden die Angebote nutzen können. Behörden stellen so den Zugang der Bürger zu ihrem Angebot sicher. Auf die Anforderung "Angebot von Informationen und Diensten über IPv6" wird damit an dieser Schnittstelle reagiert. Da die Netzbereiche „innen“ und „außen“ voneinander getrennt werden (durch Proxy bzw. Firewall) und dieser Übergang in der Regel einem Sicherheitsmonitoring unterliegt, ist dieses Vorgehen technisch sinnvoll.

### 5.1.3 Teilmigration

Das geschilderte schrittweise Vorgehen ermöglicht zudem Teilmigrationen. Der Vorteil einer Teilmigration ist der zunächst geringere Aufwand. Einzelne Dienste lassen sich damit vergleichsweise schnell auch mit IPv6 nutzen, und die externe IPv6-Sichtbarkeit wird hergestellt. Im folgenden Bild betrifft dies die mit roten und schwarzen Pfeilen gekennzeichneten Verbindungen.

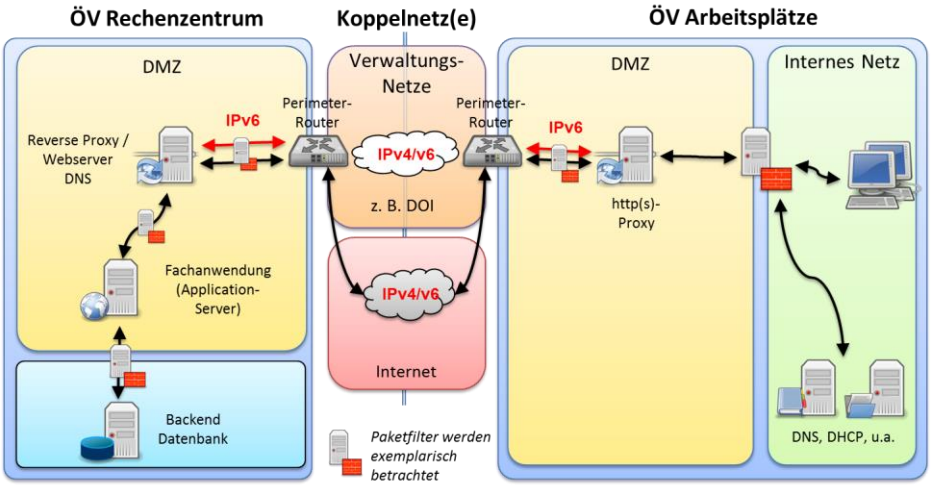


*Abbildung 7: ÖV-Teilmigration*

Das Vorgehen der Teilmigration nutzt dabei die bestehende Struktur der Netzarchitektur mit ihren Proxies. Die Kommunikation von IPv4/IPv6 wird dabei auf den Proxies terminiert, die ihrerseits eine neue Verbindung zum gewünschten Ziel

aufbauen. Dies findet oberhalb der Transportschicht statt und bietet sich daher auch zur Umsetzung zwischen IPv4 und IPv6 an. Im konkreten Fall kann damit eine Fachanwendung einer Verwaltung mit geringem Aufwand „IPv6-fähig“ gemacht werden, sobald ein oder mehrere IPv6-Koppelnetze zur Verfügung stellen.

Ein ähnliches Vorgehen kann auch zur Anbindung bestehender IPv4-Inseln an ein IPv6-Netz oder zum Aufbau interner, nativer IPv6-Netze (ohne IPv6-Konnektivität am Standort) genutzt werden.

Dieses Vorgehen hat allerdings die Einschränkung, dass es nicht bei allen Diensten umsetzbar ist. Bestimmte Protokolle einiger Dienste lassen sich bisher nicht auf Proxies terminieren und können deshalb nicht wie beschrieben teilmigriert werden. Die betrifft bisher nur wenige Dienste. Betroffen sind bestimmte VoIP- und Videokonferenz-Protokolle, bestimmte VPN-Konstellationen sowie diverse Eigenentwicklungen von Fachverfahren, siehe Abschnitt 9.3.2.

## 5.2. Vorgaben für die Verwaltung

Die öffentliche Verwaltung hat, koordiniert durch die LIR de.government, sinnvolle Vorgaben in Abstimmung mit den Bundesressorts, den Ländern und den Kommunen entwickelt. Diese werden kontinuierlich fortgeschrieben. Zudem hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) Sicherheitsleitlinien für den Einsatz von IPv6 erarbeitet [ISi-LANA]. Diese Informationen erhalten Behörden über die LIR de.government oder ihre zuständige Sub-LIR und das BSI.

Die entsprechenden Vorgaben sollten beachtet werden und sind in diesem Migrationsleitfaden berücksichtigt.

## 5.3. Schulung von Mitarbeitern

Nicht alle der von IPv4 bekannten Konzepte sind auch für IPv6 gültig. Kritischer sind darüber hinaus diejenigen Funktionen, die auf den ersten Blick bei IPv4 und IPv6 gleich sind, aber bei IPv6 plötzlich eine grundverschiedene Aufgabe haben. Somit ist es entscheidend für einen qualifizierten und sicheren Betrieb die neuen Eigenschaften von IPv6 gut zu kennen.

Im Idealfall sollte sich durch den Austausch der IP-Version für die Anwendungen aus Nutzersicht nichts ändern. Dieser Migrationsleitfaden zeigt, dass für diesen erwünschten, reibungslosen Betrieb mit IPv6 wichtige Punkte zu beachten sind.

Ist man bereits mit generellen Konzepten von IPv4-Netzen vertraut, so wird die Einarbeitung in IPv6 leicht fallen. Zwischen IPv4 und IPv6 gibt es mehrere entscheidende Unterschiede. Einerseits gibt es abweichende Mechanismen, beispielsweise bei der Adresszuweisung durch das Neighbor Discovery Protocol (NDP) anstelle des Address Resolution Protocol (ARP). Andererseits sind durch IPv6 grundsätzlich effizientere Netzarchitekturen als unter IPv4 möglich, z. B. durch Nutzung von deutlich größeren IP-Subnetzen für Klienten (Arbeitsplätze). Hierin liegt die große Chance, zukünftige Netze leistungsfähiger und effizienter zu gestalten.

Dies setzt aber voraus, dass diese Ansätze bekannt sind und eingesetzt werden können. Eine Schulung von Mitarbeitern sollte also nicht nur darauf aufbauen, bekannte Mechanismen aus IPv4 in IPv6 „zu übersetzen“. So entfällt z. B. bei IPv6 eine Adressumsetzung mittels NAT, da ausreichend individuelle Adressen für jedes Endgerät zur Verfügung stehen. Dies ermöglicht prinzipiell auch eine direkte Ende-zu-Ende-Kommunikation direkt auf der IP-Ebene, bei der der Datenstrom zwischen den Endgeräten unverändert übertragen wird.

Für diese direkten Verbindungen können in der öffentlichen Verwaltung etablierte Sicherheitsmechanismen, welche die Verbindung auftrennen (z. B. Proxys/ALGs), nicht mehr genutzt werden. Transparente ALGs können für unterstützte Protokolle weiterhin genutzt werden. Wo diese nicht verfügbar sind, muss die Kommunikationssicherheit direkt auf dem Endgerät sichergestellt werden, auf denen aktuell nicht das gleiche Schutzniveau wie auf zentralen Sicherheitssystemen gewährleistet werden kann.

Der sorgfältigen Planung von Netzarchitekturen und Sicherheitskomponenten kommt somit eine noch größere Bedeutung zu. Dazu sollte in den entsprechenden Schulungen darauf eingegangen werden, welche grundsätzlichen Eigenschaften die IP-Kommunikation hat und welche Designentscheidungen dem IPv6-Protokoll zu Grunde liegen. Die neuen Möglichkeiten von IPv6 sollten als Chance genutzt werden, gewachsene Netzstrukturen zu überarbeiten.

Der Einsatz von IPv4 musste im Laufe der Zeit um verschiedene Hilfsfunktionen erweitert werden, da IPv4 eigentlich schon vor vielen Jahren an seine konzeptionellen Grenzen gestoßen ist. Diese „Workarounds“ sind dem IT-Personal allerdings nicht mehr als solche bewusst, da sich alle Beteiligten über Jahre an diese gewöhnt haben. Diese Workaround führen zu latent höheren Kosten in jedem IT-Betrieb, erhöhen ohne Not die Komplexität von Netzinfrastrukturen drastisch und hemmen die Weiterentwicklung von Anwendungen und Diensten.

Ein qualifiziertes IPv6-Netzdesign stellt die Datenübertragung ohne diese Hilfsfunktionen der IPv4-Welt bereit. Somit werden diese historischen Sonderfunktionen zur Unterstützung des IPv4-Betriebs eines Tages überflüssig sein.

Die theoretische Beschäftigung mit IPv6 ist nicht ausreichend, damit Mitarbeiter die notwendige Qualifikation für einen sicheren Betrieb von IPv6-Infrastrukrturen erlangen. Praktische Kenntnisse sind dringend notwendig, da die IPv6-Funktionalität vieler Netz- und Softwarekomponenten sich aktuell noch in der Weiterentwicklung befinden. Mit der stark steigenden Verbreitung von IPv6 steigt auch die Gefahr durch IPv6-spezifische Angriffe auf Datennetze. Daraus leitet sich die neue Anforderung ab, IPv6-typische Angriffsarten zu kennen und sich mit möglichen Abwehrmaßnahmen auseinander zu setzen. Einen Überblick hierzu gibt Abschnitt 8. Die notwendigen praktischen Erfahrungen können gut in einer Testinfrastruktur erworben werden.

In Anhang V findet sich eine Zusammenstellung von weiterführenden Informationen zu IPv6 und zur Migration, welche als erste Anlaufstelle genutzt

werden kann. Bei der Auswahl der Literatur und der Online-Quellen sollte u. a. darauf geachtet werden, dass die jeweils aktuellsten Informationen verwendet werden. Das IPv6-Protokoll ist zwar schon seit über 15 Jahren definiert, es wird allerdings erst in letzter Zeit in größerem Umfang eingesetzt. Daher ergeben sich Anpassungen und Weiterentwicklungen, insbesondere bezüglich der Konfigurationsempfehlungen und „Best Practice“.

Die Schulungsmaßnahmen für Mitarbeiter bzgl. IPv6 sollten mindestens folgende Bereiche umfassen:

- Allgemeine, Hersteller-neutrale, IPv6-Grundlagenschulung
- Hersteller-spezifische IPv6-Schulungen
- Schulung zur IPv6-Sicherheit

## 5.4. Testinfrastruktur

Separate Testinfrastrukturen, welche die produktiven Umgebungen nachbilden, sind eine unabdingbare Voraussetzung für einen sicheren und soliden Betrieb von Diensten in der ÖV. Nur so können notwendige Änderungen und Aktualisierungen durchgeführt werden, ohne den Wirkbetrieb zu gefährden. IPv6 als Aktualisierung einer Infrastruktur stellt hierbei keine Ausnahme dar und ist deshalb nicht ursächlich für die Notwendigkeit solcher Testinfrastrukturen. Häufig fällt allerdings erst mit der Einführung von IPv6 auf, dass schon lange eine separate Testinfrastruktur notwendig gewesen wäre. Dies ist bei der Kalkulation der Kosten für die Einführung von IPv6 zwingend zu berücksichtigen.

Ein IPv6-Testnetz bildet idealerweise den Ausgangspunkt für ein Migrations-projekt. Hier können Hard- und Softwarekomponenten in den für die jeweilige Organisation typischen und geplanten Konfigurationen getestet werden. In einem solchen „Proof of Concept“-Aufbau werden zwangsläufig offene Punkte einer IPv6-Konzeption im praktischen Einsatz sichtbar. Dabei wird deutlich, welche dieser Komponenten für den Betrieb noch fehlen oder noch nicht fehlerfrei zusammenarbeiten.

Testinfrastrukturen sind auch in Beschaffungsprozessen ideal geeignet, Anbietern die Möglichkeit zu bieten die IPv6-Funktionstauglichkeit ihrer angebotenen Komponenten und Dienste zu beweisen.

# 6. Adresskonzepte und Netzarchitekturen

## 6.1. IPv6-Adressen

IPv6-Adressen sind 128 Bit lang und damit viermal so lang wie IPv4-Adressen. Anders als bei IPv4 ist bei IPv6 die Grenze zwischen Netzadresse und Systemadresse fest vorgegeben. Die Netzadresse befindet sich in den oberen 64 Bits und setzt sich aus dem globalen Routing-Präfix und der Subnetz-ID zusammen. Die Bits der Subnetz-ID bezeichnen die Nummer eines internen Netzes einer Organisation. Die unteren 64 Bits beinhalten den Interface Identifier (deutsch: Schnittstellenadresse), welcher für einen Host eindeutig die Adresse einer Netzwerkschnittstelle identifiziert.

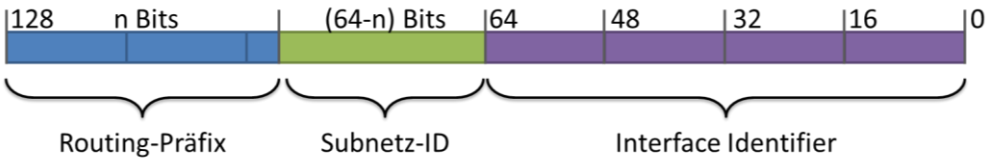


*Abbildung 8: Aufteilung einer IPv6-Adresse*

Jede vergebene IPv6-Adresse gehört zu genau einer Schnittstelle eines Hosts. Andersherum können aber jeder Schnittstelle mehrere IPv6-Adressen zugewiesen werden, z. B. für verschiedene „Scopes“ (link local, global, mobile IPv6). Für Details siehe [RFC4291] und [RFC5952].

### 6.1.1 Adresstypen

IPv6 hat wie IPv4 unterschiedliche Adresstypen. Die IPv6-Adresstypen lassen sich allerdings nicht eins-zu-eins auf die von IPv4 abbilden.

Um auf Dienste in anderen Subnetzen, an anderen Standorten oder sogar im Internet zugreifen zu können, benötigen Arbeitsplätze, Server und IP-Telefone eindeutige und routbare IP-Adressen. Für IPv6 können diese vom Typ „Global Unicast Address“ (GUA) oder „Unique Local Address“ (ULA) sein. Der Einsatz von ULA erfordert allerdings zwingend einen Proxy-Dienst, um Dienste außerhalb der eigenen Organisation oder ÖV nutzen zu können. Diese und andere Adresstypen werden im Folgenden im Detail erklärt.

Die verschiedenen Typen von IPv6-Adressen lassen sich wie folgt an den oberen Bits unterschieden und erkennen:

| Adresstyp | Binären Präfix | IPv6-Schreibweise |
|---|---|---|
| Unspezifiziert | 00…0 (128 Bits) | ::/128 |
| Loopback-Schnittstelle | 00…1 (128 Bits) | ::1/128 |
| Multicast | 11111111 | ff00::/8 |
| Link Local Unicast | 1111111010 | fe80::/10 |
| Unique Local (ULA) | 11111100<br>11111101 | fc00::/8<br>fd00::/8 |
| Global Unicast (GUA) | Alle anderen Adressen | |

*Tabelle 2: IPv6-Adresstypen*

IPv6-Anycast-Adressen werden aus dem Unicast-Adressraum zugeordnet (aus link local oder global unicast) und sind syntaktisch nicht von Unicast-Adressen unterscheidbar.

#### 6.1.1.1 Link Local Unicast

Link-lokale IPv6-Adressen sind in [RFC4291] definiert. Sie werden für die lokale Kommunikation innerhalb eines IP-Subnetzes oder über eine Punkt-zu-Punkt-Verbindung (point-to-point (PPP)) genutzt. IP-Router leiten keine Pakete mit Link Local Unicast Adressen weiter. Für IPv6 werden diese Adressen mit dem fe80::/64 Präfix gebildet. Zumeist werden sie vom Betriebssystem je Schnittstelle durch eine Autokonfigurationstechnik vergeben. Jedes IPv6-fähige Netzwerk-Interface muss mindestens eine Link-Local IPv6-Unicast-Adresse zugewiesen bekommen.

Zusätzlich ist der Einsatz von Link-Local-Adressen typisch in Transfernetzen zwischen zwei Routern und beim Aufbau von redundanten, ausfallsicheren Netzkopplungen.

#### 6.1.1.2 Multicast

IPv6-Multicast-Adressen werden verwendet, um mit einer einzelnen IPv6-Adresse eine Gruppe von Empfängern zu erreichen, genauer: eine Gruppe von Netzwerkschnittstellen. An diese Adresse gesendete IPv6-Pakete werden an alle Schnittstellen mit dieser Adresse geliefert. Eine einzelne Netzwerkschnittstelle kann auch zu mehreren Multicast-Gruppen gehören, indem sie deren IPv6-Multicast-Adressen zugewiesen bekommt.

IPv6-Multicast-Adressen bestehen aus dem Präfix FF00::/8, 4 Bits Flags, 4 Bits Scope (Reichweite) und einer 112 Bit langen GroupID. Als Scopes sind im

Standard definiert: Interface-Local, Link-Local, Admin-Local, Site-Local, Organization-Local und Global scope. Siehe dazu auch [RFC4007].

Für IPv6 sind Multicast-Adressen von zentraler Bedeutung, da über diese eine Vielzahl von Protokoll-eigenen Funktionen realisiert wird, die bei IPv4 über lokale Broadcasts implementiert wurden (Broadcasts entfallen bei IPv6). Dazu wurden wohlbekannte („well known“) IPv6-Multicast-Adressen im Standard definiert, z. B. für „alle Router in meinem Subnetz“ oder „alle NTP Server meiner Organisation“.

#### 6.1.1.3 Anycast -Adressen

IPv6-Anycast-Adressen [RFC4291] werden verwendet, um mit einer einzelnen IPv6-Adresse einen aus einer Gruppe von Empfängern zu erreichen, genauer: aus einer Gruppe von Netzwerkschnittstellen. An diese Adresse gesendete IPv6-Pakete werden an *eine* ausgewählte Schnittstelle mit dieser Adresse geliefert. Es ist Aufgabe der IPv6-Router einer Infrastruktur, dafür zu sorgen, dass Pakete zu dieser Anycast-Adresse zur „nächstgelegenen“ Schnittstelle mit der gewünschten Adresse geleitet werden. Eine einzelne Netzwerkschnittstelle kann auch zu mehreren Anycast-Gruppen gehören, indem sie deren IPv6-Anycast-Adressen zugewiesen bekommt.

IPv6-Anycast-Adressen können aus einem der o. g. Unicast Adressräume (Link-lokal oder Global) stammen, sie besitzen kein spezielles Präfix.

Anycast wird verwendet, um eine Redundanz zu erreichen, so dass immer mindestens ein Server aus einer Gruppe erreichbar ist. Der Vorteil für Klienten ist, dass dieses Fail-Over für sie transparent ist, da sich die IPv6-Adresse des angesprochenen Dienstes nicht ändert. Anycast-Adressen können z. B. als DNS-Server-Adressen verwendet werden, wenn mehrere, redundante DNS-Server in einer Organisation vorhanden sind.

#### 6.1.1.4 Global Unicast Address (GUA)

IPv6 Global Unicast Adressen ([RFC4291], Abschnitt 2.5.4) dienen der IPv6-Kommunikation zwischen zwei IPv6-Schnittstellen, üblicherweise an zwei verschiedenen Endgeräten. GUA bestehen wie in Abschnitt 6.1 beschrieben aus einem globalen Routing-Präfix, einer Subnetz-ID und einer Schnittstellenadresse (siehe auch Abbildung 8 und Abschnitt 6.1.2). GUAs werden standardmäßig für die globale IPv6-Kommunikation zwischen Systemen genutzt.

#### 6.1.1.5 Unique Local Address (ULA)

Unique Local Adressen [RFC4193] sind Unicast Adressen für eine organisations-interne IPv6-Kommunikation, welche mit hoher Wahrscheinlichkeit auch global einmalig sind. Sie sind routbar innerhalb einer Organisation, gegebenenfalls auch über Standorte/Liegenschaften hinweg. ULA sollten per Definition nicht im Internet geroutet werden. ULA sind an ihrem in Tabelle 2 aufgelisteten Präfix zu erkennen und können dadurch leicht an administrativen Grenzen gefiltert werden. Ihre Hauptanwendung besteht in der lokalen Kommunikation innerhalb eines Standortes oder innerhalb einer begrenzten Gruppe von Standorten. Dort können sie verwendet werden, ohne das eine Umnummerierung (Renumbering) notwendig würde, falls sich das globale Präfix eines Standortes ändert (wie bei

GUA). Mit ULAs ist eine globale Ende-zu-Ende Kommunikation über dritte Netze (insbesondere, das Internet) im Allgemeinen nicht möglich.

Aus technischer (Software-)Anwendungssicht können ULA und GUA gleich behandelt werden, d. h. eine Anpassung von Anwendungen speziell auf die Verwendung von ULA oder GUA ist nicht notwendig.

#### 6.1.1.6 IPv6-eingebettete IPv4-Adressen

IPv6-Adressen mit eingebetteten IPv4-Adressen sind in [RFC4291] definiert. Es werden zwei Typen unterschieden:

- „IPv4-compatible IPv6 address“
- „IPv4-mapped IPv6 address“

Der erste Adresstyp ist überholt und wird nicht mehr verwendet. Geräte, Klienten und Anwendungen müssen diesen Adresstyp nicht mehr unterstützen.

Die „IPv4-mapped“-Adressen finden jedoch für die Transition zu IPv6 bei einigen Techniken Verwendung (z. B. NAT64). Sie repräsentieren IPv4-Adressen als 128 Bit lange IPv6-Adressen, z. B. in einem IPv6-only-Umfeld. Das Format der „IPv4-mapped“ Adressen ist:

**0000:0000:0000:0000:0000:ffff:<IPv4-Adresse>**

Siehe in [RFC4038] für weitere Hintergrundinformationen zu diesen Adressen. Dieser Adresstyp ist die Grundlage für ein Konzept zur deutlichen Verringerung der Anzahl von IPsec-SAs in vollvermaschten IPsec-Overlay-Netzen der öffentlichen Verwaltung.

### 6.1.2 Wahl des Adresstyps (GUA / ULA)

Bei der Erstellung eines IPv6-Adressschemas für eine öffentliche Verwaltung gilt es für jedes IP-Subnetz einen IPv6-Adressbereich zu planen. Dabei muss je IP-Subnetz auch ein IPv6-Adresstyp ausgewählt werden. Je nach den Anforderungen des jeweiligen IP-Subnetzes macht es Sinn, „Global Unicast“ Adressen (GUA) oder „Unique Local“ Adressen (ULA) in diesem Subnetz zu verwenden. Bei diesen Anforderungen geht es im Wesentlichen um zwei Fragestellungen:

(a) die Kommunikationsanforderungen für Systeme in diesem Subnetz und

(b) der Schutzbedarf dieses Subnetzes.

Im Folgenden werden hier die wichtigsten Eigenschaften der beiden Adresstypen genannt:

ULA

- ULA-IP-Adressen sind nicht im Internet routbar

- ein Subnetz-Präfix kann ohne eine Beantragung / Registrierung erstellt werden
- Interne IP-Kommunikation über Subnetz-Grenzen hinweg ist möglich

GUA

- Globale Adressierbarkeit von Endsystemen ist möglich
- Globale Routbarkeit dieser IPv6-Adressen im Internet ist gegeben
- (potentiell) ist eine Ende-zu-Ende-Kommunikation möglich (dort wo es sicherheitstechnisch zugelassen ist)
- Können auch ausschließlich intern verwendet werden

Für behördenübergreifende Kommunikation wird der Einsatz von GUAs aus dem Adressbereich der LIR de.government empfohlen. ÖV-interne Subnetze können je nach Anforderung ULA- oder GUA-basierte Adressen verwenden.

Für weitere Details und Erörterungen sollten auch die Ausführungen bezüglich der Netz- und Adresstypen in [ISi-LANA] beachtet werden, bevor eine endgültige Entscheidung für einen Adresstyp (je Subnetz) getroffen wird.

Folgende sinnvolle Optionen bestehen z. B. je Subnetz für die Adressauswahl:

1. Zugangs- und Koppelnetze (DOI oder Internet) → GUA
2. DMZ-Netze → GUA
3. Interne Netze ganz ohne Zugang „nach außen“ (z. B. Sensornetze oder Managementnetze) → ULA sind ausreichend
4. Interne Netze mit Zugang „nach außen“ ausschließlich über Proxy → ULA oder GUA
5. Interne Netze mit Zugang „nach außen“ ohne Proxy → GUA

Insbesondere bei Arbeitsplatz-Subnetzen vom Typ 4 ist im Einzelfall zu entscheiden, welcher Adresstyp verwendet werden soll. Dabei sollten auch zukünftige Entwicklungsmöglichkeiten wie IT-Konsolidierungen beachtet werden.

Technisch ist auch die parallele Nutzung beider Adresstypen parallel in einem IP-Subnetz möglich. Dies bringt jedoch einen erhöhten Verwaltungsaufwand und Sicherheitsrisiken mit sich.

### 6.1.3 Schnittstellenadressen

Für die Vergabe der einzelnen IPv6-Adressen an die Netzwerkschnittstellen (engl.: Interface Identifier) der Hosts innerhalb von IPv6-Subnetzen gelten sinngemäß dieselben Regeln wie für IPv4:

- Server müssen feste Adressen erhalten (mindestens eine pro Schnittstelle)

- die Server-Adressen sollten im DNS registriert werden (AAAA Datensätze sind anzulegen)
- Arbeitsplatzrechner können dynamisch Adressen aus einem Adress-Pool erhalten (oder IPv6-Autokonfiguration verwenden)
- weitere Informationen hierzu sind in Anhang II im Unterabschnitt 14.2.2.1 zu Klienten zu finden.

Für Hosts aus der o. g. Beispiel-ÖV könnten die Adressen dann z. B. wie folgt lauten:

| Host | IPv4-Adresse | IPv6-Adresse | Hinweis |
|---|---|---|---|
| Dateiserver | 192.168.22.**9** | <ÖV-Präfix>:1022::**9** | fest auf ::9 definiert |
| Zeitserver | 193.193.98.**3** | <ÖV-Präfix>:f098::**3** | fest auf ::3 definiert |
| Arbeitsplatz-PC | 10.**0.20.147** | <ÖV-Präfix>:0010::3000 | Dynamisch aus IP Pool vergeben (hier z. B.: 3000-3fff) |

*Tabelle 3: Beispielhafte IPv4/IPv6-Adressen für verschiedene Endsysteme*

Ferner ist zu entscheiden, wie die vorgesehenen IPv6-Adressen technisch den Endgeräten zugewiesen werden. Dazu gibt es verschiedene Techniken:

- Statisch konfiguriert
- Stateful DHCPv6
- SLAAC mit Route Announcements (RA)

Auch IP-Adress-Management-Systeme (siehe Abschnitt 6.4) nutzen diese Techniken, um – basierend auf einer Datenbank – die Adressen zuzuweisen und zu dokumentieren.

## 6.2. IPv6-Adresskonzepte

Bei der Einführung von IPv6 werden allen betroffenen Geräten zusätzlich eine oder mehrere IPv6-Adressen zugeordnet. Für eine strukturierte und nachhaltige Migration ist ein Adresskonzept für die konkrete ÖV zu erstellen. Angelehnt an die vorhandene Netzinfrastruktur sollten die Netzwerksegmentierungen, die in den Beschränkungen von IPv4 begründet sind, überarbeitet werden. Das Konzept sollte so aufgebaut sein, dass es auch zukünftige Subnetze in einer ÖV mit berücksichtigen kann. Es ist hierfür sinnvoll, ein Adresskonzept zu erstellen, welches alle Subnetze einer ÖV abdeckt, auch wenn zuerst nur einige Subnetze

(z. B. DMZ mit öffentlichen Servern) auf Dual-Stack-Unterstützung umgestellt werden. Ferner sollten Reservebereiche im Adressschema vorgesehen werden, um später weitere IPv6-Subnetze eines bereits vorhandenen Typs (z. B. Arbeitsplatznetz) bezüglich ihrer Netzpräfixe fortlaufend nummerieren zu können. Dies vereinfacht die Konfiguration von Routern und Sicherheitskomponenten durch die dann mögliche Aggregation von Routen bzw. Regeln.

### 6.2.1 Vergabe von Netzwerkpräfixen

Zu allererst benötigt eine ÖV als Basis für ihr IPv6-Adresskonzept ein ihr zugeordnetes, statisches und eindeutiges IPv6-Präfix. Dieses beginnt in Deutschland immer mit **2a02:1000::/26**, dem IPv6-Adressbereich, den das Bundesministerium des Innern (BMI) von der internationalen Organisation „Réseaux IP Européens Network Coordination Centre“ (RIPE NCC) am 16.11.2009 für die öffentlichen Verwaltungen in Deutschland erhalten hat.

Eine ÖV muss ihr IPv6-Präfix im Allgemeinen bei der für sie verantwortlichen Sub-LIR („Local Internet Registry“) beantragen. Im Ergebnis dieses Prozesses wird der ÖV ein IPv6-Präfix zugewiesen. Dieses setzt sich zusammen aus den o. g. 26 Bits, plus 6 Bits, die vom Bundesverwaltungsamt in seiner Funktion als Local Internet Registry (LIR) „de.government“ vergeben werden, plus 16 Bits, welche von der Sub-LIR vergeben werden. Dies ist in der folgenden Abbildung 9 zusammengefasst.

Detaillierte Hintergrundinformationen hierzu finden sich im IPv6-Referenzhandbuch [IPV6_REF] und in [RIPE_ADDR].

Wird einer ÖV ein 48 Bit langes Präfixes zugewiesen, so setzt sich dieses wie folgt zusammen:

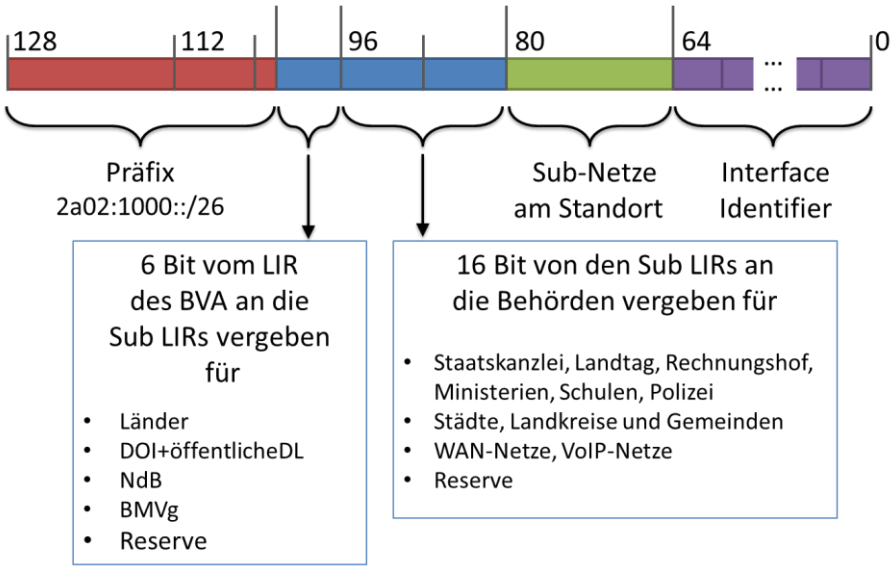


*Abbildung 9: Zusammensatzung einer IPv6-Adresse für ÖVs in Deutschland*

Aus Sicht einer ÖV werden ihr die Adressbits für den roten und blauen Bereich von extern zugeordnet; über den grünen Bereich kann die IT-Administration der

ÖV selbst entscheiden. Für den Bereich der Interface Identifier (lila Bereich) müssen für Server eigene, feste Nummern durch die lokale IT-Administration vergeben werden (analog zu Serveradressen bei IPv4).

Für Arbeitsplätze wird eine automatische Vergabe der Interface Identifier mittels einer der dafür vorgesehenen IPv6-Techniken empfohlen. Für Details hierzu siehe Abschnitte 6.1.2 und 6.1.3 in diesem Dokument.

### 6.2.2 Mittlere ÖV

Einer mittelgroßen ÖV wird in der Regel von ihrer Sub-LIR (Unter-Verteilstelle) für IPv6 ein 48 Bits langes Präfix zugeordnet werden. Dies bedeutet für die Strukturierung der IPv6-Adressen, dass zwischen Präfix und Interface Identifier 16 Bits verbleiben, mit denen eine ÖV ihre lokalen Subnetze strukturieren kann, da laut IPv6-Standard immer 64 Bits für die Schnittstellenadresse verwendet werden.

Es lassen sich also bei einem /48-Präfix bis zu $2^{16} = 65536$ IPv6-Subnetze anlegen. Das folgende Bild veranschaulicht diese Aufteilung einer IPv6-Adresse:

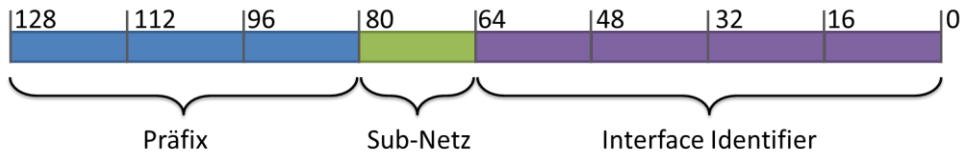


*Abbildung 10: Aufteilung einer IPv6-Adresse bei Verwendung eines /48-Präfixes*

*Auf das Zustandekommen des hier blau markierten Präfixes geht Abschnitt 6.1 in diesem Dokument im Detail ein.*

Bei dem gezeigten Schema ist es vorteilhaft, die Subnetze einer ÖV nicht einfach von „0000“ an durchzunummerieren, sondern stattdessen die 16 Bits der Subnetzmaske semantisch zu strukturieren. Hierfür wird in der Praxis empfohlen, die höherwertigen Bits „von links“ für eine semantische Strukturierung, z. B. Subnetztypen, und „von rechts“ zur Durchnummerierung (0, 1, 2, 3, …) zu verwenden. Folgendes Schema wird zur Strukturierung der 16 Bits empfohlen, wenn ein /48 Präfix vorhanden ist:

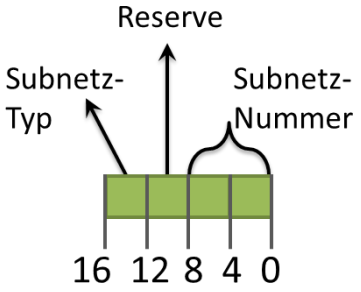


*Abbildung 11: Aufteilung der Subnetze in 4-Bit-Blöcke*

Dieses Schema ist vorteilhaft, da es erlaubt, Netzwerkpolitiken (engl. „network policies“) und Zugangskontrolllisten (engl. „access control lists“, ACLs) je Subnetztyp durch eine Maskierung und Filterung auf den ersten 48+4=52 Bits zu überschaubar zu halten.

Bei wachsenden Netzinfrastrukturen kann dieses Schema auch zusätzlich den Reservebereich nutzen, ohne das bisherige Schema verlassen zu müssen (keine Renummerierung notwendig). Je nachdem, ob noch mehr Subnetztypen oder noch mehr Subnetze (>256 je Typ) angelegt werden sollen, kann das Schema wie folgt erweitert werden:

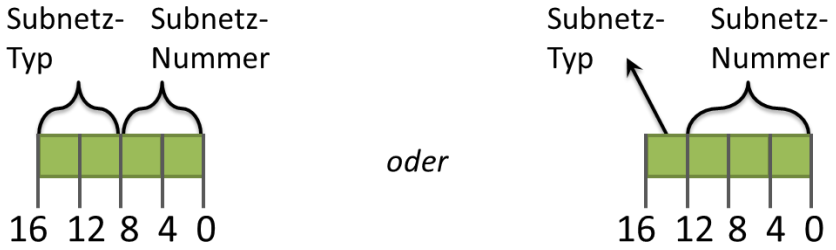


*Abbildung 12: Alternative Aufteilung der 16-Bit-Subnetzmaske in 4-Bit-Blöcke*

Der Bereich der Subnetznummern kann in der Praxis zur Einbettung der vorhandenen IPv4-Subnetznummern verwendet werden. Dies erleichtert die Administration der Netzwerke durch eine erleichterte Lesbarkeit der IPv6-Adressen. Zum Beispiel kann zu einem vorhandenen IPv4-Subnetz 192.168.**98**.0/24 – dem sog. „98er“ Netz – bei der Migration zu Dual Stack das IPv6-Subnetz mit dem Adressraum <Präfix>:00**98**::/64 zugeordnet werden. Für Details zur Wahl von IPv6-Subnetzen siehe auch Abschnitt 6.3 in diesem Dokument.

### 6.2.3 Kleine ÖV

Für eine kleine ÖV gilt sinngemäß das Gleiche, was in Abschnitt 6.2.2 für eine mittlere ÖV geschrieben wurde, jedoch wird hier in der Regel nur ein /56-Präfix vergeben werden.

Als „kleine ÖV“ sehen wir hier stellvertretend:

(a) Kleine Verwaltung, z. B. Ordnungsamt einer Kommune

(b) Teile einer inhaltlich zusammenhängenden, größeren ÖV
(z. B. eine von mehreren Schulen in einem Bezirk)

(c) Räumlich abgegrenzte Liegenschaften, z. B. ein kommunaler Ableger eines größeren Amtes.

„Klein“ bezieht sich hier auf die Anzahl der vorhandenen bzw. zukünftig zu erwartenden Geräte, welche in der ÖV IPv6-Adressen benötigen.

Das folgende Bild veranschaulicht die Aufteilung einer 128-Bit-IPv6- Adresse bei Verwendung eines /56-Präfixes:

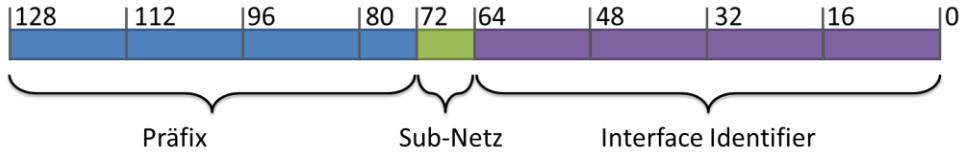


*Abbildung 13: Aufteilung einer IPv6-Adresse bei Verwendung eines /56-Präfixes*

Analog zu Abschnitt 6.2.2 können die hier verbleibenden 8 Bits zur Strukturierung von Subnetzen verwendet werden. Falls keine funktionell verschiedenen Subnetze vorhanden sein sollen, können die 8 Bits auch direkt zur Nummerierung der Subnetze verwendet werden. Beide Varianten sind im Folgenden dargestellt:

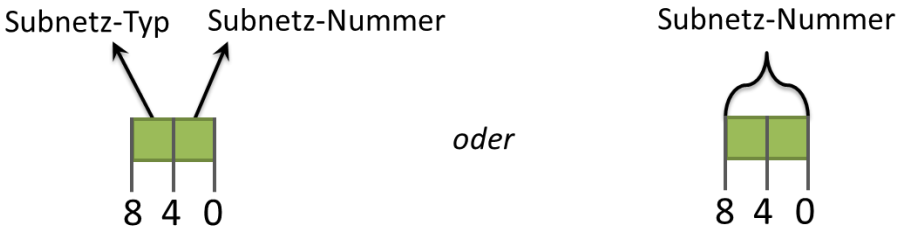


*Abbildung 14: Alternative Aufteilung der 8-Bit-Subnetzmaske in 4-Bit-Blöcke*

Ferner ist eine Aufteilung mit 2 Bits Subnetztyp plus 6 Bits Subnetznummer möglich, dies erschwert jedoch die Lesbarkeit von IPv6-Adressen und damit die Administration und ggf. die Fehlersuche.

### 6.2.4 Heimarbeitsplätze

Eine Sonderrolle bei der IPv6-Adressvergabe stellen Heimarbeitsplätze und sehr kleine Verwaltungseinheiten (z. B. ein einzelnes, u. U. temporär ausgelagertes Büro einer ÖV) dar (engl.: small office / home office, SoHo). Diese beiden Fälle ähneln sich sehr stark:

- es sind nur einige wenige Systeme am Standort vorhanden, die IP-Adressen benötigen (Faustregel: 1-30)
- es sind keine Server oder Dienste am Standort vorhanden
- die Anforderungen an die Verfügbarkeit einer Internetverbindung sind gering (geringe Kritikalität)
- die Anforderungen an die gemeinsam genutzte Bandbreite der dort vorhandenen Geräte ist gering

Für diese Fälle wird empfohlen, einen Internetzugang über einen öffentlich verfügbaren Internetprovider zu nutzen. Dies kann z. B. ein DSL-, Kabel- oder auch UMTS-Internetanschluss sein. Bevorzugt sollten leitungsgebundene Anschlüsse genutzt werden.

Der Provider sollte hierfür natives IPv6 plus IPv4 direkt an seinen Anschlüssen anbieten, also Dual Stack Funktionalität ohne die Notwendigkeit für Tunnelprotokolle zur Verfügung stellen. Hierbei wird das Präfix für den Standort direkt vom Provider vergeben. In diesem Fall muss das Home-Gateway (engl. customer premises equipment, CPE) die ICMPv6 mit Präfixdelegation (ICMPv6 prefix delegation, ICMPv6-PD) unterstützen.

Ist IPv6 nicht direkt vom Provider verfügbar, so wird empfohlen, auf dem Home-Gateway (CPE) bzw. dem Gateway der ÖV einen IPv6-Tunnelendpunkt zu installieren (6in4-Tunnel), welcher mit einem IPv6-Tunnelbroker bei einem kommunalen RZ oder LRZ verbunden wird. Siehe hierzu auch Abschnitt 7.5 zu den Empfehlungen bzgl. aktueller Übergangstechniken. Auch für einen Zugang mittels eines Tunnelprotokolls muss das CPE ICMPv6-PD unterstützen.

Für den sicheren Zugang zu internen Netzwerken und Diensten (z. B. Dateiserver) einer ÖV von solchen kleinen Standorten bzw. Heimarbeitsplätzen aus sollte – unabhängig vom IPv6-Internetzugang – ein IPsec-basiertes VPN-Gateway verwendet werden, welches IPv6 auf Transportebene unterstützt (innerhalb und außerhalb des IPsec-Tunnels). Es wird empfohlen, die VPN-Verbindung direkt von den Endsystemen und nicht von einem vorhandenen Home-Gateway (keine LAN-zu-LAN-Kopplung) aufzubauen, um eine möglichst weitgehende Ende-zu-Ende-Sicherheit (Verschlüsselung) zu erreichen.

### 6.2.5 Rechenzentrum / Große ÖV

Für große öffentliche Verwaltungen, z. B. Ministerien, gilt, dass bei einem begründeten Bedarf an IPv6-Netzen größer /48, je Liegenschaft ein separates /48-Präfix vergeben werden kann. Dies geschieht in Absprache mit der zuständigen Sub-LIR. Im Falle von Rechenzentren gilt dies analog, da hier oft auf Grund virtualisierter Netze und IT-Infrastrukturen (z. B. mandantenfähige Diensteinstallationen) große Mengen von Hosts und IP-Subnetzen in Betrieb sind.

Für die Strukturierung der IPv6-Adressen in Subnetztyp und Subnetznummer gilt das in Abschnitt 6.2.2 „Mittlere ÖV“ geschriebene. Insbesondere für ein Rechenzentrum wird jedoch voraussichtlich eine noch stärkere semantische Strukturierung der Adressen sinnvoll sein, z. B. indem einige Bits der Adresse zur Kodierung von VLANs oder direkt von Mandantennummern genutzt werden könnten.

Beim Management großer IT-Infrastrukturen mit IPv6 wird die direkte Eingabe alphanumerischer IPv6-Adressen voraussichtlich eine geringere Rolle spielen als bisher, und statt dessen werden verstärkt semantische Namen genutzt werden (zusammen mit IP-Adressmanagementsystemen (IPAM), siehe dazu Abschnitt 6.4).

## 6.3. Beispielhaftes Adressschema für eine mittlere ÖV

Dieser Abschnitt zeigt eine mögliche Vergabe von IPv6-Adressen in einer ÖV auf, welche zusätzlich zu vorhandenen IPv4-Adressen in ihren Netzwerken und IPv6 einführen möchte (Dual-Stack-Betrieb).

Als erstes sollte dazu – sofern nicht bereits vorhanden – eine Analyse und Dokumentation der aktuell vorhandenen IPv4-Netzwerke durchgeführt werden. In diesem Beispiel wird angenommen, dass die IP-Subnetze aus Tabelle 4 vorhanden sind.

Zur Vorbereitung eines IPv6-Adressschemas sollten folgende Punkte geklärt werden:

- Woher (RZ oder Sub-LIR) erhalte ich ein globales IPv6-Präfix für meine ÖV? Befindet sich meine zuständige Sub-LIR bereits im Wirkbetrieb?
- Wurde meiner ÖV durch das Adressrahmenkonzept der zuständigen Sub-LIR bereits ein Adressbereich zugewiesen oder muss ein Antrag gestellt werden?
- Welche Präfixlänge ist geplant und ist diese nach den RIPE-Regeln begründbar? Wie viele Präfixe sind geplant?
- Ist an allen Netzübergängen aller Liegenschaften meiner ÖV schon IPv6 verfügbar?
- Existiert eine Vereinbarung mit dem Dienstleister für den Netzübergang, das globale IPv6-Präfix meiner ÖV zu routen?

Für eine detaillierte Planung empfiehlt sich ein Durcharbeiten der Checkliste Migrationsplanung im Anhang I ab Seite 150 in diesem Dokument.

Entscheidend für die Adressplanung ist, dass die Präfixlänge bereits fest steht. Im folgenden Beispiel wird ein IPv6-Präfix der Länge 48 Bits angenommen. Bei einem /48 Präfix bedeutet die Planung der Adressen für die vorhandenen IP-Subnetze gleichzeitig die Frage, wie die dem Präfix folgenden 16 Bits zur Strukturierung genutzt werden. Die restlichen 64 Bits der Adresse dienen der Identifikation einer Schnittstelle eines Hosts; siehe Abschnitt 6.1.2.

Zur Vereinfachung des späteren IPv6-Netzwerkmanagements für die IT-Administration in der ÖV ist es sinnvoll, das numerische Schema vorhandener IPv4-Adressen auch im IPv6-Adresskonzept wiedererkennen zu lassen, für eine „visuelle“ Wiedererkennung von IP-Subnetzen. Zum Beispiel sollten Server aus dem IPv4-Subnetz 193.193.98.0/24 zukünftig auch unter IPv6 einem „98er“-Subnetz zugeordnet sein, also eine „98“ innerhalb der IPv6-Adresse enthalten. Dies macht die Pflege und Fehlersuche in den neuen IPv6-Subnetzen deutlich einfacher.

Im Folgenden wird aufgezeigt, wie die neuen IPv6-Adressen „passend“ zu den vorhandenen IPv4-Adressen strukturiert werden können. Im angenommenen Beispiel seien folgende Netze vorhanden:

| | IPv4-Netzadresse / Präfixlänge | Subnetztyp | Bemerkung |
|---|---|---|---|
| 1 | 10.0.0.0 / 8 | Privates, internes /8 IPv4-Subnetz | Class A Subnetz, Arbeitsplätze |
| 2 | 192.168.22.0 / 24 | Privates, internes /24 IPv4-Subnetz | Class C Subnetz, interne Server |
| 3 | 193.193.96.0 / 23 | Öffentlicher IPv4-Adressbereich der ÖV für IPv4-Quell-NAT | NAT-Bereich für Arbeitsplätze |
| 4 | 193.193.98.0 / 24 | Öffentliches IPv4-Subnetz der ÖV, für DMZ-Subnetze | DMZ mit öffentlichen Servern der ÖV, z. B. Webserver |
| 5 | 193.193.99.8 / 28 | Weiteres Öffentliches IPv4-Subnetz der ÖV, für DMZ-Subnetze | Kleine Projekt-DMZ der ÖV mit Servern bestimmter Projekte |

*Tabelle 4: Beispielhafte Erfassung vorhandener IPv4-Netze*

Basierend auf dieser Aufstellung kann eine mögliche Klassifizierung in Subnetztypen in „interne Netze ohne Internetzugang“, „Arbeitsplatznetze mit Internetzugang“, „DMZ-Netze“ usw. erstellt werden. Ein Subnetz*typ* zeichnet sich dadurch aus, dass alle Netzwerke dieses Typs von Gateways, Routern und Firewalls gleich behandelt werden.

Ferner ist beim Aufbau des neuen Adressschemas zu beachten, dass für IPv6 kein Quell-NAT (auch „Masquerading“ genannt) mehr verwendet wird. Bei IPv6 entfällt die Notwendigkeit für IP-Adressbereiche, welche bei IPv4 dediziert für NAT reserviert wurden („NAT-Pools“, siehe Zeile 3 in o. g. Beispieltabelle).

Bei der Verwendung von /48 IPv6-Präfixen für eine Liegenschaft wird empfohlen, die verfügbaren 16 Bits für Subnetze wie folgt in 4-Bit-Blöcke, sogenannte Nibbles, aufzuteilen:

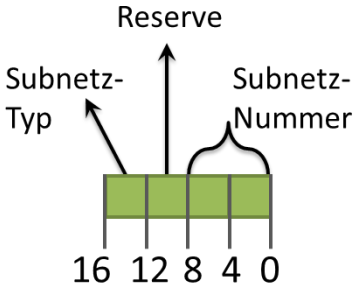


*Abbildung 15 : Aufteilung der Subnetze in 4-Bit-Blöcke*

Durch eine Unterteilung wie in Abbildung 15 lassen sich 16 Subnetztypen unterscheiden, wobei zu jedem Typ 256 Subnetze erstellt werden können. Je nach den Anforderungen der Zukunft lässt sich dieses Konzept ohne Änderung des Schemas erweitern. Dazu wird das noch nicht genutzte Nibble entweder zur Vergrößerung des Subnetz-*Typ*-Bereichs oder des Subnetz-*Nummern*-Bereichs verwendet. Der Subnetz-Typ-Bereich kann damit von 16 auf 256 Netztypen erweitert werden, alternativ kann die Anzahl der adressierbaren Subnetze von 256 auf 4096 anwachsen.

Sei z. B. eine gewählte Zuordnung der Subnetztypen [0-9a-f]:

| Subnetztyp | Bedeutung | Bemerkung |
|---|---|---|
| 0 | Arbeitsplätze | |
| 1 | Interne Server | |
| 2-9 | | noch ungenutzt |
| a, b, c, d, e | | noch ungenutzt |
| f | DMZ-Subnetze | |

*Tabelle 5: Beispielhafte Abbildung von Subnetznummern auf Subnetztypen*

Für das oben genannte Beispiel können die fünf in Tabelle 4 erfassten IP-Subnetze nun wie folgt in IPv6 abgebildet werden:

| | IPv4-Netzadresse / Präfixlänge | IPv6-Netzadresse / Präfixlänge | Bemerkung |
|---|---|---|---|
| 1 | **10**.0.0.0 / 8 | <ÖV-Präfix>:**0**0**10**:: / 64 | „10er“ Netz |
| 2 | 192.168.**22**.0 / 24 | <ÖV-Präfix>:**1**0**22**:: / 64 | „22er“ Netz |
| 3 | 193.193.96.0 / 23 | --- | *entfällt bei IPv6* |
| 4 | 193.193.**98**.0 / 24 | <ÖV-Präfix>:**f**0**98**:: / 64 | „98er“ DMZ-Netz |
| 5 | 193.193.**99**.8 / 28 | <ÖV-Präfix>:**f**0**99**:: / 64 | „99er“ DMZ-Netz |

*Tabelle 6: Beispielhafte Abbildung von Subnetznummern auf Subnetztypen*

Bei der Abbildung der Netznummern (hier: 10, 22, 98, 99) ist zu bedenken, dass es sich in der Schreibweise der IPv6-Adressen um hexadezimale Zeichen handelt. Daher unterscheiden sich bei einer Netzwerkanalyse die Werte der tatsächlich in den IP-Adressbytes auftauchenden Bits:

- IPv4: (dez) 10 = (binär) **00001010** ; IPv6 (hex) 10 = (binär) **00010000**
- IPv4: (dez) 99 = (binär) **01100011** ; IPv6 (hex) 99 = (binär) **10011001**

Bei textueller Ausgabe der IP-Adressen, welche die meisten Netzwerk-Tools und -Analyser unterstützen, spielt dieser Unterschied in den Adressbytes jedoch keine Rolle. Dies gilt ebenso für typische Logfiles (syslog, htaccess), in denen IP-Adressen ausschließlich in menschenlesbarer, textueller Form auftauchen.

Als Nebeneffekt des o.g. Formats stellt sich die Frage, wie vorhandene Netznummern ≥ 100 innerhalb der IPv6-Adresse abgebildet werden können. Alternativ nutzt man ein Schema mit 3 Zeichen für die Subnetznummer (z. B. (IPv4) 193.193.**175**.0 → (IPv6) :**0175**:), oder man verwendet weiterhin zwei Zeichen und nutzt für Netznummern ≥ 100 den hexadezimalen Zahlenbereich >(hex)99, also die Werte „a0“ bis „ff“.

Zum vorgeschlagenen IPv6-Adressschema und dessen Planung sollten weiterhin folgende Hinweise beachtet werden:

- Auch ehemals sehr kleine IP-Subnetze bekommen auf Grund des großen Adressraumes von IPv6 immer mindestens einen Adressbereich für $2^{64}$ mögliche Hosts.
    - IPv4-Subnetze gleichen Typs sollten soweit sinnvoll und technisch machbar in ein IPv6-Subnetz zusammengefasst werden. Dies vereinfacht interne Routingtabellen, da im Vergleich zu IPv4 weniger Routing-Einträge zu pflegen sind.
    - Ferner sollten aber Geräte mit unterschiedlichen Anforderungen, die bei IPv4 in einem Subnetz liegen mussten, in IPv6 eigene Subnetze bekommen.
- Alle IPv6-Adresstypen, bis auf Link-lokale Adressen, sind grundsätzlich global routbar. Dies trifft folglich auch die in Tabelle 3 aufgelisteten IPv6-Adressen zu. Notwendige Zugangsbeschränkungen müssen daher immer durch entsprechende Firewall-Regeln umgesetzt und sichergestellt werden.
- Das vorgeschlagene Adressschema führt zu einer sehr kompakten und damit effizienten Firewall-Konfiguration. Im o. g. Beispiel werden externe Verbindungen nur zu Adressen im Bereich <ÖV-Präfix>:f/52 zugelassen.
    - Soll zwischen verschiedenen DMZ-Subnetztypen unterschieden werden, so können auch über das „f“-Subnetz hinaus weitere DMZ-Netze reserviert werden (vergl. Tabelle 5), beispielsweise 8, 9 und a – e. In diesem Fall würden 0 – 7 für interne Netze genutzt. In jedem Fall sollte die Anzahl der DMZ-Subnetztypen eine Zweierpotenz sein (1, 2, 4, oder 8).
    - Die Aufteilung der Ziffern für die Subnetztypen sollte den vorhandenen Anforderungen der konkreten ÖV angepasst sein.

- Dedizierte Adressbereiche für eine Adressumsetzung mit NAT (genauer: Source NAT = „Masquerading“) entfallen.
- Das beschriebene Vorgehen hat neben den vielen und überwiegenden Vorteilen auch Nachteile. Zum einen erleichtert ein strukturiertes Adresskonzept nicht nur dem Administrator die Orientierung, sondern auch möglichen Angreifern, zum anderen schränkt das Abbilden von ehemaligen IPv4-Subnetzen auf IPv6-Präfixe die Größe des Adressraums ein. Dies spricht aber nicht grundsätzlich gegen den Ansatz, da die Unkenntnis über Systemadressen keine „echte“ Sicherheit bietet und die IPv6 Adressbereiche so groß sind, dass sie, auch wenn der Bereich nicht vollständig genutzt wird, i. d. R. ausreichend sind.

*Im Allgemeinen gilt es bei der Schaffung eines IPv6-Adressschemas eine Umsetzung zu finden, die die neuen IPv6-Subnetze innerhalb einer ÖV gemäß ihrer Funktionen und vorhandener Richtlinien sinnvoll abbildet.*

*Es wird in diesem Zusammenhang dringend empfohlen, die „Checkliste Migrationsplanung“ im Anhang I ab Seite 150 sowie die IPv6-Leitlinie im Anhang II ab Seite 184 zu studieren.*

## 6.4. IPv6-Adressmanagementsysteme

Die um mehrere Zehnerpotenzen größere Anzahl an Adressen bei IPv6 und die deutlich längeren IP-Adressen haben den Nachteil, dass sich Menschen diese schlechter merken können und es auch deutlich mehr aktive Adressen geben wird. Um dennoch, auch zur Gewährleistung eines sicheren Betriebs und zur Dokumentation des Adressbereichs, den Überblick zu behalten, ist der Einsatz eines IP-Adressmanagement-Tools zu empfehlen (IPAM-Tool).

Die Adressvergabe wird damit nicht mehr von Hand durchgeführt, sondern Adressen werden aus einem zentralen Pool vergeben (Master-DHCP-Server) und über nachgelagerte DHCP/DNS-Server (Slave) zugewiesen. Die IPAM-Technologie wird gelegentlich auch als 'DNS, DHCP, IP-Adressmanagement' (DDI-Management) bezeichnet. Die Adressvergabe kann dabei statisch und/oder dynamisch erfolgen. Ein Einsatz in Kombination mit Zugangstechniken, wie 802.1X ist möglich, aber nicht zwingend notwendig.

Soll mittels IPAM eine Teilautomatisierung der Adresszuweisungen erreicht werden, so muss das gewählte IPAM-Tool mit dem DHCP- und DNS-Dienst integriert werden können. Hier bestehen zudem Abhängigkeiten zu den eingesetzten Betriebssystemen. Wie bei den sonstigen Netzdiensten ist die vollständige IPv6-Unterstützung eines IPAM-Tools zu prüfen.

Dieses Vorgehen verbindet die Vorteile eines zentralen Managements mit einer Lastverteilung auf mehrere Zugangsserver. Weiterhin erlaubt das Vorgehen, sich mit mobilen Endgeräten an beliebigen, kabelgebundenen Zugangspunkten an das Netz anzuschließen, sofern dies keine Sicherheitsregeln verbieten. Alle Aktivitäten der Adressvergabe werden protokolliert, so dass Adresszuweisungen jeder Art nachvollzogen werden können. Der Nachweis, wer wann wo mit dem

Netz verbunden war, kann geführt werden. Die Nachvollziehbarkeit wann bestimmte Sub-Netze oder Serveradressen neu zugewiesen wurden und von wem, ist z. B. für die Anforderungen des Standards ISO 27001 notwendig. Die folgende Abbildung zeigt beispielhaft das Prinzip einer solchen Infrastruktur.

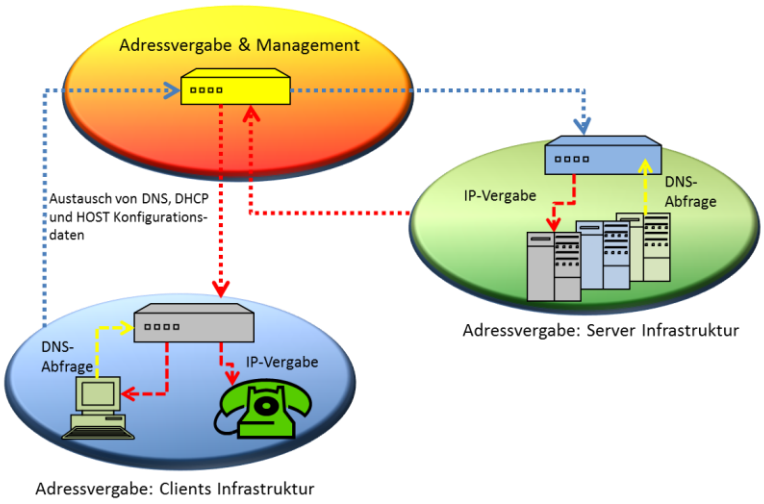


*Abbildung 16: Prinzipieller Aufbau einer IPAM-Lösung*

IPAM-Systeme schreiben in Logs mit, welche IP-Adresse zu welchem Zeitpunkt an welche MAC-Adresse vergeben wurde. Damit ist eine maschinenspezifische Zuordnung gegeben. Eine benutzerspezifische Erfassung lässt sich z. B. mit IEEE 802.1x realisieren. Zu beachten ist hierbei, dass es sich im Falle von Arbeitsplatzsystemen die einzelnen Personen zugeordnet sind, bei den entsprechenden IP-Adressen laut diverser Gerichtsentscheidungen um Personen bezogene Daten im Sinne des BDSG handelt.

Die LIR de.government passt aktuell (Stand: Januar 2012) das open source IPAM-Tool „netDot“ für den LIR-Betrieb an.

# 7. IPv4/IPv6-Übergangstechniken

Für die Umstellung von IT-Komponenten (Basisinfrastruktur, Netzwerke, Computer, Fachverfahren, Klientensoftware) von einer Umgebung, die ausschließlich IPv4 bietet, in eine Umgebung, die zusätzlich IPv6-Unterstützung bietet, gibt es mehrere mögliche Verfahren, die jeweils verschiedene Vor- und Nachteile haben. Auch lässt sich nicht jedes Verfahren bei jeder Geräteklasse[2] anwenden.

Dieses Kapitel gibt eine Übersicht über die möglichen Verfahren, zusammen mit Hinweisen, wo und wie diese sinnvoll angewendet werden können.

Für die allermeisten Anwendungsszenarien wird empfohlen, einen Ausbau und eine Konfiguration der vorhandenen Strukturen mit nativer IPv4/IPv6-Dual-Stack-Unterstützung zu realisieren. Wo dies nicht möglich ist (z. B. falls ein Internetprovider seinen Kunden noch kein IPv6 anbieten kann), so können für den IPv6-WAN-Anschluss ausgewählte Übergangstechniken, wie z. B. fest konfigurierte Tunnel zum Einsatz kommen.

Bei der Beschaffung von Netzdienstleistungen im und zum Internet muss bedacht werden, dass IPv6-Unterstützung relevant ist für interne Systeme und Dienste, für den WAN-Zugang, sowie für extern gehostete Systeme (z. B. in einem kommunalen Data Center). Internet-Zugangsanbieter und Server-Hosting-Anbieter stehen bereits unter dem Druck, nicht nur IPv6 auszurollen, sondern parallel auch IPv4-Adressen einzusparen. Deshalb werden diese Anbieter in ihren Angeboten verstärkt Übergangstechniken nutzen, die eine Ersparnis an verwendeten IPv4-Adressen zur Folge haben. Aktuell führen die Anbieter am Markt bereits Preisaufschläge für zusätzlich genutzte IPv4-Adressen ein.

Im Folgenden werden die möglichen Verfahren beschrieben, gruppiert in:

(a) Dual-Stack-Techniken

(b) Tunnelverfahren

(c) Verfahren zur Umsetzung zwischen IPv4- und IPv6-Netzwerken, sog. Protokollumsetzung (engl.: protocol translation)

(d) Weitere Verfahren, die im Bereich IP-Transport eine Rolle spielen

Einige grundlegende Verfahren, namentlich (a) Dual-Stack-Betrieb und (b) Kapselung von IPv6 Paketen in IPv4 mittels Punkt-zu-Punkt-Tunneln sind in [RFC4213] beschrieben.

**Dual-Stack-Betrieb** (vgl. Abschnitt 7.1.1) bedeutet, dass ein System (Host, Router, Firewall, etc.) IPv4 und IPv6 parallel und unabhängig voneinander unterstützt und dies sowohl gleichzeitig auf einer physikalischen und logischen Netzwerkschnittstelle als auch auf unterschiedlichen Schnittstellen. Alle verbreiteten Betriebssysteme für Arbeitsplatzrechner, Smartphones und Tablet-

[2] Siehe [IPV6_PROFILE] für eine Auflistung der Geräteklassen.

PCs unterstützen IPv6 und Dual-Stack aktuell bereits. Der Funktionsumfang bzgl. IPv6 unterscheidet sich jedoch noch deutlich. Bei Smartphones und Tablet-PCs z. B. wird IPv6 häufig nur auf der WiFi-Schnittstelle unterstützt und noch nicht auf der 3G-Funkschnittstelle (Stand Dezember 2011). Die IPv6-Unterstützung der Anwendungen hängt stark von der eingesetzten Version ab und muss im Einzelfall geprüft werden. Das konkrete Verhalten der Anwendungen in einer Dual-Stack-Umgebung hängt von der Kombination aus Netzwerk, Betriebssystem und Anwendung ab.

Bei **Tunnelverfahren** werden komplette IP-Datenpakete zum Transport als Nutzdaten (Payload) in andere Datenpakete verpackt und versendet. Üblicherweise erfolgt der Transport über UDP/IP, TCP/IP oder direkt in einem IP-Tunnel (IP-in-IP). Dabei kann die IP-Version der Tunnelpakete und der getunnelten Pakete verschieden sein. So können IPv4-only-Netze von IPv6-Paketen durchquert werden und umgekehrt. Optional können die getunnelten Pakete hierbei verschlüsselt werden. Da die Kopplung von IP-Netzen mittels IPsec im Tunnel-Mode schon unter IPv4 in der ÖV weit verbreitet ist, bietet sich hier die Nutzung des IPsec-Tunnel-Modus zur sicheren Übertragung von IPv4 in IPv6 und umgekehrt an.

Bei einer **Protokollumsetzung** auf Paketebene zwischen IPv4 und IPv6 werden hingegen die IPv4-Header durch neu generierte IPv6-Header ersetzt. Dies muss so geschehen, dass die so generierten IP-Pakete im Internet routbar sind und ggf. ein zweiter Protokollumsetzer wieder die originalen IPv4-Header regenerieren kann. Mit diesem Verfahren lassen sich IPv4-Pakete über IPv6-only-Netzwerke transportieren. Ebenso ist auch die umgekehrte Anwendung möglich, mit der IPv6-Pakete IPv4-only-Netzwerke passieren können. Eine Protokollumsetzung ermöglicht – im Gegensatz zu Tunneltechniken – auch die Kommunikation zwischen Endpunkten mit verschiedenen IP-Versionen, also z. B. zwischen einem IPv6-only-Host und einem IPv4-only-Server. Da bei vielen Anwendungsprotokollen die IP-Adressen nicht nur im Kopf der IP-Pakete sondern auch im Anwendungsprotokoll verwendet werden, funktioniert die Protokollumsetzung in der Praxis nur sehr eingeschränkt. Existierende Implementierungen gelten aktuell als wenig ausgereift.

Bei einer Umsetzung mittels eines klassischen **Proxy-Servers** werden die IP-Verbindungen am Proxy terminiert und „im Auftrag“ des Klienten durch den Proxy eine weitere IP-Verbindung zum eigentlichen Ziel der Datenkommunikation aufgebaut. Die Verbindung zwischen Klient und Proxy einerseits und dem Proxy und Zielsystem andererseits kann dabei über IP-Datenströme mit verschiedener IP-Version erfolgen. Je nach verwendeter Proxy-Software sind alle Kombinationen möglich (4-4, 6-6, 4-6, 6-4). Voraussetzung ist jedoch, dass das verwendete Applikationsprotokoll (z. B. http) auch über einen Proxy genutzt werden kann.

Das Kapitel 7 schließt mit einem Überblick der Techniken und Empfehlungen zu deren Nutzung ab, sowie einem Ausblick auf mögliche zukünftige IPv6-only-Netzwerke.

## 7.1. Dual-Stack-Techniken

Als Dual-Stack wird die Technik bezeichnet, bei der auf den Komponenten, die an der IP-Kommunikation beteiligt sind, die IPv4- und IPv6-Unterstützung gleichzeitig aktiv ist. Dies betrifft dabei die Software dieser Komponenten, welche das Internet Protokoll *spricht*, den sogenannten „IP-Stack“.

Dual-Stack kann in unterschiedlichen Varianten eingesetzt werden, insbesondere durch Zugangsanbieter (Internet Service Providers (ISP)), um in der einen oder anderen Art IPv4-Adressen einzusparen. Dual-Stack bedeutet, dass der Kunde über seinen ISP IPv4 und IPv6 parallel nutzen kann. Es bedeutet aber nicht zwangsläufig, das beide Protokolle nativ vom Provider bereit gestellt werden. Der Trend, bei neuen Endkunden-Anschlüssen natives IPv6 zusammen mit IPv4 über Tunnel-Techniken zu schalten, kann jedoch im Vergleich zu nativem IPv4/IPv6 funktionelle Nachteile für den Endkunden bedeuten.

### 7.1.1 Dual-Stack mit nativem IPv4/IPv6

**Struktur:**

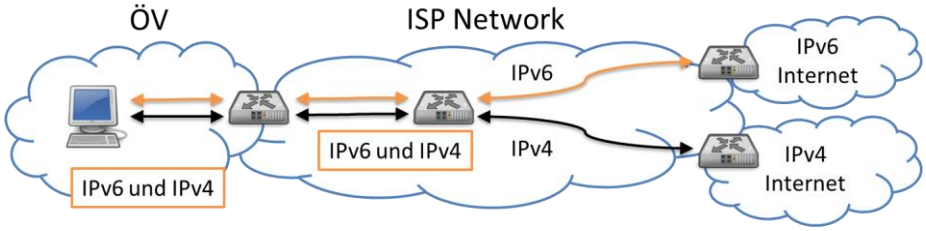


*Abbildung 17: Dual-Stack-Verfahren*

**Details:**

Nativer Dual-Stack-Betrieb bedeutet einen parallelen Betrieb von IPv4 und IPv6. Für einen solchen Dual-Stack-Betrieb - ohne Nutzung von Tunneln - ist es notwendig, für alle an einer Verbindung beteiligten Systeme auch IPv6-Unterstützung bereit zu stellen. Dabei sind für ein Fachverfahren potentiell viele Geräte und Komponenten der Infrastruktur involviert: Router, Switches, Klienten und Server, Firewalls, Infrastrukturdienste (z. B. DNS-Server), sowie Betriebssysteme und Anwendungssoftware.

In manchen Standards wird Dual-Stack auch als Dual-IP bezeichnet.

Für den Dual-Stack-Betrieb auf dem Pfad zwischen Fachanwendung und deren Nutzern ist es notwendig die IT-Infrastruktur auf der IP-Ebene (OSI-Layer 3) für IPv4 und zusätzlich für IPv6 zu betreiben. Dies bedeutet, dass vorhandene Funktionen aus den IPv4-Netzwerken auch für IPv6 verfügbar sein müssen, unter anderem:

- IP-Adressen und IP-Adressvergabe
- IP-Paketweiterleitung (engl.: packet forwarding)

- IP-Routing-Protokolle
- IP-Paketfilter (firewalls)
- Anwendungsspezifische Gateways (application-level gateway – ALGW)
- Eine Ausnahme bilden ggf. vorhandene, transparente IPv6-über-IPv4-Tunnel, durch welche eine Fachanwendung über IPv6 mit ihren Nutzern kommunizieren kann, auch wenn Teilnetze zwischen beiden nur IPv4 beherrschen.

Eine Umstellung hin zu einem Dual-Stack-Betrieb erfordert bei existierenden Netzwerken ein wohlgeplantes Vorgehen, um vorhandene Funktionalitäten nicht zu kompromittieren. Da es Abhängigkeiten gibt, ist auch die Reihenfolge der Migration der verschiedenen o. g. Systeme zu beachten. Details dazu sind in Abschnitt 5.1 sowie in Anhang I: IPv6-Migrations-Checklisten dokumentiert.

Einen detaillierten technischen Überblick zum IPv4/IPv6-Dual-Stack-Betrieb und die Transitionstechniken gibt RFC4852: „IPv6 Enterprise Network Analysis IP Layer 3“ [RFC4852]. In diesem Dokument wird auch ausführlich auf die verschiedenen Ausgangssituationen eingegangen und die Notwendigkeit eines abgestuften Plans zur Einführung von IPv6 motiviert.

### 7.1.2 Nutzung von VLANs zum parallelen Betrieb von IPv4 und IPv6 im Intranet

Mit dieser Übergangstechnik kann der IPv6-Datenverkehr über eigene VLANs verteilt werden, separiert von den bereits bestehenden und vom IPv4-Datenverkehr genutzten VLANs. Voraussetzung dafür ist, dass bestimmte VLAN-Funktionen nach IEEE 802.1Q von allen betroffenen Geräten unterstützt werden.

Die Technik wird in [RFC4554] „Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks“ beschrieben. Sie basiert darauf, IPv6-Datenverkehr im Intranet über Layer-2-VLANs zu verteilen. Die nach [RFC4554] konfigurierten Switches spannen hierfür ein VLAN-basiertes IPv6-Overlay über die Netzwerkverbindungen der existierenden IPv4-LANs auf. Dies ist in der folgenden Abbildung skizziert:

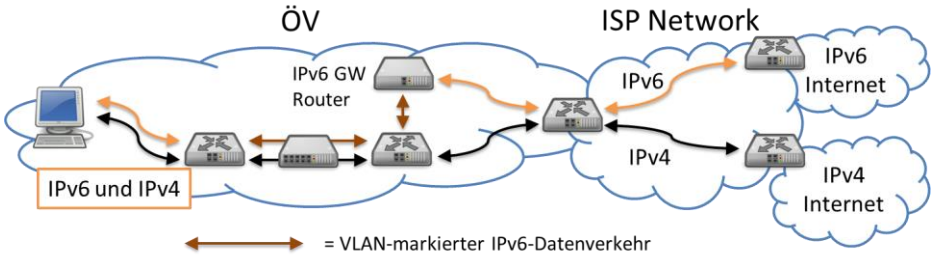


*Abbildung 18: IPv6 über VLANs im Intranet*

Eine Modernisierung auf Dual-Stack-fähige Router, Switches und Security-Devices sollte dieser Technik jedoch im Allgemeinen vorgezogen werden. Die bei dieser Technik unterschiedliche Verarbeitung und Wegeführung der beiden IP-

Versionen führt zu einem Risiko von stark unterschiedlichen Laufzeiten und sehr komplexen Fehlerbildern, wenn eines der beiden Protokolle ausfällt.

Bei einem Design nach [RFC5445] müssen die betroffenen Router und Switches kein IPv6 bzw. Dual Stack unterstützen. Lediglich die Endgeräte (Hosts, Server) müssen Dual-Stack-Unterstützung bieten, und ein IPv6-Gateway zum Internet sowie dessen vorgeschaltete Security-Devices müssen IPv6 unterstützen (bei nativem IPv6-Internetzugang) bzw. Dual-Stack, falls der IPv6-Internetzugang über einen Tunnelmechanismus wie 6to4 realisiert ist.

Für Hosts werden für IPv4 und IPv6 aufgrund der logischen Teilung in IPv4- und IPv6-Netze („Layer2-VLAN-Overlay“) verschiedene Default-Routen in die Infrastruktur existieren.

Bei Verwendung von Switches, welche *Protokoll-basiertes* VLAN-Tagging unterstützen, muss auf den Endsystemen (Hosts/Router) kein VLAN-Tagging unterstützt werden, da der von einem Endsystem genutzte Switch die IPv6-Datenpakete in das korrekte VLAN zuordnen kann.

Die Technik nach [RFC4554] bietet sich dort an, wo auf vorhandener, nicht IPv6-tauglicher Infrastruktur ohne ein Upgrade ein IPv6-Netz aufgespannt werden soll, z. B. falls in einer ÖV für die Nutzung von neuen, IPv6-fähigen IP-Telefonie-Geräten aus Gründen der Verkehrsseparierung ein komplett getrenntes IPv6-Netzwerk aufgespannt werden soll.

Diese Übergangstechnik ist nicht notwendig, wenn die IPv6- und die IPv4-Netzwerke auf kongruente VLANs abgebildet werden, also wenn es keine Topologieunterschiede zwischen IPv4-Netz und IPv6-Netz gibt.

### 7.1.3 Dual-Stack zusammen mit anderen Verfahren

Die Mehrzahl der im Weiteren genannten Verfahren bilden am Zugangspunkt einer ÖV den IPv6-WAN-Zugang ab. Dies bedeutet, dass aus Sicht eines Klienten im Intranet ein IPv6-Zugang ins Internet oder zu externen Fachverfahren verfügbar ist, ohne dass der Host selbst das genutzte Verfahren am WAN-Zugang (z. B. IPv6 über Tunnel-Broker) kennen muss. Daraus folgt, dass auch bei Übergangsverfahren, die am dem WAN-Zugang Tunneltechniken nutzen, innerhalb einer ÖV die Klienten für die Nutzung von IPv4 und IPv6 nur normale Dual-Stack-Unterstützung benötigen. Bei späterer Verfügbarkeit von nativem IPv6 am WAN-Anschluss kann dann die schon vorhandene IPv4/IPv6-Dual-Stack Infrastruktur im Intranet nahtlos weiter genutzt werden.

## 7.2. Tunneltechniken

### 7.2.1 6to4

**Struktur:**

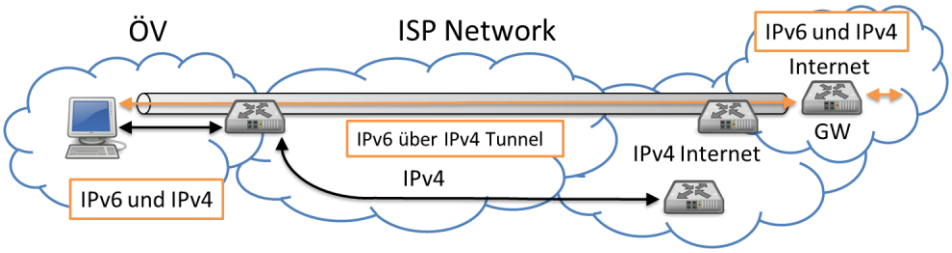


*Abbildung 19: Verfahren 6to4*

**Details:**

Bei 6to4 handelt es sich um einen automatischen Tunnelmechanismus inklusive eines Adresszuordnungsverfahrens, bei dem IPv6-Pakete in IPv4-Paketen getunnelt werden. Dadurch können IPv6-only-Klienten über IPv4-only-Netze hinweg miteinander und mit anderen Hosts im Internet kommunizieren. 6to4 ist in [RFC3056], [RFC3068] und [RFC5158] beschrieben.

Über 6to4 findet keine Übersetzung, bzw. Zuweisung von IPv6-Adressen zu IPv4-Adressen statt, sondern es stellt einen automatischen Tunnelmechanismus zur Verfügung, der es ermöglicht, dass IPv6-Hosts miteinander kommunizieren. Ferner kann in solch einem Netzwerk über Relay-Router der Datenverkehr in IPv6-only Netze weitergeleitet werden.

Bei 6to4 kann unterschieden werden zwischen einem einzelnen Host, der den Tunnelmechanismus verwendet, und einem Netzwerk, bei dem ein Gateway-Router die Umsetzung für das dahinterliegende Netzwerk übernimmt. Sowohl der Router als auch der Host brauchen eine globale erreichbare IPv4-Adresse (ohne Verwendung von NAT). Diese global erreichbare IPv4-Addresse wird in der Regel eine öffentlich erreichbare IPv4-Adresse sein, da davon ausgegangen werden kann, dass es sich bei dem IPv4-Netz über das kommuniziert werden muss, um das Internet handelt. Sollte es sich nicht um das Internet handeln, muss es sich um eine global erreichbare IPv4-Adresse aus dem jeweiligen IPv4-Netz handeln.

Der 6to4-Tunnelmechanismus führt folgende drei Funktionen aus:

- Zuweisung eines IPv6/48-Adressblocks als 6to4-Präfix zu jedem Host oder Netzwerk, die eine global erreichbare IPv4-Adresse haben. Dabei setzt sich der 6to4-Adressblock aus dem Präfix 2002::/16 und der global erreichbaren IPv4-Adresse in hexadezimaler Darstellung zusammen.
- Einbetten der IPv6-Pakete in IPv4-Pakete, so dass diese über ein IPv4-Netzwerk geroutet werden können. Dabei wird der 6in4-Mechanismus verwendet.

- Routen von Datenverkehr zwischen 6to4-Netzen und nativen IPv6-Netzen über sogenannte Relay Server.

Die folgenden Komponenten sind im Zusammenhang mit 6to4 relevant:

- 6to4-Host: Ein 6to4-Host hat mindestens eine 6to4-Adresse zugewiesen bekommen.
- 6to4-Router: Hierbei handelt es sich um einen regulären IPv6-Router, der die Verwendung einer 6to4-Tunnelschnittstelle unterstützt und der in der Regel zur Weiterleitung von Datenverkehr zwischen den 6to4-Hosts des Standortes, zu anderen 6to4-Routern und zu einem Relay-Router dient.
- Relay-Router: Ein Relay-Router ermöglicht die Weiterleitung von 6to4-Adressen zu nativen IPv6-only-Hosts, z. B. solchen im IPv6-only Internet.

Bei einer Kommunikation zwischen zwei Standorten, welche beide IPv6 via 6to4 in ihren Netzen unterstützen, müsste am Perimeter ein 6to4-Router mit einer global erreichbaren IPv4-Adresse eingesetzt werden. Dieser ist verantwortlich für die Weiterleitung von Datenverkehr zwischen den 6to4-Hosts der beiden Standorte.

Die folgende Abbildung zeigt den 6to4-Tunnelmechanismus zwischen zwei Standorten, inklusive der beteiligten Komponenten:

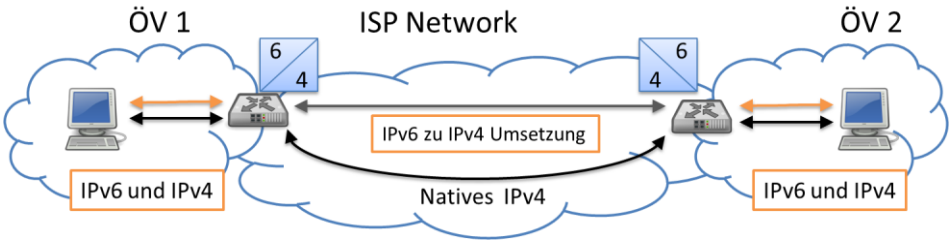


*Abbildung 20: 6to4 Kommunikation zwischen zwei Standorten*

Problematisch bei der Verwendung von 6to4 ist die Tatsache, dass aufgrund der offenen Architektur die 6to4-Komponenten in IPv4 eingebettete IPv6-Pakete von allen IPv6-Adressen empfangen können. Aus diesem Grund ist z. B. ein IP-Spoofing relativ einfach durchzuführen. In [RFC3964] sind Sicherheitshinweise zum Betrieb der 6to4-Komponenten dargestellt.

In der ÖV wird u.a. deshalb eine Tunnelung von IPv6 in IPv4 mittels IPsec Tunnel-Mode i. d. R. bevorzugt verwendet.

### 7.2.2 IPv6 Rapid Dployment (6rd)

**Struktur:**

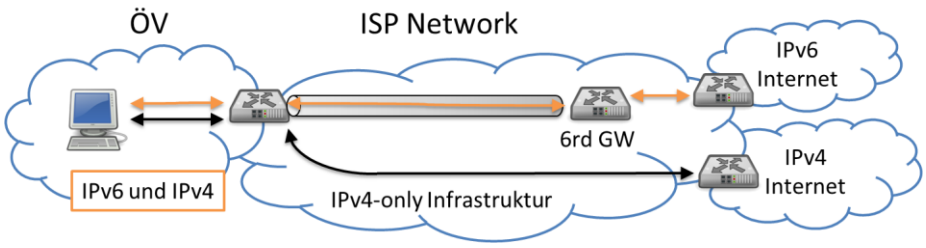


*Abbildung 21: IPv6 Rapid Deployment (6rd)*

**Details:**

6rd [RFC5969] ist ein im August 2010 vorgeschlagener Standard, welcher ein schnelleres Ausrollen von IPv6 für Kunden von Internet Service Providern (ISP) ermöglichen kann. 6rd basiert auf 6to4 [RFC3056], unterscheidet sich jedoch von diesem durch Nutzung eines IPv6-Präfixes des Providers an Stelle des allgemeinen Präfixes 2002::/16 bei 6to4. 6rd bietet eine IPv6-Verbindung zwischen einem Zugangspunkt des Kunden und dem Internet über IPv4-Netzwerke des Providers, ohne die Notwendigkeit expliziter IPv6-über-IPv4-Tunnel.

6rd basiert auf einer algorithmischen Abbildung zwischen dem IPv6-Adressraum eines ISPs und den ihm zugewiesenen IPv4-Adressen. Diese Zuordnung bestimmt auch den 6rd-Gateway. Über diesen wird der IPv6-Datenverkehr der Kunden aus dem IPv4-basierten Providernetzwerk an das IPv6-Internet weiter geleitet. Da die algorithmische Adressumsetzung ohne zusätzliche Statusinformationen (stateless) erfolgen kann, stellen 6rd-Gateways keine Begrenzung bezüglich der erreichbaren Performance dar.

Für 6rd benötigt der ISP eine Menge von 6rd-Gateways zum Internet (6rd Border Relays, BRs) und der Kunde ein Gateway (Customer Edge Router, CE-Router), welches nach innen IPv6-fähig ist und nach außen (zum ISP hin) 6rd unterstützt.

Für die Kunden des 6rd-Providers ist der mit 6rd nutzbare IPv6-Service äquivalent nutzbar zu nativem IPv6. Dies ist auch der Fall für 6to4, jedoch ist bei 6rd eine bessere Qualitätssicherung als bei 6to4 der Fall, da hierbei alle Gateways unter Kontrolle des 6rd-Providers sind. Ferner kann 6rd parallel mit 6to4 genutzt werden, falls dies gewünscht wird.

6rd ist eine empfehlenswerte Technologie für den Übergang von IPv4 zu IPv4/IPv6-Dual-Stack-Betrieb in Providernetzwerken, da es (a) mit Ausbringung einiger 6rd-Gateways über bereits vorhandene IPv4-Providernetzwerke verwendet werden kann und (b) parallel zum Ausbau einer nativen IPv6-Unterstützung aktiv bleiben kann. Wenn ein 6rd-Provider letztendlich auch natives IPv6 komplett unterstützt, kann er 6rd abschließend in seinem Netzwerk deaktivieren.

### 7.2.3 Dual-Stack-Lite (DS-Lite)

**Struktur:**

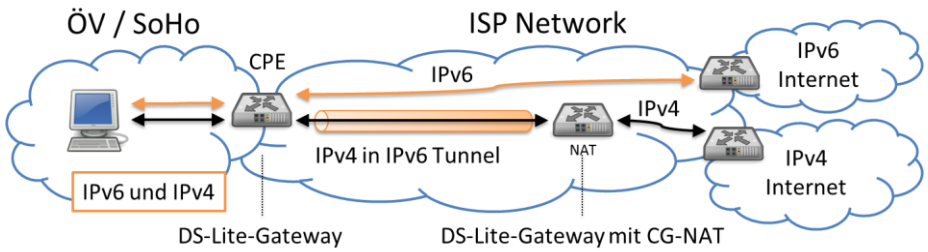


*Abbildung 22: Dual Stack Lite*

**Details:**

Dual-Stack-Lite [RFC6333] ist ein vorgeschlagener IETF Standard der es einem ISP, seine Kunden über einen Tunnel den IPv4-Zugang zum Internet anzubieten, für den Fall, dass der Provider seinen (Neu-)Kunden am Zugangspunkt des ÖV-Gateways (GW) bzw. des Heim-Gateways (Customer Premises Equipment, CPE) nativ nur einen IPv6-only Zugang zum Internet anbietet.

Dazu müssen das Gateway und der Provider DS-Lite unterstützen. Ist dies der Fall, so können Rechner im lokalen Netzwerk, welche Dual-Stack unterstützen, das IPv4- und IPv6-Internet nutzen, als wäre IPv4- und IPv6-Unterstützung nativ vom Provider verfügbar.

Bei DS-Lite wird zur Einsparung von IPv4-Adressen auf Providerseite zusätzlich ein Carrier Grade NAT (CG-NAT) auf der IPv4-Adresse genutzt, die über den DS-Lite-Tunnel zur Verfügung gestellt wird. Dies bedeutet für DS-Lite, dass auch dieselben Nachteile für den Nutzer bezüglich des IPv4-Datenverkehrs entstehen, wie bei Nutzung von CG-NAT allein (ohne DS-Lite und IPv6). Der IPv6-Zugang bei DS-Lite ist jedoch vollwertig, da dem CPE des Kunden ein natives IPv6-Subnetz zugeteilt wird.

Diese Technologie wird von einigen Kabelnetzprovidern geplant, um kurzfristig IPv4 Adressen einzusparen.

### 7.2.4 Teredo

**Struktur:**

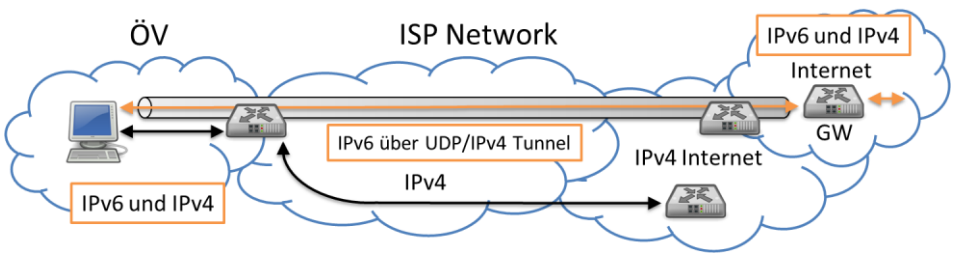


*Abbildung 23: Teredo-Verfahren*

**Details:**

Das Teredo-Protokoll ist eine Übergangstechnik, mit der Hosts in einem IPv4-LAN Zugriff zum IPv6-Internet erlangen können. Voraussetzung ist eine Teredo-Implementierung, sowie IPv6-Unterstützung auf dem Host selbst.

Bei Teredo wird vom Host selbst ein IPv6-über-UDP/IPv4-Tunnel aufgebaut. Einen Tunnelendpunkt bildet der Host selbst, den anderen Tunnelendpunkt bildet ein „Teredo-Relay“ genanntes Gateway, welches Zugang zum nativen IPv6-Internet besitzt. Für den Host ist der so verfügbare IPv6-Service äquivalent zu einem nativen IPv6-Zugang.

Ein großer Vorteil von Teredo ist, dass es auch für Hosts hinter einem NAT-Gateway einen vollwertigen IPv6-Zugang zum Internet ermöglicht. Dies ist auch bei Nutzung von Teredo über Carrier Grade NAT der Fall. Lediglich durch symmetrische NATs funktioniert es nicht[3].

Der große Nachteil von Teredo ist, dass es durch den Aufbau eines Tunnels effektiv vorhandene Paketfilter und Schutzmaßnahmen auf IP-Ebene umgeht. Ein Host mit aktivem Teredo ist auf IPv6 Ebene nicht mehr durch vorhandene IPv4-Paketfilter (z. B. Firewall) geschützt.

Die Nutzung von Teredo wird daher aus Sicherheitsgründen für die ÖV nicht empfohlen. Insbesondere sollten auch bei vorhandenen Systemen (speziell Windows) die Teredo-Funktionen explizit abgeschaltet werden bzw. Teredo am Firewall einer ÖV durch Blockierung von UDP-Port 3544 für ausgehenden IPv4/UDP Verkehr gesperrt werden.

### 7.2.5 Intra-Site Automatic Tunnel Addressing Protocol

**Struktur:**

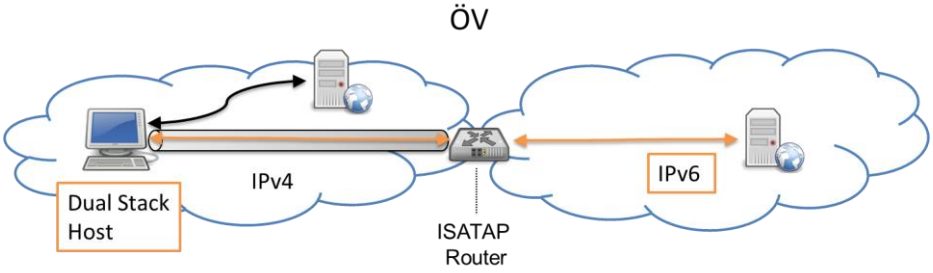


*Abbildung 24: ISATAP Verfahren*

**Details:**

Das Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) ist ein von Microsoft und Cisco im Oktober 2005 vorgeschlagener Standard [RFC4214], der im März 2008 durch den Standard [RFC5214] abgelöst worden ist. Eine

[3] siehe [RFC5389] für die verschiedenen Typen von NATs.

Erweiterung des Standards ist beschrieben in [RFC5579] „Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) Interfaces“.

Bei ISATAP handelt es sich wie bei 6to4 um einen Tunnelmechanismus, der nur mit Dual-Stack-Unterstützung funktioniert und bei dem Dual-Stack Nodes (Hosts und Router) über ein IPv4-only Netz miteinander verbunden werden können. Dies bedeutet, dass Dual-Stack-Nodes ISATAP verwenden um IPv6-Pakete in IPv4-Paketen zu tunneln. Im Gegensatz zu 6to4 wird bei ISATAP kein Multicast verwendet, sondern das IPv4-only Netz wird als ein virtuelles „Non-broadcast Multiple-Access Netzwerk“ (NBMA) verwendet. Der Vorteil, der sich hieraus im Gegenzug zu 6to4 ergibt, ist, dass ISATAP nicht auf Multicast-Unterstützung im zugrunde liegenden IPv4-only-Netz angewiesen ist.

Bei ISATAP werden Link-Local-IPv6-Adressen von einer IPv4-Adresse abgeleitet. Zusätzlich gibt es einen Mechanismus der Neighbor-Discovery über IPv4 ermöglicht.

Eine Link-Local-Adresse wird dadurch erstellt, dass die 32-bit IPv4-Adresse an das 96-bit Präfix fe80::5efe: angehängt wird. Das heißt beispielsweise für die IPv4-Adresse 192.168.0.2, dass folgende IPv6-Adresse entsteht: fe80::5efe:192.168.0.2 . In der Hexadezimaldarstellung sieht diese Adresse dann folgendermaßen aus: fe80::5efe:c0a8:0002 (c0a8:0002 ist 192.168.0.2 in der Hexadezimaldarstellung).

Da ISATAP IPv4 als nicht Multicast-fähigen Link Layer benutzt, kann ICMPv6-Neighbor-Discovery nicht auf dem Standardweg durchgeführt werden. Die Link-Layer-Adresse bei ISATAP besteht nicht aus einer MAC-Adresse sondern aus der 32-Bit-IPv4-Adresse die dem 96-bit-Präfix angehängt wird, d. h. die Zuordnung zum Link-Layer geschieht über die IPv4-Adresse, daher kann Neighbor-Discovery nicht verwendet werden. Das Problem, dass sich in diesem Zusammenhang ergibt, ist, dass eine automatische Router Discovery ohne die Verwendung von Multicast nicht möglich bzw. wesentlich schwieriger ist. Aus diesem Grund muss jeder ISATAP-Host mit einer potenziellen Router Liste (engl.: Potential Router List (PRL)) konfiguriert werden. Bei der Kommunikation unter ISATAP wird zuerst über ICMPv6-Router-Discovery-Nachrichten geprüft, ob die in der PRL enthaltenen Router aktiv sind. Diese stellen dann die Liste der on-Link IPv6 Präfixe zur Verfügung die dazu benutzt wird um globale IPv6-Adressen zu erstellen. In der Regel wird die PRL über die Abfrage eines DNS Servers bereitgestellt, z. B. isatap.bund.de.

Bei der ISATAP-Kommunikation zwischen zwei IPv4-only-Netzen, die beide IPv6 an ihrem Perimeter unterstützen, würde am Perimeter je ein ISATAP-Router mit einer global erreichbaren IPv4-Adresse eingesetzt werden. Diese beiden Router sind verantwortlich für die Weiterleitung von Datenverkehr zwischen den ISATAP-Nodes der beiden Standorte.

Die folgende Abbildung stellt die Kommunikation von ISATAP zwischen zwei ÖVs dar.

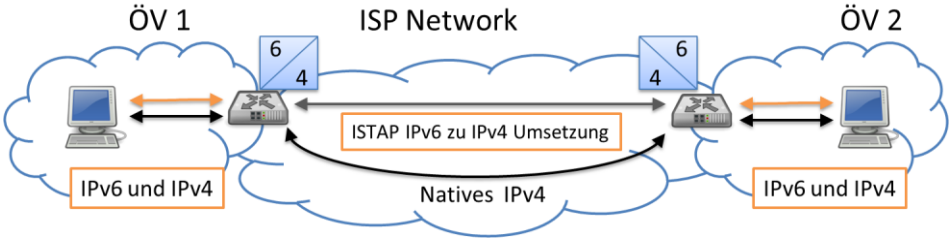


*Abbildung 25: Kommunikation über ISATAP zwischen zwei ÖVs*

Ein wesentlicher Nachteil von ISATAP ist, dass es die gleichen Sicherheitsrisiken wie 6to4 beinhaltet. Wie bei 6to4 muss der virtuelle IPv4-only Link am Perimeter so weit gesichert werden, dass es nicht möglich ist, dass externe IPv4-only-Nodes vorgeben können, Teil des ISATAP-Links zu sein. Dies wird in der Regel dadurch erreicht, dass an der Firewall das Protokoll 41 geblockt wird. Zusätzlich versucht ISATAP, den unqualifizierten DNS-Namen „isatap“ aufzulösen und baut dann, wenn es als Antwort eine IPv4-Adresse erhält, einen Tunnel auf.

### 7.2.6 4to6

Die 4to6-Technik kann dazu benutzt werden, um IPv4 Datenverkehr über IPv6-only-Netzwerke zu transportieren. Hierfür ist es, ebenso wie bei 6to4, möglich, eine Adressumsetzung vorzunehmen, ohne vorab einen expliziten Tunnel aufbauen zu müssen. In Fall von 4to6 werden dabei die IPv4-Adressen der Endpunkte in routbare IPv6-Adressen eingebettet, welche dann zum Transport über die IPv6-only-Netzwerke verwendet würden.

Diese Technik ist zurzeit noch nicht standardisiert, da es noch keinen praktischen Bedarf gibt. Die 4to6-Technik kann in Zukunft relevant werden, wenn es die ersten *IPv6-only*-Internetprovider geben wird, und deren Kunden auch bereits vorhandene IPv4-only-Dienste über das Internet nutzen möchten.

*Hinweis*: Gelegentlich wird im Internet die Bezeichnung „4to6“ auch als Bezeichnung für den Tunnelendpunkt eines 6to4 Tunnels benutzt. Der Term „4to6“ sollte in diesem Zusammenhang *nicht* verwendet werden, da es sich um eine andere Technik handelt. Korrekt ist hierfür Tunnelendpunkt oder Tunnel-Broker (aus dem Englischen).

### 7.2.7 MPLS (L2/6PE/6VPE)

MPLS – Multi-Protocol Label Switching – ist ein Mechanismus, um Datenpakete in Netzwerken zu transportieren. MPLS nutzt zur Adressierung 20 Bit lange Labels zur Identifikation von Datenströmen („virtual paths“). Es und ist damit effizienter bei der Paketweiterleitung (packet forwarding) und leichter zu implementieren, als Protokolle, die mit längeren Adressen arbeiten.

MPLS bietet ein verbindungsorientiertes Verkehrsverhalten für Datenpakete. Dies bedeutet, dass ein MPLS-Pfad vor seiner Nutzung zuerst durch Konfiguration der beteiligten MPLS-Router aufgebaut werden muss. Die Technik ist unabhängig vom Datenprotokoll der transportierten Pakete und kann so IPv4, IPv6, ATM, SONET, Ethernet und andere Datenpakete transportieren. MPLS wird oft als ein

Layer-2,5-Protokoll bezeichnet und wird auf Grund der genannten Eigenschaften häufig in den Hochgeschwindigkeitsnetzen von Internetprovidern genutzt, jedoch nur innerhalb administrativer Domänen, da aufgrund der 20-Bit-Labels keine globale Adressierung möglich ist.

MPLS wird in der Praxis in verschiedenen Varianten zur Netzkopplung verwendet:

- L2 - Layer-2 MPLS
- 6PE - Provider Edge MPLS [RFC4798]
- 6VPE - VPN Provider Edge MPLS [RFC4659]

Für 6PE und 6VPE werden über das Border Gateway Protokoll (BGP) Routing-Informationen zu den angeschlossenen Netzen ausgetauscht (IPv6-Präfixe und Label für 6PE; VPNv6-Präfixe für 6VPE). In beiden Fällen kann der MPLS-Backbone selbst auch IPv4-basiert arbeiten. Für Details siehe zum Beispiel in [6PE_6VPE].

Für den Einsatz von MPLS zum Transport von IPv6-Datenpaketen ist es notwendig, dass (i) die Übergabepunkte zum/vom MPLS-Netzwerk[4] IPv6-fähig sind, dass (ii) die MPLS-Frames eine genügend große Paketgröße (Maximum Transmission Unit, MTU) erlauben – bei IPv6 mindestens 1280 Bytes – und (iii) an den Übergabepunkten die IPv6-Path-MTU-Discovery korrekt unterstützt wird.

*Im praktischen MPLS-Einsatz für ÖV-Datenverkehr muss die unterstützte MTU sogar größer als 1280 Bytes sein, um verschlüsselten IPv6-Verkehr (z. B. mit IPsec) transportieren zu können.*

Eine größere MTU kann außerdem die Anzahl der notwendigen Datenpakete verringern und damit die Effizient der Leitungsausnutzung erhöhen.

### 7.2.8 SSL/TLS, GRE, IPSEC, PPP/PPTP

Verschiedene andere – nicht IPv6-spezifische – Tunneltechniken werden eingesetzt, um Datenströme über Datennetze wie das Internet zu transportieren, darunter:

- Secure Sockets Layer (SSL) [RFC6101],
- Transport Layer Security (TLS) [RFC 5246],
- Generic Routing Encapsulation (GRE) [RFC2784],
- Internet Protocol Security (IPsec) [RFC4301] und das
- Point-to-Point (Tunneling) Protokoll (PP(T)P) [RFC1661], [RFC2637].

[4] Genauer: customer edge (CE) *und* provider edge (PE) müssen IPv6-fähig sein, da der Einstiegspunkt zum MPLS-Netzwerk auf Provider-Seite liegt.

Diese Protokolle dienen verschiedenen Zwecken, wie Sicherheit, Transport-Enkapsulierung und dem Zugang zu IP-Netzen (PPP/PPTP). Ihnen allen gemein ist, dass sie – eine korrekte Konfiguration vorausgesetzt – zum Transport von IPv6-Datenpaketen eingesetzt werden können. Hierfür ist eine IPv6-Unterstützung in den Geräten notwendig, die die Tunnelendpunkte bereitstellen. Ferner muss das eingesetzte Tunnelprotokoll auf diesen Geräten die Übertragung von IPv6-Paketen mit einer Mindestgröße von 1280 Bytes unterstützen.

## 7.3. Protokollumsetzung zwischen IPv4 und IPv6 Netzwerken

### 7.3.1 NAT64 / DNS64

NAT64 ([RFC6052], [RFC6146]) ist ein Mechanismus, der es IPv6-only-Klienten ermöglicht, mit IPv4-Servern zu kommunizieren. Dabei bildet der NAT64-Server einen Kommunikationsendpunkt mit mindestens einer IPv4-Adresse, und bildet den Übergang zu einem /96 IPv6-Subnetz. Der NAT64-Server arbeitet hierbei als Gateway-Router zwischen IPv6 und IPv4.

Der IPv6-Klient, der zu einem IPv4-Server kommunizieren will, baut die IPv4-Adresse des Servers dazu in eine IPv6-Adresse ein und sendet Datenpakete für den IPv4-Server an die resultierende IPv6-Adresse. Der NAT64-Server erstellt daraus automatisch ein lokales Adress-Mapping und kann die Datenpakete über seine IPv4-Schnittstelle an den gewünschten IPv4-Server weiter leiten. In der umgekehrten Richtung muss der NAT64-Server mit Hilfe des Mappings IPv4-Pakete wieder in IPv6-Pakete für den Klienten konvertieren.

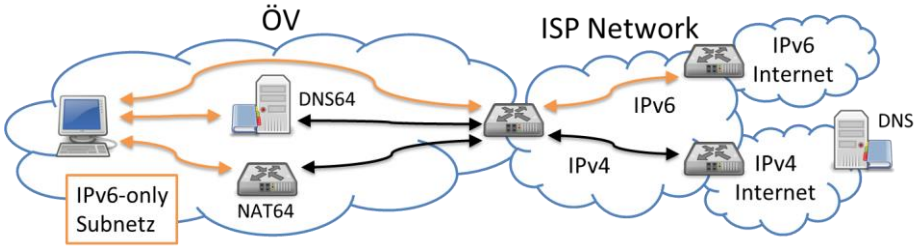


*Abbildung 26: NAT64 / DNS64*

Zusammen mit dem NAT64-Server wird üblicherweise ein DNS64-Server [RFC6147] eingesetzt. Dieser leitet für DNS-Anfragen, die nur einen A-Record (für IPv4) zurück liefern, automatisch einen AAAA-Record (mit einer IPv6-Adresse) ab. Der erste Teil (96 Bits) dieser abgeleiteten IPv6-Adresse zeigt üblicherweise auf den NAT64-Server, und die unteren 32 Bits beinhalten die per DNS gewonnene IPv4-Adresse.

Beim Einsatz von NAT64 und DNS64 sind folgende Punkte zu berücksichtigen:

(i) Anwendungen/Protokolle, welche numerische IPv4-Adressen verwenden,

(ii) Zugriff auf DNSSEC-gesicherte Domains und

(iii) NAT64 erlaubt wie auch andere NAT-Systeme keine Verbindungen von außen *zu* den (IPv6-only-)Klienten.

### 7.3.2 Proxy / ALG

Ein Proxy oder „Application Level Gateway“ wird oft zwischen internen Netzen (Intranet) und dem WAN-Zugang einer Institution verwendet (vgl. auch Abbildung 4 auf Seite 24). Existiert für ein Anwendungsprotokoll ein Proxy, wird die Verbindung eines Klienten zu einem externen Server unterbrochen und der Proxy kontaktiert den externen Server „in Vertretung“ der Klienten. Somit besteht die Möglichkeit der Überwachung des jeweiligen Anwendungsprotokolls, für welches ein Proxy existiert. Da der Proxy die Verbindung terminiert, besteht somit an dieser Stelle vollständige Kontrolle über den Datenstrom. Somit können hier umfangreiche Sicherheits- und Datenschutzfunktionen implementiert werden.

Der Einsatz von Proxies ist auch in gemischten Umgebungen sinnvoll: Arbeitet z. B. ein http-Proxy-Server auf der WAN-Seite im IPv4/IPv6-Dual-Stack-Betrieb, so kann darüber ein IPv4-only-Klient aus dem internen Netz auch externe IPv6-Webseiten abrufen, da der Proxy auf beiden Seiten verschiedene IP-Protokolle zur Kommunikation nutzen kann.

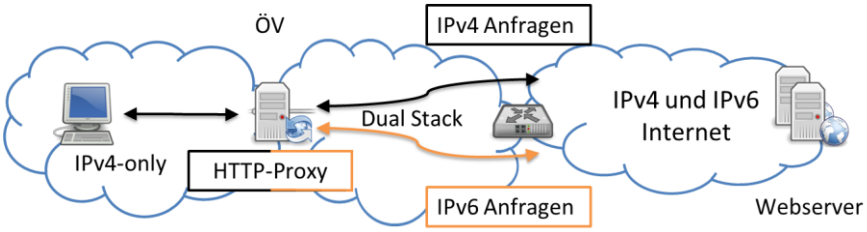


*Abbildung 27: http-Proxy*

In der öffentlichen Verwaltung findet man Proxies und ALGs oft als Teil der Standard-PAP-Netzarchitektur (packet filter – ALG – packet filter), wie sie in [ISi-LANA] beschrieben ist.

### 7.3.3 HTTP(S) Reverse Proxy

Für den Betrieb eines IPv4-only-Webservers oder einer web-basierten Anwendung, welche über das http-Protokoll (bzw. https) angesprochen wird, gibt es die Möglichkeit, diesen Webserver ohne Modifikation, nur mit Hilfe eines Vorgeschalteten Proxy-Servers im IPv6-Internet sichtbar zu machen. Der Webserver ist dann über IPv4 und IPv6 erreichbar, als wenn er selbst Dual-Stack-fähig wäre. Diese Technik lässt sich sowohl für öffentliche Webserver im Internet, als auch private Webserver im Intranet verwenden. Im Allgemeinen ist die Technik nicht nur anwendbar auf Webseiten, sondern generell auf Dienste, die von einem http(s)-Server bereitgestellt werden.

Benötigt wird für diese Technik ein zusätzlicher Rechner (dies kann auch eine virtuelle Maschine sein), auf dem eine Reverse-Proxy-Software aktiv ist. Als Reverse-Proxy kommen mit entsprechender Konfiguration z. B. apache, lighttpd oder nginx in Frage. Der Proxy-Rechner benötigt eine global routbare IPv6-Adresse, sowie eine IPv4-Adresse, von der aus der eigentliche Webserver

erreicht werden kann. Im DNS muss die IPv6-Adresse des Proxy-Rechners als IPv6-Adresse (AAAA-Datensatz) für die gehostete(n) Domain(s) des Webservers eingetragen werden und auf dem Proxy-Rechner muss die IPv4-Adresse des IPv4-only-Webservers bekannt sein (in der Proxy-Konfigurationsdatei).

Folgendes Bild illustriert das Setup mit einem Http-Reverse-Proxy:

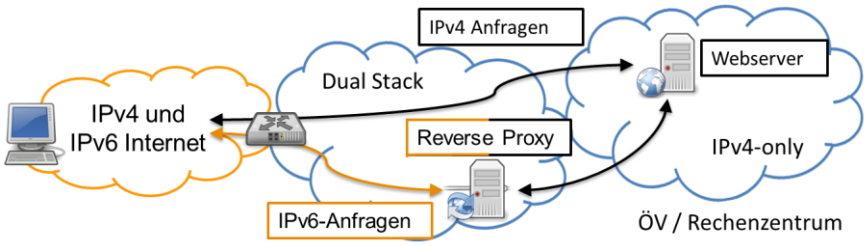


*Abbildung 28: Http-Reverse-Proxy*

Aus Sicherheitsgründen wird empfohlen, dem IPv4-only-Webserver eine weitere IPv4-Adresse zuzuordnen, welche explizit nur vom Reverse-Proxy angesprochen wird. Ferner sollte, wie in Abbildung 28 zu erkennen ist, eine dedizierte zweite Firewall die Datenströme zwischen Reverse-Proxy und Webserver kontrollieren.

Falls auf dem IPv4-only-Webserver komplexere Webdienste (z. B. CMS, Tomcat-Server) aktiv sind, so ist u. U. eine komplexere Proxy-Konfiguration notwendig, als für die Bereitstellung einfacher, statischer Webseiten.

Kommt ein IDS-System zum Einsatz, so muss sein Regelwerk angepasst werden, um Fehlalarme aufgrund der konzentrierten Anfragen des neuen Reverse-Proxies zu vermeiden.

### 7.3.4 Paketbasierte Protokollumsetzer

IPv4/IPv6-Protokollumsetzer sind geeignet, eine logisch transparente Ende-zu-Ende-Kommunikation zwischen IPv4- und IPv6-Komponenten (IPv4-only zu IPv6-only, oder umgekehrt) zu ermöglichen. Eine solche Umsetzung ist jedoch sehr aufwändig, da neben dem eigentlichen Transportprotokoll häufig auch das jeweilige Anwendungsprotokoll umgesetzt werden muss (z. B. FTP, SIP). Darüber hinaus müssen weitere Protokolle umgesetzt werden, z. B. ICMP-Nachrichten und DNS-Anfragen.

Ein praktischer Anwendungsfall für Protokollumsetzer ist z. B. die Verwendung in einem modernen LTE-Mobilfunknetz, in dem nur IPv6 verfügbar ist, aber für die Mobilfunknutzer auch der Zugriff auf das IPv4-Internet möglich sein soll.

Als Alternative zu einem Protokollumsetzer können Proxies verwendet werden, sofern für das jeweilige Anwendungsprotokoll ein Proxy verfügbar ist.

## 7.4. Weitere Verfahren

### 7.4.1 Carrier-Grade NAT (CGN)

**Struktur:**

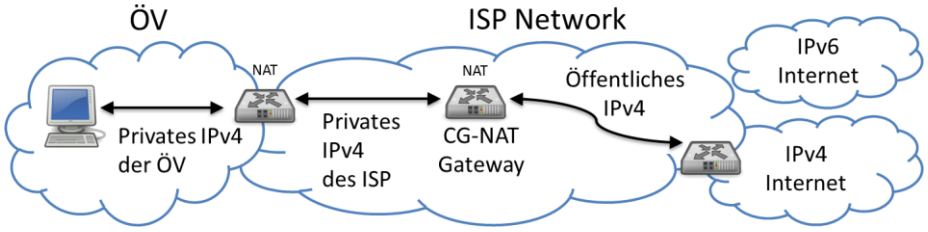


*Abbildung 29: Verfahren Carrier Grade NAT (CGN)*

**Details:**

Carrier Grade NAT (Carrier Grade Network Address Translation; Netzwerk-adressumsetzung auf Providerebene) ist eine Technik, die Provider anwenden können, um dem Problem der IP-Adressknappheit bei IPv4 zu begegnen. Diese Technik findet dort Verwendung, wo sehr viele IP-Adressen benötigt werden, z. B. in großen Mobilfunknetzen.

Carrier Grade NAT ist eine Variante des seit Jahren gebräuchlichen Source-NAT (Netzwerkadressumsetzung auf Quell-IP-Adressen; gelegentlich auch als „Masquerading“ oder NAT44 bezeichnet). Bei Source-NAT übersetzt ein Internet-Gateway zwischen den privaten IPv4-Adressen von Computern in einer Firma oder in einem Heimnetz auf eine (bzw. einige wenige) öffentliche IPv4-Adressen, welche der Firma bzw. dem Heimanschluss vom Provider zugewiesen worden sind. Das Source-NAT ermöglicht es so, viele Computer über wenige IPv4-Adressen mit dem Internet kommunizieren zu lassen und ist somit in erster Linie eine Sparmaßnahme für die schon seit vielen Jahren knappen IPv4-Adressen. Allerdings hat dies Nachteile, z. B. für Serveranwendungen oder VoIP-Telefonie, welche eingehende Verbindungen akzeptieren können müssen. Diese Probleme lassen sich lösen, was jedoch zusätzlichen administrativen Aufwand fordert (z. B. Nutzung von Port-Weiterleitungen oder STUN [RFC5389]).

Bei Carrier Grade NAT (CGN) wird dieses Verfahren nun auch auf Providerebene genutzt, d. h. das ein Kunde des Providers (z. B. LTE-Nutzer oder DSL-Anschluss-Nutzer) vom Provider keine öffentlich im Internet routbare IPv4-Adresse bekommt, sondern eine private IPv4-Adresse (zumeist aus dem 10.0.0.0/8 Adressbereich). Diese ist nur innerhalb des Netzwerkes des eigenen Providers routbar und muss zur Kommunikation ins Internet über ein Internet-Gateway des Providers geleitet werden, welches die privaten IPv4-Adressen auf eine kleinere Anzahl öffentlicher IPv4-Adressen umsetzt. Dabei treten neben den beschriebenen Problemen mit Serveranwendungen auch Probleme bei der normalen Nutzung von Webanwendungen auf, da diese heute Plausibilitätsprüfungen mittels der IP-Adresse und die Ziel- und Quellports durchführen. Eine Datenverbindung *aus* dem Internet *zu* Anwendungen des Nutzers kann im Allgemeinen nicht mehr über den Internet-Gateway des

Providers aufgebaut werden. Ferner stößt Carrier Grade NAT mit steigender Nutzeranzahl auch an Skalierungsprobleme, bei denen der Internet-Gateway des Providers einen Flaschenhals für die Datenströme der Nutzer darstellt.

Ein Internetzugang mit CGN hat bezogen auf IPv4 eine stark beschnittene Funktionalität. Dies wird mit steigender Verbreitung zu einer instabilen Kommunikation der Bürger mit IPv4-Diensten im Internet, auch die der ÖV, führen. In der Folge werden, aufgrund der Kommunikation ohne Übergangstechniken, IPv6-Dienste zukünftig deutlich stabiler und damit attraktiver als IPv4-Dienste sein. Dies ist eine wesentliche Ursache für den flächendeckenden Migrationsdruck zu IPv6.

Im Zusammenhang mit der Nutzung bereits vorhandener NAT-Gateways wird Carrier Grade NAT gelegentlich auch als NAT444 bezeichnet.

## 7.5. Empfehlungen für den Einsatz von IPv6-Übergangstechniken

Die Internetprotokolle IPv4 und IPv6 werden auf absehbare Zukunft den Datenaustausch zwischen Computern und über das Internet dominieren. Es ist davon auszugehen, dass IPv6 eine weitere Verbreitung finden und mittelfristig zum dominierenden Internetprotokoll wird. IPv4 wird jedoch im Internet noch relativ lange parallel in Betrieb sein. Ein Parallelbetrieb ist in weiten Teilen der IT nicht nur sinnvoll, sondern oft unumgänglich, um Kunden aus beiden Welten (IPv4-only, ebenso wie IPv6-only) versorgen zu können. Auch wenn IPv6 einmal eine sehr weite Verbreitung erlangt haben wird, wird man weiterhin mit vielen IPv4-Legacy-Systemen arbeiten müssen. Ein paralleler Betrieb von IPv4 und IPv6 ist die Folge. Dafür ist „Dual Stack“ die Technik der Wahl für die Zukunft.

Erst wenn diese Legacy-Systeme nur noch in geringem Umfang betrieben werden müssen, ist es sinnvoll möglich, diese in separate IPv4-only-Subnetze auszugliedern und die Netzinfrastruktur ansonsten auf IPv6-only umzustellen. Einen Ausblick auf ein mögliches, zukünftiges IPv6-only-Netzwerk gibt der Abschnitt 7.6. Wie im Detail mit IPv4-only-Geräten umgegangen werden kann, ist in Abschnitt 11.1 beschrieben.

Im Folgenden wird erläutert, mit welchen Techniken IPv6 in den Rechenzentren und an den Arbeitsplätzen der öffentlichen Verwaltungen in Deutschland (zusätzlich zu IPv4) eingeführt werden sollte, um eine nachhaltige und zukunftssichere Lösung zu erreichen. Neben Dual-Stack werden für die Fälle, in denen ein nativer IPv6-Internetzugang (noch) nicht möglich ist, Lösungen mit Tunneln betrachtet.

Die Empfehlungen für die Einführung von IPv6 in den öffentlichen Verwaltungen werden im Folgenden differenziert betrachtet für:

(a) Den Zugang zum IPv6-Internet

(b) IPv6 am Arbeitsplatz

(c) IPv6-Zugang für Server, Dienste und Portale

Eine ausführliche Auflistung der Empfehlungen in Form einer IPv6-Leitlinie für die Migration findet sich in diesem Dokument in Anhang II ab Seite 184.

### 7.5.1 Zugang zum IPv6-Internet

Um in einer ÖV den Zugang zum IPv6-Internet zu ermöglichen, muss zuerst der verwendete Zugangsrouter (Access Router, CPE) Dual-Stack beherrschen. Der Internetprovider einer ÖV sollte neben IPv4 natives IPv6 anbieten. Insbesondere bei Neubeauftragungen sollte dies als Vergabekriterium festgelegt werden.

Ohne native IPv6-Unterstützung kann ein Zugang zu IPv6-Netzen, mit Einschränkungen, mittels Tunneltechniken geschaffen werden. Nativer Dual-Stack-Unterstützung ist dringend der Vorzug zu geben. Im Hinblick auf die Marktmacht der öffentlichen Verwaltungen in Deutschland kann hier sicherlich der eine oder andere Provider motiviert werden IPv6 anzubieten.

Technisch wird folgende Konfiguration empfohlen:

- Der oder die Zugangsrouter einer ÖV müssen IPv4/IPv6-Dual-Stack-Betrieb beherrschen.
- Diese Zugangsrouter sollten einen nativen IPv6-Zugang vom Provider erhalten (kommerzieller ISP, DOI, NdB, kommunales Rechenzentrum (RZ), oder Landesrechenzentrum (LRZ))
- Falls dies nicht möglich ist, so sollte vom Zugangsrouter der ÖV ein fester IPv6-in-IPv4-Tunnel zu einem Tunnelserver in einem RZ einer Kommune / eines Landes / des Bundes aufgebaut werden. Zum Aufbau der Tunnelverbindung sollte ein dedizierter Tunnel-Broker in diesem RZ genutzt werden.
    - Ein dedizierter Aufbau und Betrieb solcher Tunnel-Broker und Tunnelserver durch die RZs der ÖV ist kommerziellen Anbietern vorzuziehen, da nur dadurch ein zuverlässiger und auch abgesicherter Tunnelservice für die ÖV möglich ist.
    - Im Falle einer Lösung mit Tunneln kann der IPv6-Tunnelserver (= Tunnelendpunkt) in der ÖV auch ein zusätzliches Gerät sein, und die vorhandenen IPv4-Zugangsrouter können vorerst bestehen bleiben.
- Unabhängig von der konkreten Technik muss der IPv6-Provider (im o. g. Fall das RZ) in der Lage sein, die von der ÖV genutzten IPv6-Präfixe ins Internet zu routen und per BGP zu annoncieren. Hierfür müssen entsprechende Peering-Agreements mit übergeordneten Internetprovidern vorhanden sein.

- Für jede genutzte Technik müssen - analog zum heutigen IPv4-Betrieb - Service Level Agreements (SLAs) über die Verfügbarkeit und ggf. über die Performance des IPv6-Zugangs mit dem Provider vereinbart werden; dies ist insbesondere ein Muss für kritische ÖV-Infrastrukturen.

- Andere Tunneltechniken wie 6to4 sollten auf Grund der bei den Techniken beschriebenen Nachteile nicht genutzt werden. Siehe auch Abschnitt 14.3.1.

### 7.5.2 IPv6 am Arbeitsplatz und unterwegs

IPv6 am Arbeitsplatz bedeutet, dass Betriebssystem, Anwendungen und Infrastruktur (Switches, Router, Intranetserver) nach und nach Dual-Stack-fähig gemacht werden müssen. Der IPv6-Internetzugang am Arbeitsplatz sollte unabhängig von der verwendeten IPv6-Zugangstechnik am WAN-Router sein. Dazu muss ein IPv6-Zugangsrouter nach innen, im Intranet natives IPv6 verwenden. Nach außen sind verschiedene Techniken möglich – es sollte aber vom Provider *natives IPv6* bereitgestellt werden.

Zusammenfassend gelten für *Arbeitsplätze* folgende Empfehlungen:

- Arbeitsplatzrechner sollten selbst IPv4/IPv6 Dual-Stack-fähig sein und auf eine Dual-Stack-Infrastruktur in der ÖV zurückgreifen können.
    - Die Infrastruktur im ÖV-Intranet muss dazu IPv4/IPv6 Dual-Stack unterstützen.

- Arbeitsplatzrechner dürfen aus Sicherheitsgründen nicht selbst Tunnel in das IPv6-Internet aufbauen. Dies muss auch technisch, durch Firewalls, unterbunden werden.
    - Für Heimarbeitsplätze wird empfohlen, dass die jeweilige Zugangstechnik (VPN-Client oder separater Router) ebenfalls IPv6, zusätzlich zu IPv4, bereitstellt.
    - Stellt ein separater Router IPv6 zu Hause bereit, so muss dieser ICMPv6-Präfixdelegation (engl.: ICMPv6 prefix delegation, IPCMv6-PD [RFC3633]) unterstützen.

*Detaillierte Leitlinien für Klienten sind zu finden im Anhang II in Abschnitt 14.2.2.1.*

Für den mobilen Arbeitsplatz, also den Internetzugang mit Laptop, Smartphone, oder Tablet-PC unterwegs ist der Nutzer im Allgemeinen darauf angewiesen, dass der Provider des Mobilfunknetzes IPv6 zur Verfügung stellt.

Für den Fall, dass IPv6 hier nicht verfügbar ist, existieren zwar Übergangstechniken, diese funktionieren aber häufig nicht zuverlässig in Mobilfunknetzen.

### 7.5.3 IPv6-Zugang für Server, Dienste und Portale

Mittelfristig wird empfohlen, zu allen öffentlichen Servern, Portalen und Diensten der ÖV Deutschlands IPv6-Zugang via nativer IPv4/IPv6-Dual-Stack-Unterstützung bereit zu stellen.

Nur so kann sichergestellt werden, dass die Bürger, die zwangsweise zu IPv6 migriert werden, weiterhin ohne Einschränkungen die Netzdienste der Behörden nutzen können werden.

Schon heute haben Mitarbeiter der ÖV aus dem Ausland (insbes. aus Asien) keinen oder nur eingeschränkten Zugriff auf wichtige IPv4-Dienste der ÖV in Deutschland.

Angesichts der IPv4-Adressknappheit wird es zunehmend Provider geben, die IPv4 nur über Tunneltechniken oder über Carrier-Grade NAT bereitstellen können. Dies hat spürbar negative Auswirkungen auf die Qualität des IPv4-Internetzugangs solcher Provider.

Zusammenfassend wird daher für Server, Dienste und Portale der ÖV dringend empfohlen:

- Server, Dienste und Portale müssen per IPv4 und per IPv6 in der gleichen Qualität erreichbar sein.
- Analog zu Abschnitt 7.5.2 gilt:
    - Für den Zugang sollte ein nativer IPv6-Internetzugang seitens des betreffenden Providers genutzt werden.
    - Falls dies nicht möglich ist, so darf der IPv6-Zugang für den Dienst wie in Anhang II beschrieben auch mit Hilfe von sicheren Tunneltechniken (über den Zugangsrouter) erfolgen.
    - Der Provider muss für die Netzbereiche der ÖV aus dem Bereich der LIR de.government das Routing mittels entsprechender Peering-Agreements unterstützen.
    - Die SLAs für den IPv6-Zugang sollten separat vereinbart werden.
- Für öffentliche Webserver und ausgewählte, web-basierte Portalanwendungen wird als Übergangslösung für einen „schnellen Erfolg“ wird die Technik HTTP-Reverse-Proxy (siehe 7.3.3) empfohlen:
    - Da sich hierfür die Konfiguration des existierenden Webservers nicht verändert werden muss, lässt sich diese Technik mit geringem Aufwand umsetzen. Der Reverse Proxy Server wird zusätzlich zum vorhandenen Webserver installiert.
    - Die Software für einen Reverse Proxy ist auch als Open-Source-Software verfügbar, ausgereift und bei sorgfältiger Konfiguration zudem sicher.

- Der Aufwand für den Aufbau eines http-Reverse-Proxy-Servers ist überschaubar, auch für den Fall, dass dieser bei einem späteren Übergang zu einer Dual-Stack-Serverplattform wieder abgebaut wird.

- Bei komplexen Portal-Anwendungen, welche mit aktiven Web-Techniken arbeiten, ist zu prüfen, welche Kommunikationsmuster das Portal außer http get/post benutzt (z. B. AJAX, Web-Sockets, Nutzung von Zertifikaten zur Authentisierung). Gegebenenfalls muss die Konfiguration eines http Reverse-Proxies erweitert werden, damit diese Techniken auch über den Proxy hinweg funktionieren.

- Bei Verwendung von https/TLS mit Serverzertifikaten auf dem Webserver müssen diese auch auf dem Reverse Proxy verfügbar gemacht werden.

*Detaillierte Leitlinien für Server sind im Anhang II in Abschnitt 14.2.2.2 dokumentiert.*

Einen weiteren, speziellen Fall stellen nicht-öffentliche Server, Dienste und Portale der ÖV dar, die in Zukunft über IPv6 genutzt werden sollen. Für diesen Zugriff muss die entsprechende IT-Infrastruktur und der Service selbst Dual-Stack-tauglich gemacht werden. Für detaillierte Schritte hierzu siehe hierzu die Checklisten in Anhang I in diesem Dokument.

Ist kein natives IPv6 verfügbar, so wird empfohlen, betroffene Netze ohne IPv6 mittels IPsec-VPN-Tunneln (LAN-zu-LAN) zu überbrücken. Aus der Sicht des Services und des zugreifenden Klienten erscheint die Kommunikation als durchgängig IPv6-fähig, d. h. die VPN-Tunnel sind für sie transparent.

Die IPsec-VPN-Gateways übernehmen hierbei sowohl den Transport über eine vorhandene IPv4-Infrastruktur (zwischen IPv6-Inseln), als auch die Gewährleistung der Sicherheit durch Transportverschlüsselung.

## 7.6. Ausblick: IPv6-only-Infrastrukturen

Die Herausforderung eines IPv6-only-Betriebes an IT-Infrastrukturen besteht darin, dass alle Infrastrukturkomponenten und Services die Fähigkeit besitzen müssen, ihre Netzfunktionen durchgängig über IPv6 anzubieten. Viele der aktuellen IT-Komponenten mit IPv6-Unterstützung setzen hingegen heute noch einen Dual-Stack-Betrieb voraus.

Selbst wenn in Zukunft alle wichtigen, zentralen Server und Dienste mit nativer IPv6-Unterstützung ausgestattet sein sollten, so verbleiben noch viele IPv4-Systeme, bei denen eine Aufrüstung zu IPv6 entweder technisch oder finanziell keinen Sinn macht. Darunter fallen z. B. viele der bereits aktiven und über das IP-Protokoll (z. B. mit http über eine Web-Schnittstelle) erreichbaren Komponenten wie

- Alte Fachverfahren, insbesondere wenn diese bereits vor Jahren unter Schwierigkeiten zu IPv4 migriert worden sind,
- Konfigurationsschnittstellen von Appliances, wie z. B. Router oder Intrusion-Detection Systemen (IDS),
- „embedded systems“ im Heimbereich, wie z. B. Fernseher oder Media-Player, Internetradio, Internet-fähiger digitaler Bilderrahmen oder Internet-Kühlschrank/Kaffeemaschine,
- Infrastruktursysteme, wie IP-Kamera-Systeme, Druckserver, oder Drucker mit Netzwerkschnittstelle und
- Sensoren (z. B. solche für Umweltmessdaten),
- industrielle Regelungs- und Steuerungs-Systeme.

Es wird geschätzt, dass etwa 5% aller vorhandenen IT-Geräte, die das IPv4-Protokoll nutzen, nicht sinnvoll auf IPv6 aktualisiert werden können.

Bei Standardsoftware sieht die Situation bereits heute sehr gut aus: Aktuelle Webbrowser, Webserver und Betriebssysteme bringen IPv6-Unterstützung bereits mit. Diese muss bei einigen Softwaren lediglich noch durch entsprechende Konfiguration aktiviert werden.

Es gibt allerdings auch bei Software-Systemen und –Diensten einige, bei denen die IPv6-Unterstützung zurzeit wenig verfügbar ist, z. B. NTP-Server/Clients, Fileserver, Druckserver sowie Managementsoftware für Infrastrukturkomponenten.

Der Vorteil von IPv6-only-Umgebungen – nicht zwei logische Infrastrukturen parallel betreiben zu müssen – geht mit dem Risiko einher, einzelne Altsysteme ggf. mit hohem Aufwand (Entwicklung oder ggf. Austausch) IPv6-tauglich machen zu müssen. Alternativ könnten diese IPv4-Altsysteme in einem IPv4-only-Subnetz gesammelt, gekapselt und mittels Protokollumsetzung unter IPv6 verfügbar gemacht werden.

Im Rahmen der Migrationsplanung sollte die jeweilige öffentliche Verwaltung für ihre Infrastruktur abschätzen und planen, zu welchem Zeitpunkt der Lebenszyklus aller IPv4-Altsysteme beendet ist. Ab diesem Zeitpunkt kann der IPv4/IPv6-Parallelbetrieb eingestellt werden.

# 8. IPv6 Sicherheitsaspekte

Dieses Kapitel gibt eine Übersicht über die Sicherheitsaspekte, die sich im Zusammenhang mit der Verwendung des IPv6-Protokolls in den Netzen der öffentlichen Verwaltung (ÖV) ergeben. Weitergehende Informationen zur IT-Sicherheit beim Einsatz von IPv6 bietet das BSI (http://www.bsi.bund.de) in separaten Dokumenten an (z. B. [ISi-LANA], [ISi-L-IPv6]).

Die Sicherheitsaspekte bei der Einführung von IPv6 in bestehende IT-Infrastrukturen (die auf IPv4 basieren) gliedern sich folgendermaßen auf:

- Sicherheitsaspekte des bisher ausschließlich genutzten Protokolls IPv4 – diese sind i. d. R. in der öffentlichen Verwaltung durch Sicherheitskonzepte und Maßnahmen nach BSI-Grundschutz und ggf. IT-Geheimschutz abgedeckt und werden in diesem Leitfaden nicht weiter betrachtet. Es wird davon ausgegangen, dass die bestehende IPv4 Infrastruktur vor Beginn einer IPv6-Migration nach dem aktuellen Stand der Technik abgesichert ist.

- Sicherheitsaspekte des neu hinzukommenden Protokolls IPv6, welche insbesondere durch die neuen in IPv4 noch nicht vorhandenen Funktionen zustande kommen. Die bekannten Herausforderungen bzgl. IPv6 und IT-Sicherheit sind in öffentlichen Quellen gut beschrieben. Mit der aktuellen Verbreitung von IPv6 in alle Netzbereiche steigt auch die allgemeine Auseinandersetzung mit dem Protokoll und damit die Wahrscheinlichkeit weitere Bedrohungen zu identifizieren. Das BSI hat zum Einsatz von IPv6 einen entsprechenden Leitfaden veröffentlicht [ISi-L-IPv6].

- Sicherheitsaspekte die sich aus dem kombinierten Einsatz von IPv4 und IPv6 (Dual-Stack) ergeben. Zu diesen Sicherheitsherausforderungen gibt es bisher nur wenig Erfahrung.

- Sicherheitsaspekte von einzelnen Übergangstechniken, welche den Übergang von IPv4 zu IPv6 erleichtern sollen oder dort IPv6 ermöglichen, wo wesentliche Netzkomponenten noch nicht IPv6-tauglich sind.

Einen sehr detaillierten Überblick zur Fragen der IPv6-Sicherheit gibt auch [NIST-800-119].

Darüber hinaus gelten die grundlegenden Regeln, welche schon bei der Sicherheitskonzeptionierung von IPv4-Netzen gelten, auch weiterhin für IPv6. Dies gilt insbesondere für die organisatorische Sicherheit durch:

- die Definition und Einhaltung von Sicherheitsrichtlinien

- einen klar organisierten IT-Betrieb mit dokumentierten Prozessen

- geschultes und ausreichend vorhandenes Personal

- Netzwerksicherheitskonzepte, welche regelmäßig aktualisiert werden und so gestaltet sind, dass sie die notwendige Kommunikation auch wirklich ermöglichen; damit diese Sicherheit auch gelebt und nicht umgangen wird.

- Eine angemessen dimensionierte Infrastruktur, beginnend mit einer abgesicherten Stromversorgung, über IP-verarbeitende Systeme mit ausrechender Rechen- und Speicherkapazität sowie Stellfläche und Klimatisierung in den entsprechenden Räumlichkeiten.

## 8.1. IPv6-only Sicherheit

### 8.1.1 Standardmäßige Aktivierung von IPv6

Bei fast allen modernen Betriebssystemen ist IPv6 bereits standardmäßig aktiv und zudem das bevorzugte Protokoll. Ohne eine qualifizierte und kontrollierte Einführung von IPv6 inklusive eines entsprechend angepassten IT-Sicherheitskonzepts und entsprechend konfigurierten und IPv6-tauglichen Sicherheitskomponenten, ist die Nutzung in Behördennetzen mit unerwünschten Sicherheitsrisiken verbunden.

Ist IPv6 noch nicht regulär in einer Behörde eingeführt, wie in diesem Leitfaden beschrieben, sollte IPv6 zuerst in allen Komponenten explizit deaktiviert werden. Zusätzlich sollten alle Firewallsysteme initial in der Lage sein, IPv6-Verkehr und IPv4-Tunnel, in denen IPv6 transportiert wird, zu erkennen und zu blockieren. Die Weiterleitung von IPv6 durch interne Router sollte deaktiviert werden, z. B. bei CISCO Routern mit dem Kommando „no ipv6 unicast-routing“.

*Tabelle 7: IPv6 deaktivieren / aktivieren in gängigen Betriebssystemen*

| Betriebssystem | IPv6 aktiviert? | deaktivieren | aktivieren |
|---|---|---|---|
| **Windows 7**<br>**Windows Vista**<br>**Windows Server 2008** | Ja | `HKLM\System\CurrentControlSet\System\Services\TCPIP6\Parameters\DisabledComponents=0xffffffff`<br>(DWORD-Wert (32Bit))<br>& Bindung der Netz-Adapter an " (TCP/IPv6)" entfernen<br><br>Werte für „DisabledComponents”**:**<br>**0** alle IPv6-Komponenten aktivieren. (Windows-Standardeinstellung)<br>**0xffffffff** deaktiviert alle IPv6-Komponenten außer IPv6-Loopback. Vista verwendet so in Präfixrichtlinien IPv4 statt IPv6.<br>**0x20** IPv4 statt IPv6 in Präfixrichtlinie verwenden.<br>**0x10** systemeigene IPv6-Schnittstellen deaktivieren.<br>**0x11** deaktiviert alle IPv6-Schnittstellen außer IPv6-Loopback | `HKLM\System\CurrentControlSet\System\Services\TCPIP6\Parameters\DisabledComponents=0x00000000`<br>(DWORD-Wert (32Bit))<br>& Bindung der Netz-Adapter an "(TCP/IPv6)" herstellen<br><br>Weitere Herstellerinformationen:<br>http://support.microsoft.com/kb/929852/de |
| **Windows XP** | Nein | `netsh interface ipv6 uninstall` | `netsh interface ipv6 install` |
| **Windows 2000** | Nein | `net stop tcpipv6`<br>(wenn IPv6 installiert ist) | Installation des<br>"IPv6 Technology Preview for Windows 2000"<br>`net start tcpipv6` |

| | | | |
|---|---|---|---|
| **LINUX** | Ja,<br>seit Kernel<br>2.6.28-4 | RHEL / CentOS / Fedora / Suse<br>`alias net-pf-10 off`<br>`-> /etc/modprobe.conf`<br><br>Debian/Ubuntu<br>`/etc/modprobe.d/aliases`<br>`alias net-pf-10 ipv6`<br>Ersetzen durch:<br>`„alias net-pf-10 off`<br>`alias ipv6 off“` | RHEL / CentOS / Fedora / Suse<br>`alias net-pf-10 ipv6`<br>`-> /etc/modprobe.conf`<br><br>Debian/Ubuntu<br>`alias net-pf-10 ipv6`<br>`-> /etc/modprobe.d/aliases` |
| **Android** | Ja | `net.ipv6.conf.default.disable_ipv6 = 1`<br>`-> /system/etc/sysctl.conf`<br><br>oder im Terminal<br>`sysctl`<br>`net.ipv6.conf.default.disable_ipv6`<br>(nur rooted Geräte!) | `net.ipv6.conf.default.enable_ipv6 = 1`<br>`-> /system/etc/sysctl.conf`<br><br>oder im Terminal<br>`sysctl`<br>`net.ipv6.conf.default.enable_ipv6`<br>(nur rooted Geräte!) |
| **Apple iOS/**<br>**MacOS** | Ja<br>Ja | nicht möglich<br>`networksetup -setv6off ethernet` | nicht möglich<br>`networksetup -setv6automatic ethernet` |
| **FreeBSD** | Ja, seit 6.1 | `ipv6_enable="No" -> /etc/rc.conf` | `ipv6_enable="YES"-> /etc/rc.conf` |

### 8.1.2 Wegfall der Network Address Translation (NAT)

Bei IPv4 wird eine IP-Adressumsetzung im Netzwerk (network address translation, NAT) oft auch als Sicherheitsfunktion angesehen. NAT ist jedoch für IPv4 in erster Linie als Methode zum Einsparen von offiziellen Internetadressen entwickelt worden. Die mögliche Verschleierung der Struktur interner lokaler Netze, z. B. einer Behörde und die „Ventilfunktion“, bei der eingehender Datenverkehr blockiert wird, wenn nicht eine passende Verbindung zuvor vom internen Netz aus aufgebaut wurde, sind eigentlich Seiteneffekte von NAT.

Da NAT heute bei IPv4 allgemein als Sicherheitsfunktion fehlinterpretiert wird, besteht die Gefahr, dass sich Betreiber und Nutzer von NAT-Gateways in einer trügerischen Sicherheit wiegen. Korrekt ist, dass NAT in der Form „Full Cone NAT“ nach dem Standard RFC 3489 nicht prüft, ob die eingehenden Datenpakete auf einem mit NAT geöffneten Port auch tatsächlich vom zuvor angefragten externen System stammen. Diese sicherheitstechnisch notwendige Prüfung erhalten Betreiber und Nutzer erst durch das sogenannte „Connection Tracking“, welches eine von NAT unabhängige Sicherheitsfunktion ist.

Folglich wird die Anforderung eingehenden Datenverkehr zu blockieren, der nicht zu einer „von Innen“ heraus aufgebauten Verbindung gehört, nur von Firewalls und Routern umgesetzt, die „Connection Tracking“ und die zustandsbasierte Filterung beherrschen, unabhängig von NAT für IPv4.

Da bei IPv6 ausreichend Adressen zur Verfügung stehen, entfällt die Notwendigkeit für den Einsatz von NAT. In den IPv4-Altnetzen wird NAT jedoch weiter verwendet werden (müssen), um der akuten IPv4-Adressknappheit zu begegnen. Im Dual-Stack-Betrieb bedeutet dies eine asymmetrische Art der Kommunikation zwischen IPv4 und IPv6. Dem ist bei der Konzeption von IT-Infrastrukturen mit Dual-Stack Rechnung zu tragen.

Das Dokument „Local Network Protection for IPv6“ [RFC4864] der Internet Standardisierungsorganisation IETF beschreibt detailliert die Implementierung von IPv6 (ohne NAT) mit Sicherheitsfunktionen, die den aus IPv4 mit NAT gewohnten Sicherheitsmerkmalen entsprechen.

### 8.1.3 IPv6 Herstellersupport

IPv6 wird mittlerweile von vielen aktuell am Markt erhältlichen Produkten unterstützt. Da IPv6 – obwohl es schon seit über einem Jahrzehnt standardisiert ist – erst seit etwa 2011 eine breite Marktrelevanz erlangt hat, kann die Unterstützung von bestimmten IPv6-Funktionen heute bei einzelnen Herstellern noch unvollständig und unterschiedlich ausgereift sein.

Eine oft unterschiedliche Implementierung einer Funktion in IPv4 und IPv6 betrifft die Weiterleitung von IP-Paketen in Routern. In modernen Mittelklasse- und Enterprise-Routern geschieht dies durch spezialisierte Hardware. Abhängig vom jeweiligen Router Model lässt sich diese Hardware nicht oder nur unvollständig mit einem Softwareupdate IPv6-tauglich machen, oder der Hersteller hat aufgrund seines Geschäftsmodells kein Interesse, ein solches Update für Altsysteme zu erstellen. Die jeweiligen Router sind dann zwar generell in der Lage, IPv6 zu verarbeiten, allerdings ist ggf. die IPv6 Funktionalität in Software implementiert,

welche auf dem vergleichsweise langsamen Hauptprozessor des Routers abgearbeitet wird. Das Resultat sind deutlich geringere Durchsatzraten von IPv6-Datenverkehr gegenüber IPv4-Datenverkehr. Zudem entsteht hierdurch ein Sicherheitsrisiko für Denial-of-Service-Attacken.

Behörden sollten bei der Beschaffung darauf achten, dass ihnen die Hersteller von Netzkomponenten eine annähernd identische Leistung beim Einsatz von IPv6 und IPv4 vertraglich zusichern. In der Folge gilt dies auch für die Vergabe von Netzdienstleistungen, z. B. Netzanschlüsse und WAN-Kopplungen.

### 8.1.4 IPv6 First Hop Security

Der mit Abstand überwiegende Teil von bekannten und neu entdeckten Sicherheitsschwächen bezogen auf IPv6 ist nur wirksam wenn sich der Angreifer bereits im gleichen, lokalen Netzsegment wie die Zielsysteme befindet und direkten Zugriff auf die Netzschnittstellen der Zielsysteme hat. Dieser Bereich von Netzwerksicherheit wird als „First Hop Security“ bezeichnet. Die folgenden Mechanismen wirken in diesem Bereich.

**Neighbor Discovery:**

Das Neighbor Discovery Protokoll (NDP) [RFC4861] ist der funktionelle Ersatz für das Address Resolution Protocol (ARP) unter IPv4. Durch den Einsatz vom NDP ergeben sich neue Angriffsvektoren in Netzwerken. Diese lassen sich in drei Kategorien unterscheiden (vgl. [RFC3756]):

1) Nicht auf Router bzw. Routing bezogene Angriffsvektoren
2) Auf Router bzw. Routing bezogene Angriffsvektoren
3) Replay- und Remote-Angriffsvektoren

Nicht auf Router bzw. Routing bezogene Angriffsvektoren:

Diese Angriffsvektoren beziehen sich direkt auf Funktionen des Neighbor Discovery Protokolls:

- **Neighbor Solicitation (NS) / Advertisement (NA) Spoofing**: Für die Zuordnung einer MAC-Adresse zu einer IP-Adresse wird Neighbor Solicitation / Advertisement verwendet. Durch das Senden von falschen Neighbor Solicitations oder falschen Neighbor Advertisements im lokalen Netzsegment kann ein Angreifer andere Netzwerkknoten dazu veranlassen, Pakete an falsche Ziele zu senden.
- **Neighbor Unreachibility Detection (NUD) Angriff**: Ein Angreifer kann fingierte Neighbor Advertisements als Antwort auf NUD Neighbor Solicitations senden. So wird vorgetäuscht, dass ein bestimmter Netzwerkknoten nicht erreichbar ist.
- **Duplicate Address Detection (DAD) Angriff**: Ein Angreifer antwortet selbst auf jeden Versuch eines neuen Netzwerkknotens, der über DAD

herausfinden will, ob die IPv6-Adresse, die er erhalten soll, bereits vergeben ist. Der Angreifer teilt diesem unter Verwendung von NS und NA in seiner Antwort mit, dass diese IPv6-Adresse vergeben (NS) ist oder er selbst ein DAD (NA) ausführt.

Die drei genannten Angriffe fallen in die Kategorie der Denial-of-Service (DoS)-Angriffe, benötigen aber einen direkten Zugang zum lokalen Netz (first hop attacks).

*Sicherheitsleitlinien hierfür sind zu finden in Anhang II in Abschnitt 14.3.*

Auf Router bzw. Routing bezogene Angriffsvektoren:

Diese Angriffsvektoren nutzen die die Router-Entdeckung und Router-bezogene Funktionen:

- **Bösartiger Last Hop Router**: Ein Angreifer kann sich als Last Hop Router ausgeben. Dazu antwortet der Angreifer auf Multicast Router Advertisements (RA) Solicitations von einem neuen Host mit RAs als Multicast oder Unicast und gibt sich so als Last Hop Router aus.
- **Nicht-Verfügbarkeit des Default Routers**: In diesem Angriff stellt ein Angreifer es so dar, als ob der Default Router nicht verfügbar wäre. Dies wird entweder durch eine DoS-Attacke erreicht, oder durch das Senden eines gefälschten RAs mit einer Lebenszeit (Lifetime) die den Wert Null enthält. Ist kein Default Router vorhanden, so führen die Netzwerkknoten ein Neighbor Discovery aus und senden ihre Pakete direkt weiter. Dies hat zur Folge, dass die Pakete im gleichen Netzwerksegment bleiben und nicht über den Router weitergeleitet werden.
- **Spoofed Redirect Nachricht**: Die Link-Local-Adresse des Next-Hop Routers wird von einem Angreifer verwendet, um eine Redirect Nachricht an einen Netzwerkknoten zu senden. Dieser wird die Redirect-Nachricht akzeptieren, da es den Anschein hat, als ob die Redirect-Nachricht vom Next-Hop-Router kommt. Solange ein Angreifer auf die NUDs antwortet, bleibt der Redirect erhalten.
- **Falsches On-Link-Präfix**: Ein Angreifer kann eine RA-Nachricht senden, die einen Präfix mit beliebiger Länge enthält. Damit wird erreicht, dass ein Netzwerkknoten dieses Präfix für On-Link[5] hält, so dass er für dieses Präfix nicht über den Next-Hop Router kommuniziert.
- **Falscher Adresskonfigurationspräfix**: Es wird von einem Angreifer eine RA-Nachricht mit einem ungültigen Subnetzpräfix gesendet. Ein Netzwerkknoten, welcher Address Auto Configuration durchführt, verwendet dieses Präfix und konfiguriert sich somit eine Netzwerkadresse, die ungültig ist.

[5] On-Link bedeutet hier: gültig für diesen Netzwerkabschnitt.

- **Parameter Spoofing**: Bei diesem Angriff werden bestimmte Parameter in RAs von einem Angreifer verändert. Dabei werden gültige RAs, die ein Router aussendet, kopiert. Bei den kopierten RAs werden bestimmte ausgewählte Parameter angepasst, so dass beim Versenden der veränderten RAs der Datenverkehr im Netzwerk unterbrochen werden kann. Parameter, die angepasst werden können, sind z. B. Hop-Limit und die „M"- und „O"-Flags.

Replay- und Remote- Angriffsvektoren:

Die Replay- und Remote-Angriffsvektoren lassen sich wie folgt untergliedern:

- **Replay-Angriffe**: Neighbor- und Router-Discovery Nachrichten sind anfällig für Replay-Angriffe. Ein Angreifer schneidet Neighbor- und Router-Discovery-Nachrichten mit und sendet diese zu einem späteren Zeitpunkt erneut.

- **Neighbor Discovery DoS-Angriffe**: Ein Angreifer erstellt Adressen mit dem gleichen Subnetzpräfix und schickt dann kontinuierlich Nachrichten an diese Adressen. Der Last Hop Router versucht, über NS-Nachrichten, diese Adressen aufzulösen. Dies führt dazu, dass Knoten, die dem Netz beitreten möchten, den ND-Dienst nicht nutzen können. Dieser Angriff wird in der Regel von einem entfernten Netzsegment aus durchgeführt.

### 8.1.5 Domain Name System Security Extensions (DNSsec)

Die Sicherheitsaspekte, welche in einem IPv4-Netzwerk bzgl. DNS relevant sind, behalten auch durch die Einführung von IPv6 weiterhin ihre Gültigkeit. Dies umfasst zum einen die Absicherung der DNS-Server selbst und zum anderen die Sicherheit des DNS-Dienstes.

Bezogen auf den DNS-Dienst bedeutet Sicherheit z. B. die Verwendung von kryptografischen Schutzmechanismen. Zwei Standards sind hierfür definiert worden: "DNS Security Extensions" (DNSSEC) [RFC4033], [RFC4034] und [RFC4035] für vertrauenswürdige DNS-Abfragen und „The Secret Key Transaction Authentication" (TSIG) [RFC2845] für abgesicherte Zonentransfers zwischen zwei DNS Servern. Wesentlich ist hierbei, dass in den DNS-Einträgen bei DNSsec vertrauenswürdiges Schlüsselmaterial hinterlegt wird. Diese Funktionen sind weitgehend identisch für IPv4 und IPv6.

DNSsec kann darüber hinaus noch einen Sicherheitsaspekt auflösen, welcher typisch für IPv6 ist. Bei der ursprünglichen Spezifikation von IPv6 wurde festgelegt, dass eine vollständige IPv6 Implementierung in jedem Fall eine IPsec-Implementierung zur Verschlüsselung und Signierung des IPv6 Datenverkehrs beinhalten muss. Um diese sicher nutzen zu können, ist es allerdings notwendig, ein kryptographisches Zertifikat zu erhalten, zur Prüfung, ob man mit der gewünschten Gegenstelle kommuniziert. Bisher gibt es keine flächendeckende öffentliche Infrastruktur oder einen passenden Mechanismus, um von jedem möglichen weltweiten System dieses Zertifikat erhalten zu können. DNSsec bietet nun mit dem Konzept der „Opportunistic Encryption" die Möglichkeit dieses

Schlüsselmaterial auch für IPsec vorzuhalten und über DNS-Abfragen bereitzustellen.

In der aktuellen Spezifikation ist IPsec-Unterstützung inzwischen als optional gekennzeichnet. Dies ist ein Eingeständnis an die Leistungsfähigkeit von eingebetteten Systemen (embeded systems) und Sensoren mit direkter IP-Datennetzverbindung. Solche Systeme werden in zunehmendem Maße auch IPv6 unterstützen müssen, bieten aber nicht genügend Rechenressourcen für IPsec. Für alle anderen Systeme (Server, Arbeitsplatzrechner, aktuelle Mobilgeräte und Tabletcomputer) sollte IPv6 mit IPsec-Unterstützung im Betriebssystem bzw. im IP-Stack vorhanden sein, auch wenn dies im IPv6-Standard nicht mehr explizit gefordert wird.

### 8.1.6 Multicast

Multicast überträgt Datenpakete im Gegensatz zu Unicast nicht zwischen zwei Systemen, sondern von einem System an ein Menge anderer Systeme. Es wurde schon für IPv4 spezifiziert und war hauptsächlich zur effizienten Übermittlung großer Datenmengen an viele Benutzer gleichzeitig gedacht, z. B. synchrones Videostreaming von TV-Programmen. Hierfür hat sich Multicast in öffentlichen Netzen nie durchsetzen können und wird vermutlich auch in den Netzen der öffentlichen Verwaltung zukünftig kaum eine Rolle spielen. Folglich kann das Einsatzszenario von Multicast und IPsec im Transport Mode, welches die Aushandlung von sogenannten Gruppenschlüsseln erfordern würde, vernachlässigt werden.

IPv6 nutzt Multicast allerdings, anders als IPv4, um eine automatisierte Konfiguration zwischen Endgeräten in einem lokalen Subnetz zu erreichen. Grob gesagt nutzt IPv6 Multicast dort, wo IPv4 Broadcasts verwendet. Da man somit in den lokalen Netzen Multicasts mindestens für bestimmte Nachrichtentypen zur korrekten Funktion von IPv6 erlauben muss, ist es für die Sicherheit wichtig, diese Kommunikation lokal zu begrenzen. Multicastpakete sollten hierzu an den Netzübergängen zu öffentlich Netzen und externen Organisationen i. d. R. blockiert werden. Es sollten auch lokal nur Multicastpakete mit den Scope-Typen 1-3 und ggf. 4-8 durch Filterregeln zugelassen werden (1 – Node-local, 2 – Link-local, 3 – Subnet-local, 4 - Admin-local, 5 - Site-local, 8 - Organization-local).

Folgende Aspekte müssen beachtet werden:

- **MLD-Pakete (Multicast Listener Discovery)**: IPv6-fähige Router, Firewalls und Tunnelendpunkte müssen Multicast-Scope-Grenzen festlegen, so dass MLD-Pakete nicht routbar sind.
- **Bekannte Multicast-Adressen**: Bekannte Multicast-Adressen können dazu verwendet werden, um die IP-Adressen von Routern oder Servern regulär herauszufinden. Diese Multicast-Adressen sollten an Netzwerkübergängen blockiert werden, so dass Router und Server nicht nach außen bekannt werden oder sich externe Systeme als interne ausgeben können.

### 8.1.7 Mobile IPv6

Mobile IPv6 (MIPv6) wird dazu eingesetzt, eine durchgehende IP-Konnektivität für mobile Geräte, wie z. B. Notebooks, PDAs und Smartphones auch während fortgesetzter Mobilität zu gewährleisten.

Der Einsatz von MIPv6 ist sehr komplex. Aus diesem sind Sicherheitsaspekte bereits zum Beginn der Entwicklung von MIPv6 mit betrachtet worden. Folgende RFCs sind u. a. in diesem Zusammenhang relevant:

- [RFC3776]: Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents
- [RFC4225]: Mobile IP version 6 Route Optimization Security Design Background
- [RFC4285]: Authentication Protocol for Mobile IP
- [RFC4487]: Mobile IPv6 and Firewalls: Problem Statement
- [RFC4449]: Securing Mobile IPv6 Route Optimization Using a Static Shared Key
- [RFC4877]: Mobile IPv6 Operations with IKEv2 and the revised IPsec Architecture
- [RFC4882]: IP Address Allocation Privacy and Mobile IPv6: Problem Statement
- [RFC5845]: Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6
- [RFC5726]: Mobile IPv6 Location Privacy Solutions
- [RFC5637]: Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6

Zusätzlich ist bei der Verwendung von MIPv6 zu beachten, dass die Endgeräte, die MIPv6 verwenden, selbst abgesichert sein müssen. Hier sind die klassischen Sicherheitsmechanismen für Hosts anzuwenden. Diese umfassen z. B. den Einsatz lokaler Firewalls, sowie IPS- und Anti-Virus-Software auf den Endgeräten.

## 8.2. Dual-Stack

Auch in Dual-Stack-Umgebungen gelten die klassischen IT-Sicherheitsprinzipien, wie bereits zu Beginn von Kapitel 8 erwähnt. Ein Dual-Stack-Betrieb erhöht im Vergleich zu IPv4-only bzw. IPv6-only die Komplexität für das Management. Dabei ist jeder Dual-Stack-Knoten über die Schwachstellen beider Protokolle bzw. deren Implementierung / Nutzung in Anwendungen gefährdet. Die folgenden beiden RFCs setzen sich mit der Sicherheit in Dual-Stack-Umgebungen im Detail auseinander:

- [RFC4852]: IPv6 Enterprise Network Analysis IP Layer 3.
- [RFC4942]: IPv6 Transition / Coexistence Security Considerations.

Folgende Punkte sollten in Bezug auf Sicherheit in Dual-Stack-Umgebungen beachtet werden:

- **Sicherheitsrichtlinie**: Es sollte eine konsistente Sicherheitsrichtlinie für IPv4-only, Dual-Stack und IPv6-only vorhanden sein. Die Vorgaben müssen für IPv4 und IPv6 gleichermaßen umgesetzt werden (z. B. in Bezug auf Firewall-Regeln).
- **Funktionalitäten**: Neue Funktionalitäten wie z. B. Extension-Headers, Auto-Konfiguration (via SLAAC) und Neighbor Discovery (ND) sollten in die Sicherheitsbetrachtung explizit mit einfließen.
- **Tunnelmechanismen**: Bei der Verwendung von IPv4- und IPv6-fähigen Endgeräten in einem Netzwerk können u. U. automatische Tunnel aufgebaut werden, die ein Sicherheitsrisiko darstellen (vgl. Teredo). Dies ist insbesondere bei der Verwendung von Windows-Systemen zu beachten, da hier die Tunneladapter im Auslieferungszustand nach der Installation eingeschaltet sind.
- **Network Security Equipment**: Für Netzwerksicherheitskomponenten (Firewalls, IDS / IPS, ALG) müssen unter IPv6 vergleichbare Funktionalitäten wie unter IPv4 zur Verfügung stellen. Dies umfasst u. a. Filtering, Monitoring, Logging, Auditing und Reporting.
- **Performance**: Die Leistung von Systemen wie Routern, Firewalls, ALGs und IDS / IPS kann negativ beeinflusst werden, wenn beide Protokolle parallel verarbeitet werden müssen und ggf. die Verarbeitung von IPv6-Regeln langsamer von statten geht als bei IPv4. Die Leistungsfähigkeit von Geräten für IPv6 sollte vorab festgestellt werden.
- **Monitoring / Auditing**: Es sollte ein IPv6-Monitoring etabliert werden, welches den IPv6-Datenverkehr in einer ÖV überwacht, so dass nicht gewünschter IPv6-Datenverkehr und Rogue-Systeme[6] entdeckt werden können. Das Monitoring und Auditing sollte insbesondere auch Tunnel-verkehr sowie Router- und Neighbor-Solicitations entdecken können.

[6] Als Rogue-Systeme werden Systeme bezeichnet, die in einem Netzwerk platziert werden, um Informationen über das Netzwerk und aus dem Netzwerk zu sammeln.

## 8.3. IPv6-Übergangstechnologien und Sicherheit

### 8.3.1 Carrier Grade NAT

Die Verwendung von Carrier Grade NAT (CGN) bringt einige Sicherheitsrisiken mit sich. Das größte Risiko ist dabei der Ausfall des Dienstes, da ein CGN-Gateway in einem Providernetz einen zentralen „Single-Point-of-Failure“ darstellt. Aufgrund der sehr hohen Anzahl von Kommunikationsverbindungen über einen solchen Knoten hinweg (bis zu 20 Millionen bei großen ISPs) sind Hochverfügbarkeitsmechanismen, welche sämtliche Verbindungen auf einen anderen Knoten retten kaum realisierbar. Es sind darüber hinaus DoS-Angriffe leicht vorstellbar, welche bewusst eine große Anzahl von NAT-Verbindungen produzieren und so die Systeme stark belasten und ggf. verlangsamen können. Die Fehlersuche und auch forensische Untersuchungen von IT-Vorfällen über CGN-Systeme hinweg ist so gut wie ausgeschlossen, da die Lebensdauer der NAT-Verbindungen nur zwischen 30 und 120 Sekunden beträgt. Während bisher bei der Fehlersuche der Quellport einer Verbindung kaum eine Rolle spielte, ist dieser bei Verbindungen über CGN neben der IP-Adresse das wichtigste Merkmal, welches sich zudem im Sekundentakt ändern kann. Eine einzelne Quell-IP-Adresse repräsentiert nun auch nicht mehr nur einen Benutzer oder einen Anschluss, sondern eine Vielzahl von Nutzern gleichzeitig.

### 8.3.2 DS-Lite

Da DS-Lite CGN verwendet, gelten hier die gleichen Sicherheitsaspekte. Für DS-Lite sind weitere Sicherheitsaspekte zudem im [RFC6333] beschrieben.

### 8.3.3 Tunneling

In diesem Abschnitt werden die allgemeinen Sicherheitsaspekte dargestellt, die sich im Zusammenhang mit Tunneltechniken ergeben.

**Tunnelendpunkte:**

Tunnelverbindungen *zu* einer ÖV müssen als Verbindung von Extern betrachtet werden, da der Datenverkehr der an einem Tunnelendpunkt ankommt, prinzipiell von überall her kommen kann, d. h. der Ursprung des Datenverkehrs kann aus unsicheren, nicht vertrauenswürdigen Netzen stammen. Aus diesem Grund muss der getunnelte (IPv6-)Datenverkehr überprüft und kontrolliert werden. Dies bedeutet, dass Firewalls, ALGs, IDS / IPS und Anti-Virus-/Malware-Erkennungs-Software die gleichen Sicherheitsrichtlinien innerhalb eines Tunnels anwenden müssen wie außerhalb des Tunnels. Zusätzlich sollten nur Tunnel von und zu bekannten, sicher authentifizierten Kommunikationspartnern erlaubt werden. Dies kann durch ein entsprechendes Regelwerk an den Perimeter-Firewalls konfiguriert werden, welches bestimmt, von und zu welchem Kommunikationspartner und über welche Protokolle ein Datenverkehr stattfinden darf. Für den Fall, dass der Datenverkehr in den Tunneln über mit IPsec geschützt ist, ist ein geeignetes Autorisierungskonzept zu etablieren.

**Security Equipment / Firewalls:**

Es muss sichergestellt werden, dass das eingesetzte Security-Equipment, z. B. ALGs, den Tunnel-Datenverkehr untersuchen kann. Das heißt, der eingebettete IPv6-Datenverkehr muss ausgepackt und evtl. entschlüsselt werden. Für den Fall, dass dies nicht möglich ist, müssen die eingesetzten Sicherheitsgeräte den Tunnelverkehr blockieren können.

Firewalls sollten auf getunnelten IP-in-IP Datenverkehr angewendet werden können. So kann unerwünschter Datenverkehr über ein Blockieren ausgewählter Protokolle verhindert werden. Dies betrifft z. B. das Blockieren von Protokoll 41 (IP-in-IP-Verkehr). Ferner sollte ausgehender UDP-Verkehr mit Ziel-Port 3544 blockiert werden (zur Verhinderung von IPv6-Teredo-Tunneln von Klienten aus).

**IDS / IPS:**

Aufgrund der noch geringen Verbreitung von IPv6 sind IDS/IPS-Systeme für IPv6 noch selten. Es gibt jedoch inzwischen eine Reihe von Ansätzen für potentielle IPv6-Angriffe. Hersteller von IDP und IPS stellen zurzeit nur wenige Informationen darüber bereit, welche dieser Szenarien durch ihre Systeme abgedeckt werden. Daher ist zum jetzigen Zeitpunkt schwer zu beurteilen, welche der Szenarien praktische Relevanz erreichen, so dass eine begründete Liste von Anforderungen, die derartige Systeme erfüllen müssen, erst später erstellt wird.

**IPv4-Router:**

Netzwerkadministratoren müssen sich der Tatsache bewusst sein, dass auf Routern eingesetzte ACLs nicht für getunnelten IPv6-Datenverkehr wirksam sind, da der in IPv4 eingebettete IPv6-Datenverkehr nicht vom Router ausgewertet wird.

**Sicherheitsempfehlungen für Tunnel:**

Folgende weiteren Sicherheitsempfehlungen sollten im Zusammenhang mit Tunneln beachtet werden:

- **Destination Unreachable**: Das Dokument [RFC4213] „Basic Transition Mechanism for IPv6 Hosts and Routers“ empfiehlt für den Fall eines vom Security Device geblockten Tunnels, an den Sender ein „destination unreachable“ zu schicken.
- **Verwerfen**: Tunnel, die Multicast-, Loopback-, IPv4-kompatible oder IPv4-gemappte Quelladressen enthalten, sollten verworfen werden.
- **Untersuchung**: Ein Tunnel muss so konfiguriert sein, dass er vom eingesetzten Security Equipment untersucht und ggf. geblockt werden kann.
- **Endpunkte**: Tunnelendpunkte müssen so konfiguriert werden, dass Tunnel nur von und zu bestimmten Endpunkten aufgebaut werden können.

- **Separierung**: Sollten auf einen Endpunkt mehrere Tunnel terminiert werden, dann muss jeder Tunnel als separates Interface behandelt werden. Dies dient dazu, dass Scoping-Regeln nicht verletzt werden und dass ND-Datenverkehr isoliert wird.

## 8.4. IPv6-Sicherheitsplanung

Die Sicherheitsplanung soll gewährleisten, dass mindestens das bisherige Sicherheitsniveau des IPv4-only-Netzwerks auch nach der IPv6-Migration gewährleistet ist. Die Sicherheitsplanung sollte dabei folgende Punkte umfassen:

- **Sicherheitsrichtlinie**: IPv6 muss in die Sicherheitsrichtlinie einer ÖV mit aufgenommen werden.
- **Konfigurationsvorgaben**: Es sollten Konfigurationsvorgaben für alle Komponenten erstellt werden, die Konfigurationsvorgaben benötigen, z. B. Switche, Router, Firewalls, IDS / IPS, Betriebssysteme, Arbeitsplatzsysteme und Serversoftware.
- **Perimeterschutz**: Der Netzwerkperimeter muss mit IPv6-fähigen Firewalls, IDS / IPS und ALGs geschützt werden. Dabei muss für beide Protokolle ein identisches Sicherheitsniveau hergestellt werden. Beim IPv6-Rollout sollte zuerst der Perimeter gesichert werden. Zusätzlich ist die entsprechende Firewall so zu konfigurieren, dass unerwünschter Tunnel-Datenverkehr, z. B. Teredo-Datenpakete, an der Firewall blockiert werden. Das gleiche gilt für IDS- / IDS-Systeme und ALGs.
- **Patch Management**: Auch für Komponenten, die IPv6-fähig sind, müssen alle sicherheitsrelevanten Patches zeitnah eingespielt werden.
- **Infrastrukturdienste**: Für die korrekte Funktion der IPv6-Sicherheitssysteme sind IPv6-fähige Infrastrukturdienste, wie DNS, DHCPv6 und NTP notwendig.
- **Netzwerkmanagement und -Monitoring**: Für ein sicheres Netzwerkmanagement (NMS) und -Monitoring müssen diese Systeme Daten und Konfigurationen mit IPv6-Adressen verarbeiten können. Notwendig sind NMS-Systeme und Monitoringsysteme, welche bereits selbst durchgängig IPv6 nutzen können. Leider sind diese Systeme bisher am Markt selten. Die Hersteller sollten auf ihre konkrete IPv6-Releaseplanung angesprochen und zugesagte Verfügbarkeitstermine schriftlich festgehalten werden.
- **Vulnerability Management / Security Incident and Event Management (SIEM)**: Das Vulnerability Management und das SIEM sollten, falls vorhanden, IPv6-fähig sein, um die zu überwachenden Komponenten ansprechen zu können. Zusätzlich sollten diese Systeme die zu überwachenden Komponenten auf IPv6-spezifische Probleme überprüfen können.

- **Netzwerkkomponenten**: Aktivierung von IPv6 auf Routern und Switches. Die Zugriffsregeln (Access Control Lists, ACL) von Routern sind für den IPv6-Datenverkehr anzupassen, sowie, wenn möglich, 802.1x (NAC / NAP) auch für IPv6 zu aktivieren. Zusätzlich sollte Duplicate Address Detection (DAD) aktiviert werden.

- **Security-Komponenten**: Regelwerke von Firewalls, Kryptogateways, IDS / IPS und ALGs sind für beide Protokolle parallel zu pflegen. Dabei ist sicherzustellen, dass diese sowohl für IPv4 als auch für IPv6 wirksam sind. Insbesondere ist für IDS / IPS ist sicherzustellen, dass die Erkennungssignaturen gleichermaßen wirksam sind. Entsprechende Tests sind hierfür durchzuführen, um zu evaluieren ob die Erkennungssignaturen für beide IP-Protokolle wirksam sind und um die die Herstelleraussagen zu verifizieren.

- **Sicherheit von Endsystemen**: Die Sicherheitssoftware (Host-Firewall, Host-IDS / IPS, Antivirensoftware, etc.) sowie die Managementsoftware, die auf Endsystemen eingesetzt wird, muss IPv6-fähig sein.

- **Hersteller-Support**: Der Hersteller muss das notwendige Know-how zur Verfügung stellen, um in einem Problemfall die Betreiber der IT in der ÖV unterstützen zu können. Für den Betrieb müssen vorhandene Service Level Agreements (SLA) um Spezifikationen für IPv6 erweitert werden.

- **Rogue Detection**: Es sollte gewährleistet sein, dass unerwünschte (unplanmäßig auftauchende) IPv6-Systeme im Intranet einer ÖV erkannt werden.

- **Konfigurationsmanagement**: Der Dual-Stack-Betrieb ist komplexer als der Betrieb von IPv4 alleine. So sind die Auswirkungen von einzelnen Konfigurationsänderungen schwerer vorhersehbar. Aus diesem Grund sollte die Einführung eines Konfigurationsmanagementsystems abgewogen werden. Voraussetzung für dessen Einsatz ist zunächst der Test in einer separaten Testumgebung, welche auch schon unter IPv4-only für einen größeren IT-Betrieb erforderlich ist.

- **Sicherheitszertifizierung**: Sicherheitszertifizierungen von Komponenten sollten auch die Sicherheit der IPv6-Funktionen einschließen und zertifizieren.

- **Sicherheits-Monitoring / -Auditing**: Das Monitoring und Auditing von sicherheitsrelevanten Vorfällen sollte sowohl unter IPv4 und IPv6 verfügbar sein. Dabei sollten sicherheitsrelevante Vorfälle nach IPv4-only, IPv6-only und Dual-Stack klassifiziert werden.

## 8.5. IPv6 und Datenschutz

Neben den vielen Vorteilen birgt IPv6 auch neue Herausforderungen an den Datenschutz mit sich, die zum einen aus den nun wieder für jedes Endgerät verfügbaren eindeutigen Adressen, aber auch aus der Unerfahrenheit der Nutzer mit dem neuen Protokoll herrühren.

Schon ursprünglich waren für alle Knoten des Internets feste Adressen vorgesehen. Erst das rasante Wachstum des Internets und die Adressknappheit bei IPv4 führte zur Einführung der dynamischen Adressvergabe bei Einwahl-Anschlüssen von Privatkunden (typischerweise DSL oder Mobilfunk). Dabei entstand auch ein Geschäftsmodell, bei dem feste IP-Adressen (wie sie z. B. für den Betrieb eines Web-Servers notwendig sind) als höherwertig angesehen werden. Gleichzeitig konnten sich für bestimmte Anwendungen Produkte durchsetzen, die mit dynamischen IP-Adressen auf einfache Weise umgehen können. Bekanntestes Beispiel ist die Internet-Telefonie-Software Skype, die eine Erreichbarkeit unter einem festen Nutzernamen trotz wechselnder IP-Adressen ermöglicht. Bei IPv6 ist nun die Vergabe von „hochwertigen" festen IP-Adressen aufgrund der Größe des Adressraums für alle Teilnehmer möglich, und jeder Endnutzer könnte ohne Hilfsdienste unter einer bekannten IP-Adresse erreichbar sein. Diese Variante wird vor allem von technisch versierten Internet-Nutzern gewünscht. Sie können damit auf ihre Heim-Infrastruktur von außen zugreifen und eigene Web-Server betreiben. Andererseits ist damit ein Datenschutz-Problem verbunden, denn auch ausgehende Verbindungen würden diese festen IP-Adressen nutzen. Damit könnten externe Dienste-Anbieter theoretisch personenbezogene Nutzerprofile kontextübergreifend anlegen und pflegen, was in Deutschland nicht verfassungskonform ist. Es gibt also unvermeidbare Widersprüche: So möchte man beim Surfen normalerweise nicht lokalisiert oder wiedererkannt werden, für bestimmte Anwendungen oder für Notrufe möglicherweise jedoch schon.

Unabhängig von der IP-Adresse eines Nutzers gibt es zudem auch noch andere Möglichkeiten zur Wiedererkennung von Nutzern im Internet (z. B. Cookies im Browser). Zum Teil geben Nutzer auch freiwillig persönliche Daten in ihrer Internetpräsenz preis, etwa auf ihren persönlichen Seiten in Sozialen Netzen.

Für die öffentliche Verwaltung in Deutschland liegt der Unterschied von IPv6 zu IPv4 insbesondere darin, dass im Gegensatz zu IPv4 ein übergreifendes Adress-konzept erstellt wurde, bei dem durchgängig sogenannte „Global Unicast" Adressen verwendet werden können, was doppelt vergebene Adressen verhindert. Daraus resultiert, dass diese Adressen und die Personen, die für die *Verwaltung* der sehr großen Adressbereiche zuständig sind, in die weltweit öffentliche RIPE-Datenbank eingetragen werden. Die Datenschutzaspekte und Konzepte hierfür werden im Folgenden skizziert, wobei klar zwischen dem Datenschutz bei dem IPv6-Adressmanagement und dem Datenschutz beim konkreten Einsatz unterschieden wird.

### 8.5.1 IPv6-Adressmanagement und Datenschutz

Bei der gesamten Konzeption der IPv6-Adressvergabe für die deutsche ÖV durch die LIR de.government, wie sie im IPv6-Referenzhandbuch und der Beschlussvorlage für den IT-Planungsrat vom 3.3.2011 beschrieben sind, wurde von Beginn an großer Wert auf eine datenschutzfreundliche Konzeption und Umsetzung gelegt.

#### 8.5.1.1 Keine personenbezogenen Nutzerdaten

Durch die konkrete Ausgestaltung der IPv6-Adressvergabe in der ÖV entstehen keine Adressen, welche konkreten Personen zuzuordnen wären.

#### 8.5.1.2 Verbergen von Organisationsstrukturen

Die Einträge der vergebenen IPv6-Adressen in der öffentlichen RIPE-Datenbank sind auf der Grundlage der RIPE-Policy zur Vergabe von IPv6-Adressen (RIPE 512) vom August 2011 konzeptioniert und vorgesehen.

Hiernach sind Datenbankeinträge für vergebene IPv6-Adressen zwar verpflichtend, sollte jedoch die Offenlegung von Organisationsstrukturen nicht erwünscht sein, so können laut Policy sehr große IPv6-Adressbereiche in teil-anonyme Subnetze aufgeteilt und mit dem Status „aggregated-by-lir“ in die RIPE-Datenbank eingetragen werden. Möchte eine sognannte Sub-LIR dagegen die Verantwortung für einen bestimmten Adressbereich transparent delegieren, spricht dies für die Eintragung in der RIPE-Datenbank im Status „assigned“. Somit besteht die Möglichkeit die Einträge so grob zu gestalten, dass sich weder Rückschlüsse auf Bereiche in Behörden noch auf einzelne Personen durchführen lassen.

Für welchen IPv6-Adressbereich welche Art der Adressvergabe gewählt wird, muss jeweils von den Sub-LIRs in ihren Festschreibungen zum Adressrahmenkonzept dokumentiert und ggf. begründet werden. Welche Gründe in Behörden für die jeweilige Wahl der Eintragungsart sprechen und welche Auswirkungen diese haben, wurde den Sub-LIR-Verantwortlich bereits mündlich und schriftlich dargelegt. Damit wird bewusst Datenschutzanforderungen Rechnung getragen.

#### 8.5.1.3 Prozentuale Vergabedokumentation

Nach den Konzepten des IPv6-Referenzhandbuchs, wird jede Sub-LIR zum Start ihrer IPv6-Adressenvergabe mit ihrem Adressbereich, i. d. R /32, in der RIPE-DB eintragen und in der Folge lediglich die prozentuale Vergabe regelmäßig grafisch öffentlich dokumentiert. Es kann folglich nicht nachvollzogen werden, welche Teilorganisation oder gar welcher Nutzer IPv6-Adressen zugeteilt bekommen hat.

#### 8.5.1.4 Ansprechpartner für Adressbereiche in der RIPE-DB

Personenbezogene Einträge entstehen lediglich bei der öffentlichen Eintragung der Personen, die berechtigt sind, den IPv6 Adressraum der ÖV zu verwalten, also zu den Mitarbeitern der LIR de.government und der geplanten Sub-LIRs. Ein Aktuelles Bespiel für einen solchen Eintrag ist unter:

**http://www.db.ripe.net/whois?searchtext=2a02:1000::/26**

zu finden. Hierzu wurde eine erste juristische Betrachtung durchgeführt:

#### 8.5.1.5 Rollen admin-c und tech-c in der RIPE-DB

RIPE-Zitat:

> "admin-c" (administrative contact) and "tech-c" (technical contact) are network contacts, required to be listed by their nic-handles in certain RIPE Database objects. This is done for operational correspondence such as Network troubleshooting. The admin-c must be physically located at the site of the network. The tech-c does not need to be physically located at the site of the network. You can have multiple admin-c, tech-c and zone-c attributes in an object, each of them referencing different person or role objects.

In die RIPE-Datenbank werden die Ansprechpartner in den Rollen Admin-c und Tech-c eingetragen. Zu diesen Rollen in der RIPE-DB gibt es bisher keine bekannte Rechtsprechung in Deutschland, allerdings existieren diese Rollen ebenfalls im Zusammenhang mit dem Namenssystem DNS des Internet, für das in Deutschland die DENIC verantwortlich ist.

Ein Vergleich mit der Rechtsprechung zur DENIC ist juristisch grundsätzlich möglich, da die Rolle zumindest analog zu sehen ist.

Im Rahmen der Registrierung als admin-c bei der DENIC geht der überwiegende Teil der Obergerichte davon aus, dass eine Verantwortlichkeit des admin-c für die Seiteninhalte ausscheidet. Es wird lediglich eine interne Beziehung zur DENIC angenommen, also auf rein administrative Aufgaben abgestellt. Nach wie vor existiert aber auch eine anders lautende Rechtsprechung, die eine Verantwortlichkeit des admin-c sieht.

Übertragen auf die RIPE würde die vorherrschende Meinung in der Rechtsprechung bedeuten, dass auch hier eine Verantwortlichkeit für die übertragenen Daten ausgeschlossen ist. Der admin-c steht auch hier letztlich nur als Verbindungsglied und Ansprechpartner zur Verfügung. Ein Einfluss auf die übertragenen Inhalte besteht nicht. Auch die RIPE selbst geht von dieser Sichtweise aus, indem sie den Zweck einer „operational correspondence such as Network troubleshooting“ nennt. Somit sollen der admin-c und der tech-c wohl lediglich als Ansprechpartner bei Netzwerkproblemen bzw. bei allgemeinen Fragestellungen dienen.

Im Ergebnis wird eine Verantwortlichkeit des admin-c und des tech-c also zu verneinen sein. Fraglich ist jedoch, warum laut RIPE-Regeln ein personenbezogener Eintrag gewählt werden soll.

Die Telekom verfolgt den Ansatz, sowohl als admin-c als auch als tech-c lediglich auf Konzerngliederungen verweisen zu lassen, ohne Personen zu nennen (entgegen den Regeln der RIPE). Das Erfordernis einer aufwändigen Änderung der Daten im Falle eines Stellenwechsels ist so schon durch das Rollenmodell der RIPE-datenbank vermieden.

#### 8.5.1.6 Veröffentlichung der Kontaktdaten von admin-c und tech-c

Ein Widerspruch wegen der Verletzung datenschutzrechtlicher Regelungen gegen eine Weisung eines Vorgesetzten zur Eintragung als admin-c mit der Dienstadresse käme wohl nicht in Betracht. Grundsätzlich können die Mitarbeiter der Verwaltung im Rahmen ihrer Aufgaben auch dazu verpflichtet werden, in der Öffentlichkeit in Erscheinung zu treten und sich entsprechend auszuweisen, also etwa ihre dienstliche Erreichbarkeit zu nennen. Hierin liegt eine dienstliche Notwendigkeit um den Kontakt nach außen und damit überhaupt eine funktionierende Verwaltung zu ermöglichen. Eine Übermittlung dieser Daten an die RIPE kommt mithin gemäß §16 BDSG in Betracht.

Bei der Nennung einer natürlichen Person sollte jedoch immer lediglich die Dienstanschrift verwendet werden, wie dies bspw. durch das BSI gegenüber der DENIC für die Domain bund.de praktiziert wird.

### 8.5.2 Datenschutz bei der Nutzung von IPv6

Im Wesentlichen ist zu bedenken, wann ein Nutzer sich in welchem Netz mit einer statischen, immer wieder diesem Nutzer zuzuordnenden IPv6-Adresse bewegen soll und möchte und wann nicht.

Für den Bereich der privaten Internetanschlüsse bedeutet dies beispielsweise, dass der Endnutzer / Bürger zwar die Möglichkeit hat, die lokale Adressvergabe (z. B. über Privacy Extensions) und Schutz vor Tracking im Webbrowser eigenständig und selbstverantwortlich zu steuern. Jedoch ist er einer weltweit eindeutigen Zuordnung seiner Benutzer(gruppe) zu einem vom Provider zwangsweise zugeordneten, statischen IPv6-Prefix hilflos ausgeliefert.

Für die Zuweisung von Präfix und Interface-ID als Bestandteile der kompletten IPv6-Adresse sind also verschiedene Instanzen zuständig: Das Routing-Präfix stammt vom Internet Service Provider und wird auf der Seite des Endnutzers zum Präfix ergänzt, beispielsweise durch den WLAN-Router. Die Endsysteme wiederum nutzen das Präfix (eines oder mehrere) und ergänzen es um die Interface-ID. Stellt man die verschiedenen Möglichkeiten zusammen, so erhält man die folgende Übersicht mit möglichen Adressarten und Eigenschaften.

| Präfix | Interface Identifier | Betriebsart |
|---|---|---|
| Statisch | statisch | Server-Betrieb / Peer-to-peer möglich bzw. Endsysteme erreichbar |
| Statisch | temporär | „Haushalt“ erkennbar, Privatsphäre abhängig von Anzahl der Nutzer im Netz |
| Temporär | statisch | „Geräte-ID“ in verschiedenen Netzen, minimale Privatsphäre |
| Temporär | temporär | Privatsphäre maximal geschützt |

*Tabelle 8: Mögliche Kombinationen aus Präfix und Interface Identifier*

Mittels einer statischen Adresse kann ein Endsystem von außen erreicht werden, was auch die Grundlage von bestimmten, auf dem Peer-to-Peer-Modell basierten Anwendungen sein kann. Diese Endsysteme können direkt aus dem Internet erreicht werden und müssen nicht auf Hilfsdienste im Internet zurückgreifen (was auch mit eigenen Sicherheits- und Datenschutzproblemen verbunden sein kann).

Mit einer temporären Adresse ist zwar die Privatsphäre optimal geschützt, es lassen sich aber nur Verbindungen nach Außen aufbauen und man verbaut sich den Weg zu neuen, innovativen IPv6-Anwendungen. Bekommt ein Haushalt ein festes Präfix, so kann die Nutzung über dieses Präfix beobachtet werden. Die typische Präfix-Länge und typische Arten der Nutzung des Präfixes sind den Anbietern von Analysewerkzeugen bekannt. Über die Privatsphäre entscheidet dann die Anzahl der Nutzer im Netzwerk hinter dem Präfix. Entscheidend ist dann, ob man sich hinter einer Reihe von Zugriffen wirksam „verstecken“ kann, d. h. ob ein Multiplex aus gemischten Zugriffen für den Beobachter noch einen Wert hat.

Problematisch aus Datenschutz-Sicht ist der Verzicht auf eine temporäre Interface-ID insbesondere bei Mobilgeräten. Wenn diese beispielsweise über WLAN genutzt werden, so enthält ihre IPv6-Adresse über verschiedene Netze hinweg eine Art Geräte-ID durch die immer gleiche Interface-ID.

Die Deutsche Telekom kündigt an, das sie einerseits den Wechsel des Präfixes durch den Kunden („per Knopfdruck“) unterstützt und andererseits auch in ihren DSL-Routern das zugewiesene Teilnetz (unterhalb des Routing-Präfix von /56) regelmäßig getauscht wird. Von anderen Providern sind diesbzgl. noch keine Details bekannt. Die Angebote der Provider werden sich erst im Laufe der Zeit konsolidieren, wobei es viele Einflussfaktoren gibt: Die Anzahl der Internet-Angebote auf dem deutschen Markt steigt durch Angebote über Mobilfunk / Kabel, und es breiten sich IP-TV- und Internet-Telefonie-Dienste weiter aus, was einen Einfluss auf die technische Nutzung des Anschlusses hat. Nutzer von DSL-Anschlüssen oder mobilen Geräten sollten auf jeden Fall die Privacy Extensions auf ihren Endsystemen einschalten. Im Heimbereich sollte der Zugangsrouter daher wenn möglich so konfiguriert werden, dass der Adressbereich – also das genutzte Präfix – periodisch verändert wird. Der Zugriff von außen kann optional auf einen festen Adressbereich erfolgen. Diese Netztrennung zwischen Servern und Arbeitsplätzen ist auch unter Sicherheitsaspekten sinnvoll und kann z. B. in einem Paketfilter leicht auf verschiedene Zugriffsregeln abgebildet werden.

Optimal wäre die Bereitstellung von mehreren Adressbereichen gleichzeitig durch den Provider. Der Nutzer könnte für ausgehende Kommunikation, insbesondere zum Surfen im Internet, einen temporären Adressbereich nutzen und gleichzeitig eingehende Kommunikation über einen festen Adressbereich bedienen. Über einen weiteren, temporären Adressbereich aus der letzten Adressvergabe-Periode, können lang andauernde temporäre Verbindungen der letzten Periode noch fortgeführt werden [Donn11].

Deshalb ist es zur Wahrung des Datenschutzniveaus in den Behörden notwendig, eine externe Zuordnung von IPv6-Adressen zu bestimmten Mitarbeitern im Internet durch wechselnde Endgeräte-Adressteile zu verhindern. Intern können

die Behörden diese Zuordnung z. B. in einer Logdatei ggf. zur späteren Auswertung dokumentieren.

Für die Nutzung Behörden-interner Dienste kann auf ausgwählten Arbeitsplätzen ggf. auch mit statischen IPv6-Endgeräteadressen gearbeitet werden. Allerdings sind statische IPv6-Adressen auf Arbeitsplatz-Systemen im Gegensatz zu dynamisch vergebenen Adressen rechtlich als personenbezogene Daten zu behandeln und bedürfen daher eines besonderen Schutzes.

## 8.6. Zusammenfassung Sicherheitsaspekte / Sicherheitsempfehlungen

Die wichtigsten Sicherheitsempfehlungen für die Einführung von IPv6 sind:

- **Filtern von internen IPv6-Adressen**: Eine ÖV muss zusätzlich zu IPv4-Adressen interne IPv6-Adressen, die nicht direkt mit dem Internet kommunizieren sollen, (spätestens) am Perimeter blockieren.
- **Filtern von ICMP**: Es dürfen nur nicht-essentielle ICMPv6-Nachrichten blockieren werden. Zu den essentiellen IPv6-ICMP-Nachrichten gehören ND, NS, RS, SA und Path Maximum Transmission Unit (MTU) Discovery. Zusätzlich empfiehlt es sich, Echo-Reply-Nachrichten zu erlauben. Details hierzu sind beschrieben in [RFC4890].
- **Filtern von Multicast Source Adressen**: Multicast Source Adressen sollten aus Sicherheitsgründen am Übergang zu externen Netzen bzw. an Tunnelendpunkten blockiert werden.
- **Privacy Extensions**: IPv6 Privacy Extensions (PEX) stellen zur Kommunikation im Internet einen Datenschutz- und Sicherheitsgewinn für Arbeitsplatzsysteme dar. Auf Grund der Struktur der ÖVs mit ALGs und Proxies ist ein Schutz der Mitarbeiter / Mitarbeiterinnen vor Wiedererkennung von IP-Adressen durch Dritte bereits technisch gegeben. Daher muss PEX nicht verwendet werden. Der Einsatz von Privacy Extensions erschwert zudem das Troubleshooting in einer ÖV, da es das Aufspüren von Hosts im Intranet erschwert.
- **Patch- und Update-Management**: Ein kontinuierliches und stringentes Patch- und Updatemanagement ist essentiell für IKT-Systeme, um einen sicheren Betrieb zu gewährleisten. Bei IPv6 handelt es sich um ein in der Praxis noch nicht massiv genutztes Protokoll, mit dem weniger Erfahrungen als mit IPv4 vorhanden sind. Dies kann zu unvorhergesehenem Fehlverhalten von IPv6-fähigen Geräten und Applikationen führen. Diese Fehler sind – ggf. in Kooperation mit dem Hersteller – zeitnah durch Updates und Patches zu beheben.
- **Host-Sicherheit**: Aufgrund der ausgeprägteren Ende-zu-Ende Kommunikationseigenschaften von IPv6 steigt die Bedeutung den Sicherheitsmechanismen auf den Endgeräten. Daher sollte die Host-Sicherheit durch den Einsatz von Sicherheitssoftware wie Anti-Virus-Software und lokalen Host-Firewalls gewährleistet sein. Diese sollten vollständig IPv6-fähig und aktuell sein.

- **Extension Headers**: Für die Konfigurationsvorgaben der Perimeter-Router und Firewalls muss definiert werden, welche Extension Header Typen weitergeleitet werden und welche nicht. So sollten z. B. Pakete, die einen Routing Header enthalten, nicht weitergeleitet werden.
- **Routing-Protokolle**: IPsec sollte zur Absicherung von OSPFv3 und RIPng eingesetzt werden. MD5 sollte zur Absicherung von IS-IS und BGP verwendet werden. Im Zusammenhang mit BGP4 sollten die Protokoll-inhärenten Sicherheitsmechanismen verwendet werden.
- **Unerwünschte Tunnel blockieren**: Das Protokoll 41 (IP-in-UP) und UDP-Pakete mit dem Ziel-Port 3544 sollten an Firewalls blockiert werden, um den Aufbau nicht erwünschter Tunnel (z. B. Teredo) zu verhindern.
- **Deaktivierung von IPv6**: IPv6 sollte zuerst auf Hosts deaktiviert werden und solange deaktiviert bleiben, bis es aktiv und wissentlich freigeschaltet wird. Dies verhindert unvorhergesehene Seiteneffekte. Zum Beispiel können Systeme Probleme bekommen, wenn sie bereits IPv6 aktiviert haben, aber noch in einem IPv4-only-Subnetz verbunden sind. Diese können sich z. B. durch lange Zugriffszeiten auf IPv6-fähige Webseiten zeigen.
- **IPv6-Richtlinie**: Es soll eine IPv6-Richtlinie existieren, welche definiert, wann und auf welchen Systemen IPv6 aktiviert werden darf oder soll.

# 9. Migration von Komponenten in der IT-Infrastruktur

Vor der eigentlichen Migration steht die Analyse der IT-Infrastruktur. Aus der Migrationsplanung wird abgeleitet, welche Teilnetze, Komponenten und Funktionen im Einzelnen migriert werden sollen. Dabei ist nicht immer sofort klar, ob einzelne Geräte alle benötigten Funktionen für IPv6 unterstützen. Hilfestellung bietet das IPv6-Profil [IPv6_PROFILE], welches zur Untersuchung von vorhandenen Komponenten oder zur Beschaffung von neuen Geräten genutzt werden kann. Dieses Profil listet alle für IPv6 relevanten Anforderungen auf und ordnet sie auf zwei Arten den Netzwerkkomponenten zu: Die erste Strukturierung erfolgt aufgrund von Geräteklassen, darunter erfolgt eine Strukturierung durch Funktionskategorien. Im Kapitel 4 des IPv6-Profil-Dokuments [IPv6_PROFILE-DOK] wird beschrieben, wie die Tabellen genutzt werden können und wie die Angaben des Profils zu interpretieren sind.

## 9.1. Basisinfrastrukturkomponenten

In diesem Abschnitt werden die Aspekte beschrieben, welche bei der Migration von Infrastrukturkomponenten zu einem Dual-Stack-Betrieb in einer ÖV berücksichtigt werden müssen. Dies betrifft Layer-2- und Layer-3-Komponenten sowie wichtige Infrastrukturdienste. Die Vorgehensweise für eine Migration umfasst jeweils folgende Schritte:

1) Erfassung der IST-Situation
2) Schrittweise Migration
3) Prüfung des Ergebnisses

Um eine IT-Infrastruktur Dual-Stack-tauglich zu machen, gibt es mehrere Möglichkeiten. Generell können (a) vorhandene Komponenten Dual-Stack-tauglich gemacht werden (durch Upgrade oder Austausch) , oder es können (b) vorhandene IPv4-Komponenten um IPv6-Komponenten der gleichen Funktionsklasse (z. B. Router) ergänzt werden. Es wird empfohlen, wo möglich Variante (a) zu wählen, um eine möglichst deckungsgleiche Struktur der IPv4- und IPv6-Netze aufzubauen und die Komplexität der Infrastruktur in Grenzen zu halten.

Dort wo es nicht anders möglich ist wird in Variante (b) jeweils eine IPv6-only Netzwerk-Komponente parallel zur IPv4-only Komponente angeschlossen. Dies kann auch aus Performanz-Gründen überlegt werden. Aus Gründen der Übersichtlichkeit und Managebarkeit des Netzwerks ist dies nicht als Standard-Vorgehen empfohlen.

### 9.1.1 Switch

Switche sind essentielle Komponenten der IT-Netzwerkinfrastruktur einer öffentlichen Verwaltung (ÖV). Switche sind die Kopplungselemente, welche Netzwerksegmente und / oder Netzwerkelemente (Hosts, Router etc.) auf Layer 2 des ISO/OSI-Referenzmodells miteinander verbinden. Die Entscheidung für das

Weiterleiten von Datenpaketen über einen bestimmten Switch-Port ist unabhängig von IP-Adressen[7] und basiert auf den MAC-Adressen der Datenpakete. Im Zusammenhang mit IPv6 bedeutet dies, dass ein Switch im Gegensatz zu anderen Netzwerkelementen kein IPv6 unterstützen muss, um eine Weiterleitung von Datenpaketen und somit das reibungslose Funktionieren eines Netzwerks mit IPv6 bzw. Dual-Stack zu ermöglichen.

Aus Monitoring- und Management-Gründen besitzen managed Switches auch selbst eine IP-Adresse, unter der die Managementschnittstelle des Switches erreichbar ist. In einem Dual-Stack-Netzwerk sollte die Managementschnittstelle zusätzlich zu IPv4 auch unter IPv6 erreichbar sein. Zusätzlich ist zu beachten, dass ein Switch bestimmte IPv6-relevante Funktionen, wie z. B. DAD-Snooping unterstützen sollte.

Darüber hinaus enthalten Enterprise Switche häufig einfache Teilfunktionalitäten von Routern oder IP-Paketfiltern und werden dann Layer-3 Switche genannt. So sind zum Teil zustandslose Paketfiltermechanismen (ACLs) integriert. Diese können als zusätzliche Sicherheitsbarriere bei einer Netztrennung verwendet werden, allerdings niemals eigenständig ohne eine zusätzliche „echte“ Firewall mit einem zustandsbasierten Filter.

Diese einfachen IP-Mechanismen müssen, wenn sie schon unter IPv4-only in das Netzkonzept integriert und verwendet wurden auch mit IPv6 parallel zur Verfügung stehen.

#### 9.1.1.1 Erfassung der IST-Situation

**Annahme:**
Im Netzwerk einer ÖV ist ein Switch im Netzwerk vorhanden. Dieser befindet sich im produktiven Betrieb. Die Managementschnittstelle des Switches ist über IPv4 erreichbar.

**Ziel:**
Der Switch soll zusätzlich auch IPv6-Datenverkehr weiter leiten und unter IPv6 die gleiche Performanz bzgl. des Netzwerkverkehrs wie unter IPv4 gewährleisten.

**Optional:**
Das Management des Switches sollte über IPv6 möglich sein (je nach Managementschnittstelle über ssh, telnet oder http(s)). Zusätzlich sollte ein Monitoring des Switches über IPv6 möglich sein, z. B. über SNMP.

Vor der Migration sind folgende Informationen zu erfassen:

- An den Switch angeschlossene Router
- Verwendete VLANs
- IPv4-Adresse der Managementschnittstelle

[7] Ein *Router* operiert auf Layer 3 des ISO/OSI-Referenzmodells und leitet Datenpakete auf Basis von IP-Adressen weiter.

- Konfigurierte MAC-Filter
- Zuordnung Ports zu VLANs und angeschlossenen Netzwerkknoten
- Angeschlossene Netzwerke (IP-Subnetze)
- Typ und Version der Firmware
- DNS-Name des Switches (falls Eintrag existiert)
- DNS-Name des NTP-Servers, der vom Switch verwendet wird

Werden die IP-Funktionen von Layer-3 Switchen verwendet sind diese ebenfalls zu erfassen

#### 9.1.1.2 Migration

Eine Migration besteht aus den Punkten:

- Vorbereitung der Migration
- Durchführung der Migration

**Migrationsvorbereitung:**

Zur Migrationsvorbereitung gehören alle Punkte, die gewährleistet werden müssen, damit eine nachgelagerte Migration reibungslos durchgeführt werden kann. Folgende Punkte sind zu prüfen und / oder vorzubereiten:

- Sichern der Switch-Konfiguration
- Überprüfen der Firmware
- Notieren der für IPv6 zu konfigurierenden Parameter

Sichern der Konfiguration:

Die Konfiguration des Switches muss vor Änderungen oder Upgrades gesichert werden, ggf. in mehreren Versionsständen, um bei Fehlfunktionen ein Rollback auf einen funktionierenden Stand zu ermöglichen. Die Sicherung der Konfiguration ist auch für den Fall des Austauschs des Switches durchzuführen, da in der Regel die alte Konfiguration, ggf. mit Anpassungen, auf neue Systeme eingespielt werden können.

Überprüfen der Firmware:

Die Firmware des Switches muss dahingehend überprüft werden, ob sie bereits IPv6-tauglich ist. Sollte die Firmware aktuell kein IPv6 unterstützen, so gibt es folgende Möglichkeiten um die IPv6-Tauglichkeit des Switches zu gewährleisten:

**Firmware Upgrade**: Die Firmware sollte, wenn es möglich ist, auf eine die IPv6-taugliche Version aktualisiert werden.

**Austausch**: Ist es nicht möglich, die IPv6-Tauglichkeit durch das Aktualisieren der Firmware zu erreichen, sollte der Switch gegen einen IPv6-tauglichen Switch ausgetauscht werden.

**Nicht explizit IPv6-tauglicher Switch**: Sofern gesichert ist, dass keine Layer-3-Funktionalitäten (z. B. DHCP-Snooping) genutzt werden, ist eine IPv6-Tauglichkeit des Switches nicht zwingend notwendig. Ein reiner Layer-2-Switch ist IP-agnostisch und kann weiterbetrieben werden. Es wird jedoch empfohlen, auch bei reinen Layer-2-Switches nur prinzipiell IPv6-taugliche Geräte einzusetzen.

Notieren der für IPv6 auf dem Switch zu konfigurierenden Parameter:

Folgende Werte müssen für den Switch im IPv6-Adresskonzept und im IPv6-Netzwerkplan fixiert sein:

- IPv6-Präfix des IPv6-Subnetzes, in dem sich der Switch befindet
- IPv6-Adresse für die Managementschnittstelle
- IPv6-Default-Gateway für die Managementschnittstelle, sofern diese genutzt wird
- Verwendete VLANs für IPv6-Datenverkehr (je Port)
- Für Layer-3 Switche die entsprechenden Filterregeln zwischen den für IPv6 zu IPv4 funktional identischen Subnetzen und Hosts, sowie die Werte für mögliche weitere genutzte IP-Funktionen

Hinweis: Unter IPv6 sollten die gleichen VLANs verwendet werden wie unter IPv4. Der Hintergrund ist die einfachere Verwaltung und Handhabung des Netzwerks, insbesondere im Zusammenhang mit der Suche und der Behebung von Fehlern. Sollten andere VLANs unter IPv6 verwendet werden, sind diese zu definieren und zu notieren.

**Durchführung der Migration:**

Bei der Migration eines Switches sind mehrere Schritte durchzuführen. Ein Teil dieser Schritte ist optional. Dies hängt davon ab, ob die Firmware und das Betriebssystem aktualisiert werden müssen und ob bestimmte optionale Parameter konfiguriert werden müssen. Folgende Schritte umfasst die Migration:

- Optional: Upgrade der Firmware
- Optional: Austausch des Switches
- Konfiguration der IPv6-relevanten Parameter
- Optional: Konfiguration zusätzlicher Parameter

Upgrade der Firmware:

Die Firmware des Switches sollte, falls notwendig und möglich, auf eine IPv6-taugliche Version aktualisiert werden.

Austausch des Switches:

Ein Austausch des Switches ist dann vorzunehmen, wenn es nicht möglich ist, den Switch durch eine Aktualisierung der Firmware und / oder des Betriebssystems IPv6-tauglich zu machen.

Konfiguration der IPv6-relevanten Parameter:

Die vorher festgelegten Parameter sind zu konfigurieren. Dazu gehören

- IPv6-Präfix des IPv6-Subnetzes in dem sich der Switch befindet,
- IPv6-Adresse für die Managementschnittstelle,
- IPv6-Default-Gateway für die Managementschnittstelle und
- VLANs für den IPv6-Datenverkehr (je Port).

Konfiguration zusätzlicher Parameter:

Falls folgende Funktionen genutzt werden sollen, so müssen zusätzlich diese Parameter konfiguriert werden:

- **DHCPv6 Snooping**: DHCPv6-Nachrichten zwischen Teilnehmern und dem Netzwerk sind in der Weise zu filtern, dass keine falschen DHCPv6-Adressen von nicht autorisierten DHCPv6-Servern verteilt werden.
- **Router Advertisement (RA) Filtering**: Im Netzwerk sind RA- Filter zu verwenden, so dass nicht autorisierte RA-Nachrichten blockiert werden. Achtung: Diese Funktion bietet keinen völlig sicheren Schutz gegen unautorisierte RA-Nachrichten, sondern erschwert diese lediglich.
- **Neighbor Discovery**: Neighbor Solitcitations und Neighbor Advertisements unter IPv6 sollten wie bei der “Dynamischen ARP Überprüfung” unter IPv4 überprüft werden.
- **Duplicate Address Detection (DAD), Snooping und Filtering**: Nur autorisierte Adressen als Herkunftsadresse in DAD- Nachrichten von jedem Port sind zu erlauben.
- **SNMP**: Das Management über SNMP sollte für den Switch aktiviert werden und möglichst bereits IPv6 tauglich sein.

#### 9.1.1.3 Prüfung des Ergebnisses

Nach Abschluss der Konfigurationsarbeiten sollte überprüft werden, ob alle vorgenommenen Einstellungen persistent sind. Dazu sollte der Switch einmal neu gestartet werden. Bevor der Switch neu gestartet wird, sollte die Konfiguration

nochmals gesichert werden. Während des Neustarts des Switches sollte durch Sichtung des Startprotokolls überprüft werden, ob

- das Firmware-Update funktioniert hat
- das Betriebssystem-Update funktioniert hat
- die Installation von Patches funktioniert hat und
- ob die neue Konfiguration erfolgreich vom Switch geladen wurde
- und ob die Konfigurationsanpassungen aktiv sind.

Folgende Prüfungen müssen nach der Migration erfolgreich bestanden werden:

- **Managementschnittstelle**[8]: Der Zugriff auf die Managementschnittstelle des Switches über IPv4 und IPv6 muss überprüft werden:
    - Telnet: Der Switch sollte nur über Telnet erreichbar sein, falls dies auch vor der Migration gewollt und erlaubt war.
    - SSH: Der Switch muss über SSH erreichbar sein.
    - HTTP(s): Erreichbarkeit des Switches über HTTP(s).
    - SNMP: Der Switch sollte über SNMP erreichbar sein.
    - Weitere Dienste: Für den Fall, dass weitere Dienste auf dem Switch unter IPv4 aktiviert waren, so ist deren Verfügbarkeit nur für IPv4 und IPv6 zu testen.
- **Performance:** Es ist durch Lasttests zu überprüfen, ob die Performance des Switches für den Dual-Stack-Betrieb ausreicht.
- **Parameter:** Die Parameter bzgl. Snooping und Filtering von ND und DAD sind zu überprüfen.
- **NTP:** Es ist zu überprüfen, ob der Switch den NTP-Server erreichen kann.
- **DNS:** Die Namensauflösung des Switches unter IPv6 sollte überprüft werden.

### 9.1.2 Router

Router sind die zentralen Elemente jeder IT-Netzinfrastruktur. Sie verbinden mehrere IP-Subnetze und leiten IP-Datenpakete zwischen diesen Netzen weiter. Router werden überall dort als Vermittler zwischen IP-Netzen eingesetzt, wo eine Layer-3-Domäne, also ein IP-Subnetz endet. Die aktiven Routingtabellen

[8] In Abhängigkeit ob diese Dienste unter IPv4 bereits zur Verfügung gestellt wurden.

bestimmen dabei, zu welcher ausgehenden Schnittstelle am Router ankommende IP-Datenpakete weiter geleitet werden.

Im Rahmen der Umstellung von (Teil-)Netzen der öffentlichen Verwaltung auf IPv4/IPv6-Dual-Stack-Betrieb müssen alle beteiligten Router neben IPv4 auch IPv6 unterstützen und entsprechend konfiguriert werden, um eine Funktionalität analog der vorhandenen bei IPv4 umzusetzen. Die folgenden Abschnitte zeigen dazu die notwendigen Schritte auf.

#### 9.1.2.1 Erfassung der IST-Situation

**Annahme:**
Im Netzwerk der ÖV ist ein IPv4-only Router vorhanden, der sich im produktiven Betrieb befindet. Der Router ist dafür zuständig, dass Datenpakete im Netzwerk (aktuell unter Verwendung von IPv4-Adressen) zwischen IP-Subnetzen weiter geleitet werden. Der Router kann Filter (Access Control Lists, ACLs) konfiguriert haben, die auf Basis von IPv4-Adressen definiert sind. Zusätzlich besitzt der Router eine Managementschnittstelle, über die er verwaltet wird und über die er im Monitoring eingebunden ist.

**Ziel:**
Der Router soll im Dual-Stack-Betrieb die gleiche Funktionalität, Sicherheit und Performanz bzgl. des Netzwerkverkehrs gewährleisten, wie zuvor im IPv4-only Betrieb.

**Optional:**
Das Management des Routers sollte über IPv6 möglich sein (z. B. via ssh, http(s), …). Zusätzlich sollte das Monitoring des Routers über IPv6 möglich sein, z. B. über SNMP, NetFlow [RFC3954] und Syslog. Weitere optionale Funktionen, die ein Router unter IPv6 unterstützen muss, sind in Abhängigkeit vom Verwendungszweck zu definieren.

Bei einem Router ist die aktive Konfiguration zu sichern und der Netzwerk- und Patch-Plan (Netzwerk-Interface-Anschlussplan) zu analysieren und ggf. zu aktualisieren. Dabei sind folgende Informationen zu erfassen:

- Angeschlossene Netzwerkknoten (Server, Hosts, Switches etc.)
- Angeschlossene Netzwerke (IP-Subnetze)
- Zuordnung von Interfaces zu angeschlossenen Netzwerkknoten (Port-Belegung)
- IPv4-Adressen der Interfaces
- Cluster-IPv4-Adressen (virtuelle IP-Adresse (VIPs)) der Interfaces, für den Fall das der Router redundant ist.
- IPv4-Adresse der Management-Schnittstelle des Routers
- Konfigurierte IPv4-Filter (ACLs)

- Genutzte VLANs
- Statische Routen / Verwendete Routing-Protokolle
- DHCP Relay-Funktion / DHCP-Server-Funktion
- Typ und Version des Betriebssystems
- Typ und Version der Firmware
- DNS-Name des Routers (falls Eintrag existiert)
- DNS-Name des NTP-Servers, der von dem Router verwendet wird.

#### 9.1.2.2 Migration

**Migrationsvorbereitung:**

Zu den Migrationsvoraussetzungen gehören alle Punkte die gewährleistet werden müssen, damit eine nachgelagerte Migration reibungslos durchgeführt werden kann. Folgende Punkte sind zu prüfen und / oder vorzubereiten:

- Sichern der Router-Konfiguration
- Überprüfen der Firmware
- Überprüfen des Betriebssystems
- Notieren der unter IPv6 zu konfigurierenden Parameter

Sichern der Konfiguration:

Die Konfiguration des Routers muss vor Änderungen oder Upgrades gesichert werden, ggf. in mehreren Versionsständen, um bei Fehlfunktionen ein Rollback auf einen funktionierenden Stand zu ermöglichen. Die Sicherung der Konfiguration ist auch für den Fall des Austauschs des Routers durchzuführen, da in der Regel die alte Konfiguration, ggf. mit Anpassungen, auf neue Systeme eingespielt werden können.

Überprüfen der Firmware:

Sollte die Firmware des Routers kein IPv6 unterstützen, gibt es folgende Möglichkeiten um die IPv6-Tauglichkeit des Routers zu gewährleisten:

- **Upgrade Firmware:** Die Firmware sollte, wenn es möglich ist, auf eine IPv6-taugliche Version aktualisiert werden.
- **Software (optional):** Ist es nicht möglich, die IPv6-Hardware-unterstützung durch eine Aktualisierung der Firmware zu gewährleisten, so sollte überprüft werden, ob die IPv6-Hardwareunterstützung des

Routers über Software emuliert werden kann[9]. Dies kann in Abhängigkeit vom Hersteller entweder über eine Installation von Patches oder durch die Aktualisierung des Betriebssystems sichergestellt werden.

- **Austausch:** Für den Fall, dass es nicht möglich ist die IPv6-Tauglichkeit des Routers durch das Aktualisieren der Firmware oder des Betriebssystems zu erreichen, ist der Router durch einen Dual-Stack-tauglichen Router zu ersetzen.

Überprüfen des Betriebssystems:

Sollte das Betriebssystem des Routers kein IPv6 unterstützen, so gibt es folgende Möglichkeiten um die IPv6-Tauglichkeit des Routers zu gewährleisten:

- **Upgrade Betriebssystem:** Das Betriebssystem sollte, wenn es möglich ist, auf eine IPv6-taugliche Version aktualisiert werden.
- **Patch:** Einspielen von Patches, über die der Funktionsumfang des Routers um IPv6-Tauglichkeit erweitert wird.
- **Austausch:** Ist es nicht möglich, die IPv6-Tauglichkeit durch ein Upgrade oder patchen des Routers zu gewährleisten, dann ist der Router gegen einen IPv6-tauglichen Router auszutauschen.

Notieren der für IPv6 auf dem Router zu konfigurierenden Parameter:

Netzwerk:

Das IP-Subnetz, in dem sich der einzelne zu migrierende Router befindet, sollte IPv6-tauglich sein, damit der Router über IPv6 erreichbar ist[10]. Dies umfasst andere Router, Switches, betroffene Appliances (FWs, IDS etc.), Server und Arbeitsplatzsysteme.

Folgende Werte müssen für den Router im IPv6-Adresskonzept und im IPv6-Netzwerkplan fixiert sein:

- IPv6-Präfixe der IPv6-Subnetze, die an dem Router angeschlossen sind.
- IPv6-Default Gateway
- IPv6-Adressen der Router-Interfaces
- Konfiguration von ggf. eingesetzten Routingprotokollen, z. B. BGP oder OSPF
- Cluster-IPv6-Adressen (virtuelle IP-Adressen (VIPs)) der Router-Interfaces für VRRP und HSRP

[9] Eine softwarebasierte Emulation hat im Vergleich zu einer hardwarebasierten Unterstützung eine wesentlich geringere Performanz beim Datendurchsatz.
[10] Anmerkung: Switche und Router sind die ersten Netzwerkknoten die IPv6 fähig gemacht werden sollten; vgl. Abschnitt 5.1.1.

- IPv6-Adresse der Managementschnittstelle
- VLANs für IPv6-Datenverkehr

VLANs:

Unter IPv6 sollten die gleichen VLANs verwendet werden wie unter IPv4. Der Hintergrund ist die einfachere Verwaltung und Handhabung des Netzwerkes, insbesondere im Zusammenhang mit Troubleshooting im Problemfall. Sollten andere VLANs unter IPv6 verwendet werden, sind diese zu definieren und zu notieren.

NTP:

Der NTP Server sollte über IPv6 erreichbar sein, bzw. die Namensauflösung für den NTP Server sollte unter IPv6 funktionieren.

**Durchführung der Migration:**

Bei der Migration eines Routers sind mehrere Schritte durchzuführen. Ein Teil dieser Schritte sind optional. Dies hängt davon ab, ob die Firmware und das Betriebssystem aktualisiert werden müssen und ob bestimmte optionale Parameter konfiguriert werden müssen. Folgende Schritte umfasst die Migration:

- Konfiguration der IPv6-relevanten Parameter
- Optional: Konfiguration zusätzlicher Parameter

Konfiguration der IPv6-relevanten Parameter:

Der Router ist mit folgenden Basis-Parametern zu konfigurieren:

- **Default Gateway:** Es ist ein IPv6-Default-Gateway zu konfigurieren
- **IPv6-Adressen:**
    - Netzwerkinterfaces: Für jedes zu verwendende Interface ist eine IPv6-Adresse aus dem zugehörigen Netzwerk zu konfigurieren.
    - Cluster-IP-Adressen der Netzwerkschnittstellen (optional): Für jedes Netzwerkschnittstellen-Paar ist die Cluster IPv6-Adresse zu konfigurieren.
    - Managementschnittstelle: Für die Managementschnittstelle ist eine IPv6-Adresse zu konfigurieren.
- **IPv6-Filter:** Analog zu bestehenden IPv4-Filtern sind äquivalente IPv6-Filter zu konfigurieren. Diese sollen unter Betrachtung des Gesamt-Kontexts (Netzwerk-Plan, Routing etc.) das selbe Sicherheitsniveau bieten wie unter IPv4.
- **VLANs:** Die VLAN-IDs sollten für IPv6 übernommen werden.

- **Routing:** In Abhängigkeit von den zu verwendenden Netzwerkprotokollen, z. B. OSPF und BGP4, sind diese für IPv6 zu aktivieren und konfigurieren.

Konfiguration zusätzlicher Parameter:

Sind für den Router weitere Funktionen wie z. B. Mobile-IP und das Monitoring über SNMP, NetFlow oder Syslog notwendig, die unter IPv6 verwendet werden sollen, dann sind diese zu konfigurieren.

#### 9.1.2.3 Prüfung des Ergebnisses

Nach Abschluss der Konfigurationsarbeiten sollte überprüft werden, ob alle vorgenommenen Einstellungen persistent sind. Dazu sollte der Router einmal neu gestartet werden. Bevor der Router neu gestartet wird, sollte die Konfiguration gesichert werden. Nach dem Neustarts des Routers ist zu überprüfen, ob

- das Firmware- bzw. Betriebssystem-Update[11] funktioniert hat (falls ein solches durchgeführt wurde),
- die Installation von Patches funktioniert hat (falls ein solches durchgeführt wurde)
- und ob die neue Konfiguration erfolgreich vom Router geladen werden kann.

Folgende Prüfungen müssen nach der Migration erfolgreich bestanden werden:

- **Managementschnittstelle**[12]**:** Der Zugriff auf die Managementschnittstelle des Routers über IPv4 und IPv6 muss überprüft werden:
  - Telnet: Der Router sollte über Telnet erreichbar sein, falls dies vor der Migration möglich war (prüfen ob das aus Sicherheitssicht wirklich gewollt ist!)
  - SSH: Der Router muss über SSH erreichbar sein.
  - HTTP(s): Ist der Router über HTTP(s) erreichbar.
  - SNMP: Der Router sollte über SNMP erreichbar sein.
  - Weitere Dienste: Für den Fall, dass weitere Dienste auf dem Router unter IPv4 verfügbar waren, sind die entsprechenden Tests nun für IPv4 und IPv6 durchzuführen.

[11] Bei Geräten (Appliances) wie Switchen und Routern ist das Betriebssystem im Allgemeinen ein Teil der auf dem nicht-flüchtigem Speicher abgelegten Firmware.
[12] In Abhängigkeit, ob diese Dienste unter IPv4 bereits zur Verfügung gestellt wurden. Zusätzlich ist zu Telnet anzumerken, dass es aus Sicherheitsgründen nicht mehr verwendet sollte.

- **IP-Adressen der Netzwerkinterface:** Die Netzwerkinterface des Routers sollten über ICMP abgefragt werden.
- **Routing:** Überprüfung des korrekten Routings durch traceroute / tracert und Ping.
- **Performance:** Durch einen Last-Test ist zu überprüfen, ob die Performance des Routers für den Dual-Stack-Betrieb ausreicht.
- **Parameter:** Die IPv6-relevanten Parameter, welche bzgl. des Anwendungszwecks definiert wurden, sind zu testen, z. B. ob der Router als IPv6-Home-Agent funktioniert (falls Mobile-IP aktiviert wurde).
- **NTP:** Es ist zu überprüfen, ob der Router den NTP-Server erreichen kann.
- **DNS:** Die Namensauflösung der Management-Schnittstelle des Routers unter IPv6 ist zu überprüfen(inkl. Reverse Lookup).

### 9.1.3 Sicherheitskomponenten

Unter dem Begriff „Sicherheitskomponenten“ sind verschiedene Hardware-Komponenten zusammengefasst:

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

Im Folgenden wird stellvertretend für die Sicherheitskomponenten die exemplarische Migration einer zustandsbehafteten Firewall aufgezeigt. Sollte die Firewall auch zusätzliche Funktionen erfüllen (z. B. als Endsystem oder Router aktiv sein), so müssen zusätzlich die Migrationsanforderungen der entsprechenden Geräteklassen betrachtet werden.

Auf die Migration von Intrusion-Detection/Prevention-Systemen wird hier wegen der Vielfalt der unterschiedlichen Ansätze nicht explizit eingegangen.

Firewalls sind Transitsysteme, d. h. sie leiten eingehende Datenpakete weiter, wenn diese als unbedenklich und erlaubt eingestuft worden sind.

Es gilt, dass die Funktionen und die Leistung einer IPv6-Sicherheitskomponente mindestens denen einer entsprechenden IPv4-Sicherheitskomponente in der konkreten Einsatzumgebung entsprechen müssen. Bei der Migration eines IPv4-Netzes sollte zunächst analysiert werden, welche Funktionen der IPv4-Sicherheitskomponenten auf IPv6-Sicherheitskomponenten verfügbar sein müssen, damit eine mindestens gleichwertige Funktionalität und Sicherheit beim Betrieb mit IPv6 gewährleistet ist.

Dies gilt auch in Bezug auf den Schutz der Firewall-Komponente selbst, d. h. auch die Firewall-Komponente muss im Dual-Stack-Betrieb einen Selbstschutz gewährleisten können, der mit dem in einer IPv4-Umgebung vergleichbar ist.

Im Folgenden werden die notwendigen Schritte detailliert aufgezeigt:

#### 9.1.3.1 Erfassung der IST-Situation

**Annahme:**

Im Netzwerk der ÖV ist eine IPv4-only Firewall i. d. R. als Hardware-Komponente vorhanden[13], die sich im produktiven Betrieb befindet. Die Firewall ist dafür zuständig Netzwerkübergänge abzusichern und den Netzzugriff zu beschränken. Dies erfolgt anhand von definierten Regelwerken unter Verwendung von Absender- oder Zieladresse und / oder Diensten und TCP/UDP-Portnummern. Dabei wird der durch sie fließende Datenverkehr überwacht und entsprechend der definierten Regelwerke blockiert oder durchgelassen. Zusätzlich besitzt eine Firewall eine Managementschnittstelle, über die sie verwaltet wird und über die sie in ein Monitoring eingebunden ist.

Die Firewall selbst besteht aus folgenden Komponenten:

- einer Routing-Engine, vgl. mit einem Router,
- einer Softwarekomponente, die Firewall-Funktionalitäten zur Verfügung stellt und
- evtl. einem Management-Server, über den die Regelwerke konfiguriert und auf die Firewall geladen (gepusht) werden.

Diese Komponenten werden bei der Migration als Einheit betrachtet.

**Ziel:**

Die Firewall soll im Dual-Stack-Betrieb die gleiche Performanz und die gleiche Sicherheit bzgl. des Netzwerks wie zuvor im IPv4-only Betrieb gewährleisten.

**Optional:**

Das Management der Firewall sollte über IPv6 möglich sein (z. B. via ssh, telnet, http(s), …). Zusätzlich sollte das Monitoring der Firewall über IPv6 möglich sein, z. B. über SNMP. Weitere optionale Funktionen, die eine Firewall unter IPv6 unterstützen sollte wie z. B. IDS / IPS-, ALG- und Anti-Malware-Funktionalitäten sind in Abhängigkeit vom Verwendungszweck zu definieren.

Bei einer Firewall ist die aktive Konfiguration zu dokumentieren, dies umfasst insbesondere die Netzwerkkonfigurationen, -Definitionen und die sich auf der Firewall aktiven Regelwerke. Zusätzlich ist der Netzwerk- und Patch-Plan

[13] Abgrenzung: Zusätzlich gibt es persönliche Firewalls, die auf Klienten- und Server-Systemen als zusätzliche Software installiert sind um den Zugriff auf diese Systeme zu kontrollieren.

(Netzwerk-Interface-Anschlussplan) zu analysieren und ggf. zu aktualisieren. Dabei sind folgende Informationen zu erfassen:

Netzwerk:

- Angeschlossene Netzwerkknoten (Server, Hosts, Switches, weitere Firewalls etc.)
- Angeschlossene Netzwerke (IP-Subnetze)
- Zuordnung von Interfaces zu angeschlossenen Netzwerkknoten (Port-Belegung)
- IPv4-Adressen der Interfaces
- Cluster IPv4-Adressen (virtuelle IP-Adresse (VIPs)), falls die Firewall redundant ausgelegt ist
- IPv4-Adresse der Management-Schnittstelle der Firewall
- Genutzte VLANs
- Routing:
    - Statische Routen
    - Verwendete Routing-Protokolle und ihre Konfiguration
- DHCP:
    - Relay-Funktion oder
    - DHCP-Server-Funktion

Firewall-System:

- Firewall-System-Aufbau:
    - 1-Tier-Modell: Stand-Alone Firewall (auch im Cluster), inkl. Management und Logging
    - Mehr-Tier-Modell: Firewall, Management-Server, Logging-Server
- Firewall-Regelwerke:
    - Regelwerke für die Absicherung der Netzübergänge
    - Regelwerke für NAT / PAT
    - Regelwerke für Authentifizierungen und Netzwerkzugriffe
    - Weitere Regelwerke für weitere Funktionen wie Anti-Malware-Scanning und ALG-Funktionen

Firmware:

- Typ des Betriebssystems (falls dies in der Firmware enthalten ist)
- Distribution (Name und Version)

Betriebssystem:
(falls dies nicht Teil der Firmware ist; z. B. bei PC-basierten Sicherheitskomponenten)

- Typ des Betriebssystems
- Distribution (Name und Version)

DNS:

- DNS-Name(n) der Firewall[14] (falls mehrere Einträge existieren), in der Regel der DNS-Name der Managementschnittstelle
- DNS-Namen der Netzwerkschnittstellen, falls diese einen DNS-Namen erhalten haben.

NTP:

- DNS-Name des NTP-Servers, der von der Firewall verwendet wird.

PKI (optional):

- CRL-Verteilungs-Server:
  - IP-Adresse
  - DNS-Name
- OCSP-Responder
  - IP-Adresse
  - DNS-Name

RADIUS / TACACS (optional):

- IP-Adresse
- DNS-Name

#### 9.1.3.2 Migration

**Migrationsvorbereitung:**

[14] Anmerkung: Es kann für jede Netzwerkschnittstelle einen DNS-Eintrag geben.

Zu der Migrationsvorbereitung gehören alle Punkte die gewährleistet werden müssen, damit eine nachgelagerte Migration reibungslos durchgeführt werden kann. Folgende Punkte sind zu prüfen und / oder vorzubereiten:

- Sichern der Firewall-Konfigurationen
- Überprüfen der Firmware
- Überprüfen des Betriebssystems
- Notieren der unter IPv6 zu konfigurierenden Parameter

Sichern der Konfiguration:

Die Konfigurationen der Firewall sind, bevor Änderungen an der Konfiguration oder Upgrades durchgeführt werden, zu sichern, ggf. in mehreren Versionsständen, um bei Fehlfunktionen ein Rollback auf einen funktionierenden Stand zu ermöglichen. Die Sicherung der Konfigurationen ist auch für den Fall des Austauschs des Firewall durchzuführen, da in der Regel die alte Konfiguration, ggf. mit Anpassungen, auf neue Firewall-Systeme eingespielt werden können.

Überprüfen der Firmware:

Sollte die Firmware der Firewall kein IPv6 unterstützen, gibt es folgende Möglichkeiten um die IPv6-Tauglichkeit der Firewall für einen Dual-Stack-Betrieb zu gewährleisten:

- **Firmware Upgrade:** Die Firmware sollte, wenn es möglich ist, auf eine IPv6-taugliche Version aktualisiert werden.
- **Software (optional):** Ist es nicht möglich, die IPv6-Hardware-unterstützung durch eine Aktualisierung der Firmware zu gewährleisten, so sollte überprüft werden, ob die IPv6-Hardwareunterstützung der Firewall über Software emuliert werden kann[15]. Dies kann in Abhängigkeit vom Hersteller entweder über eine Installation von Patches oder durch die Aktualisierung des Betriebssystems sichergestellt werden.
- **Austausch:** Für den Fall, dass es nicht möglich ist die IPv6-Tauglichkeit der Firewall durch das Aktualisieren der Firmware oder des Betriebssystems zu erreichen, ist die Firewall durch eine Dual-Stack-tauglichen Firewall zu ersetzen.

Überprüfen des Betriebssystems:
(falls dies nicht Teil der Firmware ist, z. B. bei PC-basierten Firewalls)

[15] Eine softwarebasierte Emulation hat im Vergleich zu einer hardwarebasierten Unterstützung eine wesentlich geringere Performanz beim Datendurchsatz.

Sollte das Betriebssystem der Firewall kein IPv6 unterstützen, so gibt es folgende Möglichkeiten um die IPv6-Tauglichkeit für einen Dual-Stack-Betrieb der Firewall zu gewährleisten:

- **Upgrade Betriebssystem:** Das Betriebssystem sollte, wenn es möglich ist, auf eine IPv6-taugliche Version aktualisiert werden.
- **Patch:** Einspielen von Patches, über die der Funktionsumfang der Firewall um IPv6-Tauglichkeit erweitert wird.
- **Austausch:** Ist es nicht möglich, die IPv6-Tauglichkeit durch ein Upgrade oder patchen der Firewall zu gewährleisten, dann ist die Firewall gegen eine IPv6-taugliche Firewall auszutauschen.

Überprüfen der Firewall-Software:

Die Firewall-Software, die für die eigentlichen Firewall-Funktionalitäten zuständig ist, muss IPv6-tauglich sein. Für den Fall, dass diese nicht IPv6-tauglich ist gibt es folgende Möglichkeiten die IPv6-Tauglichkeit für einen Dual-Stack-Betrieb herzustellen:

- **Upgrade Firewall-Software:** Die Firewall-Software sollte wenn möglich auf eine IPv6-taugliche Version aktualisiert werden.
- **Firewall-Software-Patch:** Einspielen von Patches, über die der Funktionsumfang der Firewall-Software um IPv6-Tauglichkeit erweitert wird.
- **Firewall-Austausch:** Ist es nicht möglich, die IPv6-Tauglichkeit durch ein Upgrade oder patchen der Firewall-Software zu gewährleisten, dann ist die Firewall gegen eine IPv6-taugliche Firewall auszutauschen.

Notieren der für IPv6 auf dem Router zu konfigurierenden Parameter:

Netzwerk:

Mindestens eines der IP-Subnetze, in dem sich die einzelne zu migrierende Firewall befindet, sollte IPv6-tauglich sein, damit die Firewall über IPv6 erreichbar ist. Dies umfasst andere Firewalls, Router, Switches, betroffene Appliances (weitere FWs, IDS etc.), Server und Arbeitsplatzsysteme. Folgende Werte müssen für die Firewall im IPv6-Adresskonzept und im IPv6-Netzwerkplan fixiert sein:

- IPv6-Präfixe der IPv6-Subnetze an die die Firewall angeschlossen ist.
- IPv6-Default Gateway
- Cluster-IPv6-Adressen
- IPv6-Adressen der Router-Interfaces
- IPv6-Adresse der Managementschnittstelle

- VLANs für IPv6-Datenverkehr

Firewall-Regelwerke:

Für die Migration einer Firewall ist insbesondere darauf zu achten, dass das auf der Firewall konfigurierte Regelwerk für den IPv4/IPv6-Dual-Stack-Betrieb erweitert werden muss. Im Einzelnen müssen IPv4-Regeln sinngemäß und funktionsgemäß dupliziert werden und mit den IPv6-Adressen der angeschlossenen, neuen IPv6-Subnetze versehen werden. Im Ergebnis müssen die neuen Regelwerke das gleiche Sicherheitsniveau unter IPv6 wie zuvor unter IPv4 gewährleisten.

Folgende Regelwerke sind für IPv6 zu definieren:

- Regelwerke für die Absicherung der Netzübergänge
- Regelwerke für Authentifizierungen und Netzwerkzugriffe
- Weitere Regelwerke für den Fall erweiterte Firewall-Funktionen: ALG, IDS, IPS, Anti-Malware

Bei der Regelwerksdefinition ist zu beachten, dass sich die IPv4-Regelwerke nicht immer 1:1 auf IPv6 Regelwerke übertragen lassen, da zum Beispiel bei IPv6 bestimmte ICMP-Pakete nicht mehr verworfen werden dürfen. Das Hauptaugenmerk muss darauf liegen, dass gleiche Sicherheitsniveau unter IPv6 zu gewährleisten, d. h. lässt sich eine Regel nicht 1:1 abbilden, so muss ein IPv6 Äquivalent gefunden werden.

Firewall-System-Komponenten:

Besteht eine Firewall aus mehreren Systemkomponenten, z. B. dedizierte Management und Logging-Server, dann müssen diese auch IPv6-tauglich sein, bzw. über AAAA-Records und IPv6 erreichbar sein

VLANs:

Unter IPv6 sollten die gleichen VLANs verwendet werden wie unter IPv4. Der Hintergrund ist die einfachere Verwaltung und Handhabung des Netzwerkes, insbesondere im Zusammenhang mit Troubleshooting im Problemfall. Sollten andere VLANs unter IPv6 verwendet werden, sind diese zu definieren und zu dokumentieren.

NTP:

Der NTP Server sollte über IPv6 erreichbar sein, bzw. die Namensauflösung für den NTP Server sollte unter IPv6 funktionieren.

PKI:

Root CA, SUB CA, CRL-Verteilungsserver und / oder die OCSP-Responder sollten, sofern sie verwendet werden, über AAAA-Records und IPv6-Adressen erreichbar sein.

RADIUS / TACACS:

Die RADIUS / TACACS-Server sollten, sofern sie verwendet werden, über AAAA-Records und über IPv6-Adressen

**Durchführung der Migration:**

Nachdem die Migrationsvorbereitung erfolgreich abgeschlossen wurde, kann man mit der Migration der Firewall fortfahren. Die Migration sollte schrittweise durchgeführt werden, wobei ein Teil der Schritte optional ist. Dies hängt davon ab, ob bestimmte optionale Parameter konfiguriert werden müssen. Folgende Schritte umfasst die Migration:

- Konfiguration der IPv6-relevanten Netzwerk-Parameter
- Konfiguration der IPv6-relevanten Regelwerke
- Optional: Konfiguration Verbindung zu Management-Server
- Optional: Konfiguration zusätzlicher Parameter

Konfiguration der IPv6-relevanten Parameter:

Der Router ist mit folgenden Basis-Parametern zu konfigurieren:

- **Default Gateway:** Es ist ein IPv6-Default-Gateway zu konfigurieren
- **IPv6-Adressen:**
    - Netzwerkschnittstellen: Für jedes zu verwendende Interface ist eine IPv6-Adresse aus dem zugehörigen Netzwerk zu konfigurieren.
    - Cluster-IP-Adressen der Netzwerkschnittstellen (optional): Für jedes Netzwerkschnittstellen-Paar ist die Cluster IPv6-Adresse zu konfigurieren.
    - Managementschnittstelle: Für die Managementschnittstelle ist eine IPv6-Adresse zu konfigurieren.
- **VLANs:** Die VLAN spezifischen Konfigurationen sind für IPv6 zu übernehmen.
- **Routing**:
    - Dynamisches Routing: In Abhängigkeit von den zu verwendenden Netzwerkprotokollen, z. B. OSPF und BGP4, sind diese für IPv6 zu aktivieren.

- Statisches Routing: Für den Fall das statisches Routing verwendet wird, sind die statischen IPv6-Routen zu konfigurieren.

Konfiguration der IPv6 relevanten Regelwerke:

Die für den IPv6 Datenverkehr relevanten Regelwerke sind zu konfigurieren und zu aktivieren.

Firewall-Management:

Wird die Firewall über einen Management-Server konfiguriert, so sind die entsprechenden Parameter zu konfigurieren, damit der Management-Server der Firewall auch unter IPv6 erreichbar ist.

Konfiguration zusätzlicher Parameter:

Sind für die Firewall weitere Funktionen wie das Monitoring über SNMP, NetFlow und Syslog notwendig, die unter IPv6 verwendet werden sollen, dann sind diese zu konfigurieren.

#### 9.1.3.3 Prüfung des Ergebnisses

Nach Abschluss der Konfigurationsarbeiten sollte überprüft werden, ob alle vorgenommenen Einstellungen persistent sind. Dazu sollte die Firewall einmal neu gestartet werden. Bevor die Firewall neu gestartet wird, sollte die Konfiguration nochmals gesichert werden. Nach dem Neustart der Firewall ist zu überprüfen, ob

- das Firmware- bzw. Betriebssystem-Update funktioniert hat (falls ein solches durchgeführt wurde),
- die Installation von Patches funktioniert hat (falls ein solches durchgeführt wurde),
- Die Installation oder das Patchen der Firewall-Software (falls solches durchgeführt worden ist),
- und ob die neuen Konfigurationen erfolgreich von der Firewall geladen werden kann.

Folgende Prüfungen müssen nach der Migration erfolgreich bestanden werden:

- **Managementschnittstelle:** Der Zugriff auf die Managementschnittstelle der Firewall über IPv4 und IPv6 muss überprüft werden[16]:
  - Telnet: Die Firewall sollte über Telnet erreichbar sein, falls dies vor der Migration möglich war (prüfen, ob dies aus Sicherheitssicht gewollt ist!).

[16] In Abhängigkeit davon, ob diese Dienste unter IPv4 bereits zur Verfügung standen.

- SSH: Die Firewall muss über SSH erreichbar sein.
- HTTP(s): Die Erreichbarkeit über HTTP(s) sollte gegeben sein.
- SNMP: Der Router sollte über SNMP erreichbar sein.
- Weitere Dienste: Für den Fall, dass weitere Dienste auf dem Router unter IPv4 verfügbar waren, sind die entsprechenden Tests nun für IPv4 und IPv6 durchzuführen.

- **IP-Adressen der Netzwerkinterface:** Die Netzwerkinterfaces der Firewall sollten zumindest über ICMP-Echo-Anfragen (ping) abgefragt werden. Dazu sollten eingehende ICMP-Echo-Anfragen auf die Firewall kurzfristig zumindest vorübergehend durch die Firewall-Regelwerke erlaubt werden.
- **Routing:** Überprüfung des korrekten Routings durch traceroute / tracert und ping.
- **Firewall-Regelwerk:** Die Firewall-Regelwerke sollten dahingehend überprüft werden ob sie funktionieren. Dazu sind gezielte Anfragen von verschiedenen IPv6-Adressen auf verschiedenen IPv6-Adressen unter Verwendung von verschiedenen Diensten durchgeführt werden. Hierzu empfiehlt sich der Einsatz eines Last-Generators.
- **Performance:** Durch einen Last-Test ist zu überprüfen, ob die die Performance der Firewall für den Dual-Stack-Betrieb ausreicht.
- **Parameter:** Die IPv6-relevanten Parameter, welche bzgl. des Anwendungszwecks definiert wurden, sind zu testen.
- **NTP:** Es ist zu überprüfen, ob die Firewall den NTP-Server erreichen kann.
- **PKI:** Von der Firewall sollten die Root-CA, Sub-CA, CRL-Verteilungsserver und der OCSP-Responder erreicht werden können (sofern vorhanden).
- **Radius / TACACS:** Der Radius / TACACS Server sollte weiterhin erreichbar sein.
- **DNS:** Die Namensauflösung der Management-Schnittstelle des Routers unter IPv6 ist zu überprüfen(inkl. Reverse Lookup).

### 9.1.4 DHCPv6

Die dynamische Konfiguration von IP Adressen und Basisinfrastruktur-diensten spielt in Netzwerken eine zentrale Rolle. Für diese Zecke existiert das Dynamic Host Configuration Protocol (DHCP). Es ermöglicht die automatische Konfiguration von Informationen, welche ein Host für die Kommunikation in einem Netzwerk benötigt. Im Gegensatz zu DHCPv4 kann über DHCPv6 jedoch kein Default-Gateway konfiguriert werden. Deshalb sind bei IPv6 zusätzliche Router Advertisements (RA) zwingend für die IPv6-Autokonfiguration der Hosts

notwendig. Jeder DHCPv6-Klient kann zur Kommunikation mit dem DHCPv6-Server anhand eines eindeutigen DHCP unique identifier (DUID) identifiziert werden. Die vergebenen IPv6-Adressen können entweder an Hand der DUID zugeordnet werden (für Server-Systeme), oder aus einem definierten Adresspool vergeben werden (für Arbeitsplatzsysteme). Bei der Adressvergabe findet eine Überprüfung der vergebenen IPv6 Adresse statt. Dadurch wird verhindert, dass IP-Adressen in einem IP-Subnetz doppelt vergeben werden. Beim Einsatz des DHCPv6-Protokolls wird zwischen den beiden Nutzungsarten stateful und stateless DHCPv6 unterschieden.

Stateful DCHPv6: Bei dieser Methode werden sowohl die IPv6-Adresse als auch die Informationen der Basisdienste (z. B. DNS-Server) auf dem Klienten per DHCP konfiguriert.

Stateless DHCPv6: Bei dieser Methode werden ausschließlich zusätzliche Informationen (Domainname, DNS-Server) klientenseitig konfiguriert. Die IPv6-Adresse des Klienten muss entweder statisch konfiguriert oder durch eine andere Methode (z. B. SLAAC, [RFC4862]) vergeben werden.

#### 9.1.4.1 Erfassung der IST-Situation

**Annahme:**

Im Netzwerk existiert bereits ein DHCPv4-Server, der die dynamische Konfiguration von IP-Adressen und Netzwerkdiensten für Computersysteme in der ÖV durchführt.

**Ziel:**

Die Hosts auf denen DHCP für IPv4 aktiviert ist, sollen auch unter IPv6 per DHCP(v6) konfiguriert werden. Der Host auf dem der DHCPv4 Server aktiv ist, soll auf Dual-Stack-Betrieb umgestellt werden und parallel als DHCPv6-Server arbeiten.

**Optional:**

Falls ein zentraler DHCP-Server eingesetzt wird, so muss die DHCP-Relay Funktion an Subnetzgrenzen unterstützt werden und aktiviert sein.

Es müssen alle aktiven DHCPv4-Server erfasst werden. Dabei sind die IP-Adressen der Hosts zu dokumentieren, die diesen Dienst bereitstellen. Weiterhin müssen die Informationen notiert werden, die durch DHCPv4 auf den Klienten konfiguriert werden. Beim Einsatz eines zentralen DHCP-Servers für mehrere Subnetze muss der DHCP-Relay-Agent zusätzlich erfasst werden.

#### 9.1.4.2 Migration

Bevor mit der Migration begonnen werden kann, muss ein IPv6 Adresskonzept vorliegen, und die betroffen Subnetze müssen Dual-Stack-fähig sein. Anschließend muss der Host des DHCPv6-Servers auf Dual-Stack umgestellt werden. Danach muss ggf. eine neue DHCPv6-Software für den Server installiert werden, bevor mit der Konfiguration begonnen werden kann. Dabei ist die

Auswahl der Software in Abhängigkeit von dem bei den Klienten eingesetzten Betriebssystem zu treffen. Vor der Konfiguration ist zu klären, in welcher Betriebsart (stateful, stateless) der Server betrieben werden soll. Im Falle von stateful DHCPv6 ist vorab zu entscheiden, ob die IPv6-Adressvergabe anhand der DUID oder durch den Einsatz von Adresspools vergeben wird.

Beim Einsatz eines DHCPv6-Servers müssen die entsprechenden Flags der Router Advertisements gesetzt werden, damit die gewünschte Methode der automatischen Konfiguration von Klienten verwendet wird (siehe auch [RFC5175]). Des Weiteren müssen die durch den DHCPv6-Server bereitzustellenden Informationen serverseitig konfiguriert werden. Hierbei kann es sich um den Domainnamen, die IPv6-Adresse des DNS-Servers, sowie Informationen zu weiteren Basisdiensten handeln.

#### 9.1.4.3 Prüfung des Ergebnisses

Nach erfolgreicher Konfiguration sollte der Host zunächst einmal neu gestartet werden. Anschließend ist zu überprüfen, dass:

- IPv4 und IPv6 Serveradressen korrekt vergeben werden
- der DHCPv6-Server auf der konfigurierten Adresse erreicht werden kann
- die Klienten die vorgesehenen Adressen erhalten
- die Klienten die IPv6-Verbindung aufbauen können
- alle Informationen auf den Klienten konfiguriert sind und Verbindungen zu den entsprechenden Diensten aufgebaut werden können

### 9.1.5 NTP-Server

Eine genaue lokale Uhrzeit auf den Systemen einer IT-Infrastruktur ist wichtig für das korrekte Funktionieren vieler zentraler Dienste in einer ÖV, wie z. B. Dateiserver, IP-Router und Sicherheitssysteme. Es wird daher empfohlen, einen lokalen Zeitserver im Intranet oder Rechenzentrum zu betreiben. Dieser Server stellt über NTP (Network Time Protocol) Zeit- und Datumsinformation für Klienten, Server und Appliances bereit.

Im Zuge einer Migration auf IPv4/IPv6-Dual-Stack-Betrieb muss gewährleistet werden, dass der NTP Server auch über IPv6 erreichbar ist. Hierfür müssen das IP-Subnetz des NTP-Servers, der NTP-Server-Host selbst und die Server-Software IPv6-tauglich sein und IPv6 aktiviert werden. Ferner sind vorhandene Firewall-Regeln für NTP zu überprüfen und falls nötig äquivalente Firewall-Regeln für NTP/IPv6 zu erstellen.

Für technische Aspekte der IPv6-Migration eines NTP Servers siehe in der IPv6-Leitlinie in diesem Dokument in Abschnitt 14.5.1 auf Seite 197.

### 9.1.6 DNS-Server

Domain-Name-System-Server (DNS-Server) bilden einen essenziellen Teil der IT-Infrastruktur, sowohl in der öffentlichen Verwaltung, wie auch im Internet im

Allgemeinen. Je nach konkreter Situation betrifft eine Migration eines DNS-Dienstes für eine ÖV DNS-Server in einem kommunalen bzw. Landes-Rechenzentrum, d. h. selbst betriebene DNS-Server und ggf. auch externe DNS-Server. Die folgenden Migrations-Schritte beschäftigen sich im Detail nur mit Servern der ÖV bzw. ihrer Rechenzentren. In den abschließenden Empfehlungen zu DNS werden zusätzlich auch Hinweise zu Anforderungen an externe DNS-Server genannt.

Analog zur Migration eines Webservers sollten auf der höchsten Ebene wiederum die folgenden Schritte betrachtet werden: (a) Erfassung der Ist-Situation, (b) Planung und technische Umsetzung der Migration und (c) Überprüfung des Erfolges von (b). Hinzu kommt bei DNS-Servern als Teil der Planung die Festsetzung bestimmter Regeln (engl.: policies), die z. B. bestimmen, in welcher Priorität IPv4- und IPv6-Adressen vom DNS-Server als Antwort ausgeliefert werden sollen.

Zentrale Aufgabe eines IPv4- oder IPv6-DNS-Servers ist es, textuelle Computernamen (engl.: host names), wie z. B. "fileserver.example.com" zu IPv4- und/oder IPv6-Adressen aufzulösen. Dabei ist bzgl. der IPv6-Tauglichkeit eines DNS-Servers zwischen den DNS-Datensätzen und dem verwendeten Netzwerk-Protokoll zu unterscheiden: Ersteres bezieht sich auf die Frage, ob der Server zu Anfragen von Klienten auch IPv6-Adressen in Form von AAAA-Datensätzen ausliefern kann. Die zweite Frage betrifft die technische Auslieferung dieser DNS-Antwort-Datensätze: Können DNS-Nachrichten sowohl über IPv4 als auch über IPv6 zum Server gesendet und von diesem versendet werden? Beides ist notwendig, aber nicht unbedingt korreliert: So kann sich ein Dual-Stack-Klient z. B. auch über IPv4 nach der IPv6-Adresse des Servers www.example.com erkundigen und über IPv4 die DNS-Antwort (eine IPv6-Adresse) genannt bekommen.

Für einen typischen DNS-Server, d. h. eine DNS-Server-Software, ist daher im Vorfeld der Migration eine ganze Reihe von Funktionen auf IPv6-Tauglichkeit zu überprüfen. Details dazu finden sich in [IPV6_PROFILE]. Im Falle eines zentralen Adressmanagement-Systems, welches gemeinsam verschiedene Server (z. B. DNS, DHCPv6 und ggf. Monitoring) verwaltet, muss dieses System durchgängig IPv4 und IPv6 unterstützen (bzgl. GUI, Programmcode, Datenbank-Definition).

Vor der Migration des DNS-Servers selbst sind die entsprechenden Netze umzustellen, d. h. es muss gewährleistet sein, dass (i) das Netz, in dem sich der DNS-Server befindet, IPv6 unterstützt, (ii) die Subnetze auf dem Weg zu den Klienten bzw. Arbeitsplatzrechnern IPv6 unterstützen und (iii) dass die Arbeitsplatzrechner selbst IPv6 unterstützen, und diese Funktionen auch aktiviert sind. Ferner ist darauf zu achten, dass alle Subnetze zwischen Klienten und Servern, für welche diese Klienten eine IPv6-Adresse erhalten, ebenfalls bereits IPv6-tauglich sind. Dies gilt insbesondere auch für Verbindungen innerhalb einer ÖV, also z. B. für den Zugriff vom Arbeitsplatz auf bestimmte ÖV-interne Server. Im Umkehrschluss ist darauf zu achten, dass bei DNS-Anfragen aus bestimmten Netzen noch kein AAAA-Datensatz mit einer IPv6-Adresse zurück geliefert werden darf. Dies ist z. B. immer dann der Fall, wenn ein Webserver einer ÖV bereits von extern über IPv6 erreichbar ist, dieser aber für interne Klienten noch

über IPv4 erreichbar ist. In diesem Fall muss (z. B. über „DNS Zone Files“) eine Konfiguration realisiert werden, bei der DNS-Anfragen von innen anders behandelt werden als solche von außen.

Im Zusammenhang mit IPv6 und DNS existiert ein typisches Fehlerbild, das sich bei Endnutzern durch sehr lange Ladezeiten von Webseiten bemerkbar macht. Dies kommt dadurch zustande, dass ein Klient, genauer gesagt sein Betriebssystem und der Browser, der Meinung sind, dass sie schon mit IPv6 durchgängig angebunden sind, aber nur intern mit IPv6 kommunizieren können. Dann fragen die Betriebssysteme beim Zugriff auf eine Webseite zunächst den AAAA-Record des DNS Eintrags ab und bekommen dann beim Zugriff auf diese IPv6-Adresse keine Antwort. Nach einem, abhängig vom Betriebssystem relativ langen, Timeout, wird dann doch versucht die Webseite unter IPv4 zu erreichen, was i. d. R. gelingt.

Google hat auf dieses Problem bereits reagiert und antwortet auf DNS Anfragen nur noch mit dem AAAA-Record, wenn die Anfrage auch unter IPv6 gestellt wurde. Dieser Workaround und das sogenannte Whitelisting ziehen allerdings weitere Probleme nach sich und sind deshalb nicht unumstritten.

Für Hinweise zur Migration und Konfiguration von DNS in einer Dual-Stack-IT-Infrastruktur siehe Abschnitt 14.2.3 „Namensauflösung (DNS)“.

## 9.2. Dienste und Server

### 9.2.1 Portal-Migration / Webserver-Migration

Dieser Abschnitt beschreibt die Migration eines über http/https erreichbaren Webservers / Portals in einer öffentlichen Verwaltung (bzw. Rechenzentrum) mit den dafür benötigten Schritten sowie einer Liste der zu beachtenden Fragen für eine möglichst reibungslose, transparente Umstellung auf Dual-Stack-Betrieb.

Je nach Situation der konkreten Verwaltung bietet sich entweder die Umstellung mit Hilfe eines vorgeschalteten Reverse Proxy Servers (siehe dazu Abschnitt 7.3.3) oder der native Dual-Stack-Betrieb des Servers an (für Grundlagen siehe Abschnitt 7.1.1). Diese Entscheidung hängt wesentlich von den Möglichkeiten der Infrastruktur des Webservers (LANs, Switches, Router, ggf. vorgeschaltete Load-Balancer) und deren IPv6-Unterstützung ab.

#### 9.2.1.1 Erfassung IST-Situation

**Annahme**:
Ein aktiver Webserver (Portal) ist vorhanden. Dieser ist im produktiven Betrieb und über seinen DNS-Namen und ggf. über seine IPv4-Adresse aus erreichbar.

**Ziel:**
Zusätzlich zu IPv4 soll dieser Webserver zukünftig über IPv6 erreichbar sein, ebenfalls unter seinem Namen und ggf. auch direkt über die (noch zu wählende) IPv6-Adresse. Ziel ist somit die Umstellung des Webservers auf Dual-Stack-Betrieb, d. h. die Erreichbarkeit per IPv4 und IPv6 im Parallelbetrieb.

**Optional:**
Optional sollte auch das Management des Webservers über IPv6 möglich sein (z. B. ssh-Zugang oder Abfrage möglicher SNMP-Agenten auf dem Host über IPv6).

Als erstes muss das aktuelle Setup und die Konfiguration des Webservers dokumentiert werden. Dies ermöglicht es, einen schnellen Überblick über evtl. auftretende Abhängigkeiten zu erhalten. Grundsätzlich müssen bei der Erfassung folgende Bereiche betrachtet werden:

Zum einen die netzspezifischen Parameter in der sich der Webserver befindet: Dazu zählen Netzmaske, Routen, DNS sowie Sicherheitskomponenten die sich zwischen Webserver und dem Gateway-Router befinden. Zum anderen die hostspezifischen Parameter: Darunter sind das Betriebssystem, IP-Adressen und die Webserver Anwendung selbst zu verstehen.

Weitere Details zur Erfassung der Webserver-Konfiguration in tabellarischer Form enthält die Checkliste Webserver in Anhang I: IPv6-Migrations-Checklisten ab Seite 164.

#### 9.2.1.2 Migration

Bevor mit der eigentlichen Migration des Webserver begonnen werden kann, müssen zunächst folgenden Randbedingungen erfüllt sein. Um den Webserver via Dual-Stack verfügbar zu machen, ist es notwendig, dass am Standort des Servers (ÖV oder RZ) ein IPv6-Zugang vom / zum ISP vorhanden ist. Weiterhin wird die IPv6-Unterstützung durch die Switches, Router und andere Appliances (z. B. Firewall) am Standort des Servers vorausgesetzt. Details auch hierfür sind in den Checklisten in Anhang I zu finden.

Das IP-Subnetz, in dem sich der Webserver befindet (typischerweise ein DMZ-Netzwerk) muss IPv6-tauglich sein. Dies betrifft Switches, Router und ggf. andere Appliances, die das Netzwerk des Webservers mit anderen Netzwerken verbinden.

Weitere Voraussetzung ist ein vorhandenes IPv6-Adresskonzept, welches zusätzlich die Methode der IPv6 Adressvergabe definiert.

Für das vorhandene Betriebssystem ist zu prüfen:

- Wird IPv6 von diesem Betriebssystem (Distribution, Version, ggf. Kernelversion) unterstützt? (Informationen dazu sind im Profildokument [IPv6_PROFILE] im Anhang „Softwarelisten“ zu finden).
    - Falls nein, ist ein Betriebssystem-Upgrade einzuplanen.
- Ist IPv6 aktuell auf dem gewählten Server aktiviert?
    - Falls nein, muss IPv6 aktiviert werden (Konfiguration des Rechners anpassen, ggf. IPv6 Modul laden)

- Falls es sich um ein virtuelles System handelt: Wird IPv6 vom darunter liegenden Virtualisierer bzw. Hypervisor für die Gast-Systeme unterstützt? Vmware, der Microsoft HyperV und auch Citrix unterstützen IPv6 bereits relativ weitgehend, bei Virtual Box ist der IPv6 Support dagegen noch sehr begrenzt.

Folgend ist zu entscheiden, wo diese Adresse eingetragen wird, entweder:

a) durch statische Konfiguration auf dem Webserver Host selbst, oder

b) durch Konfiguration auf dem für das Netzwerk des Webservers zuständigen DHCPv6 Server und Einschalten von statischer IPv6 Adressvergabe auf diesem DHCP Server, oder

c) durch Konfiguration in einem ggf. vorhandenen zentralen IP Adress-Management Systems (s. a. Abschnitt 6.4)

Für die webserver-relevante DNS Konfiguration sollten folgende Punkte beachtet werden:

a) Der für die Domain zuständige DNS Server (engl.: Authorative DNS Server) muss die Speicherung, Abfrage und Auslieferung von IPv6-Adressen in Form von AAAA Datensätzen unterstützen.

b) Der externe DNS Name des Servers / Portals sollte für den Zugriff über IPv6 dem bisher verwendeten IPv4-Namen entsprechen, z. B. www.<domainname>

c) Der im internen DNS eingetragene Server-Name sollte gleich dem für IPv4 verwendeten Namen sein.

d) Der für die Domain zuständige DNS Server sollte auch selbst per IPv6 erreichbar sein, um Anfragen von Klienten aus IPv6-Inseln und „IPv6-only“-Netzwerken beantworten zu können.

Für weitere Details siehe Abschnitt 14.2.3 über DNS-Server und im Handbuch der entsprechenden DNS Server Software.

Sollte ein SSL-Server-Zertifikat verwendet werden, sollte dies einer Nutzung mit IPv6 nicht durch inkompatible Einträge im Weg stehen, z. B. durch Einträge für OCSP-Responder oder CRL-Download Adressen, welche nur unter IPv4 erreichbar sind.

Die Webserver-Anwendung und der Web-Server-Host muss IPv4/IPv6-Dual-Stack unterstützen (siehe dazu [IPV6_PROFILE] im Abschnitt über Endsysteme und Knoten). Hierfür ist u. U. ein Update der Webserver-Anwendung und/oder des Betriebssystems auf dem Server notwendig.

Weiterhin muss die Webserver-Anwendung entsprechend konfiguriert werden, um über IPv6 neue TCP/http(s)-Verbindungen akzeptieren zu können. Bei mehreren gehosteten Domains sind zumeist auch die dafür verwendeten vHost-

Einträge des Webservers anzupassen. Bitte konsultieren Sie dazu das Handbuch zur entsprechenden Webserver-Anwendung.

*Hinweis*: Ggf. vorhandene IP-Adressen-basierte Regeln, welche direkt auf dem Webserver konfiguriert sind müssen für IPv6 sorgfältig nachgebildet werden. Es könnten z. B. auf dem Webserver einzelne Verzeichnisse nur für Anfragen von internen IP-Adressen freigeschaltet worden sein.

#### 9.2.1.3 Prüfung des Ergebnisses

Der Webserver-Host muss nach Abschluss aller Konfigurationsarbeiten neu gestartet werden. So wird durch die folgenden Tests auch geprüft, ob alle vorgenommenen Einstellungen persistent sind, also nach einem Systemstart wieder korrekt vom System verwendet werden.

Folgende Prüfungen müssen nach der Migration erfolgreich bestanden werden:

- Zugriff auf den Webserver mittels eines Webbrowsers, in jeder Kombination von:
- IPv4-only-Klient / IPv6-only-Klient / Dual-Stack-Klient
- Von Extern („über das Internet“) und von Intern (Intranet)
- Mit den wichtigsten Browsern (Internet Explorer, Firefox, Chrome, Opera, Safari, …)
- Mit den wichtigsten Betriebssystemen (Microsoft Windows, Apple iOS, verschiedene Linux/UNIX-Distributionen, …)
- Für jede von dem Webserver gehostete Domain
- Für mehrere wichtige URLs („/“ und ausgewählte Unterverzeichnisse; ggf. „Crawler“ nutzen)

Die Performance des Portals/Webservers sollte überprüft (IPv4-only, IPv6-only, Dual-Stack-Klient) werden.

Ferner sollten die o. g. Tests mit Netzwerktools (ping, traceroute, etc.) immer mit expliziter Angabe der Protokoll-Version gemacht werden, damit nicht dem Tool überlassen wird, ob es die Verbindung über IPv4 oder IPv6 aufbaut.

### 9.2.2 Migration des E-Mail-Service

Mailserver gehören zum kritischen Teil einer IT-Infrastruktur, weil essentielle Geschäftsprozesse oft nicht mehr ohne die E-Mail-Infrastruktur funktionieren.

E-Mail-Serversysteme in Form von POP3-Servern, IMAP-Servern, SMTP-Servern und Mail Transfer Agents (MTA) müssen im Intranet und z. T. nach extern mit den Mailservern anderer Domänen kommunizieren können. Dies geschieht über Anwendungsprotokolle, welche über TCP/IP Daten austauschen.

Zum Austausch von E-Mails zwischen verschiedenen Domänen werden die Nachrichten direkt zwischen den zugehörigen MTAs über TCP/IP übertragen. Die verwendeten Protokolle zum Austausch von E-Mail-Nachrichten sind nicht abhängig von der IP-Version, jedoch entsteht ein Problem, wenn E-Mails zwischen einer IPv4-only- und einer IPv6-only-Domäne ausgetauscht werden müssen.

Da IPv4 und IPv6 nicht kompatibel zueinander sind, kann zwischen IPv4-only-MTA und IPv6-only-MTA keine direkte IP-Kommunikation stattfinden und E-Mails können nicht zugestellt werden. IPv6-only-Domänen sind insbesondere im asiatischen Raum bereits verbreitet, und ihre Anzahl wird international weiter zunehmen. Es ist daher ein entscheidendem Vorteil, den eigenen Mail-Server – zumindest für die externe Kommunikation – auf Dual-Stack-Betrieb umzustellen.

Davon betroffen ist in erster Linie die Kommunikation für den E-Mail-Austausch selbst. Es sollten jedoch bei dieser Migration nach Möglichkeit auch die Server-Schnittstellen für Management und Logging auf Dual-Stack-Betrieb umgestellt werden.

Ein weiterer wesentlicher Punkt, der mit der Nutzung von IPv6 für E-Mail einhergeht, ist der Wegfall bestimmter Parameter, die unter IPv4 für Plausibilitäts-prüfungen auf Spam-Filtern genutzt wurden. Deshalb besteht die Befürchtung, dass sich das Spam-Aufkommen in den Postfächern der Endnutzer mit der weiteren Verbreitung von IPv6 erhöhen könnte. Bisher hat sich dies nicht bestätigt.

#### 9.2.2.1 Erfassung der IST-Situation

Die notwendigerweise zu erfassenden Netzwerk- und Host-Parameter für die Migration entsprechen denen, welche auch für eine Webserver-Migration notiert werden müssen. Für Details siehe die Migrations-Checkliste Webserver.E ab Seite 164 in diesem Dokument. Analog zur Webserver-Migration sind hier die Version, Fähigkeiten und die Konfiguration des Mailservers zu notieren.

#### 9.2.2.2 Migration

Die Reihenfolge der Migrationsschritte für einen Mailserver, dessen Host und dessen Netzwerk ist analog zur Migration eines Webservers. Im Wesentlichen besteht diese aus:

1) WAN-Zugang
2) IP-Subnetzen zwischen Zugangs-Router und Mailservernetz
3) Mailserver-Host
4) Mailserver-Software
5) AAAA-Records für den Mailserver auf dem – ebenfalls IPv6-tauglichen – DNS-Server hinzufügen

Hinweis: Bei einem MTA ist insbesondere darauf zu achten, dass auch die **Reverse DNS-Auflösung** für IPv4 und für IPv6 korrekt funktioniert, denn diese

wird maßgeblich zur Verifikation der Identität von Mailservern untereinander genutzt. Unter IPv6 gilt dies allerdings nur noch eingeschränkt.

#### 9.2.2.3 Prüfung des Ergebnisses

Zur Überprüfung der korrekten Funktion des nun im Dual-Stack-Betrieb aktiven Mailservers sind die folgenden Tests empfohlen:

- Versand/Empfang von E-Mails an/von eine IPv4-only-Maildomäne
- Versand/Empfang von E-Mails an/von eine IPv6-only-Maildomäne
- Versand/Empfang von E-Mails an/von eine Maildomäne, die ebenfalls im Dual-Stack-Betrieb arbeitet

Es sollten während der Tests ständig die Logfiles des Mailservers überwacht werden und ggf. ist der Loglevel zu erhöhen. Ferner kann es sinnvoll sein, mit einem Netzwerkmonitor, z. B. Wireshark, zu beobachten, welche IP-Verbindungen tatsächlich aufgebaut werden.

### 9.2.3 VPN-Zugang

Bei Verwendung eines Virtual Private Network (VPN) sind folgende Fragen zu klären:

- Handelt es sich um ein VPN für Klienten oder eine LAN-zu-LAN-Kopplung?
- Soll/muss eine Verschlüsselung verwendet werden? Kann diese auch auf IPv6-Datenpakete angewendet werden?
- Soll oder muss der VPN-Datenverkehr *über* IPv4 und/oder IPv6 transportiert werden?
- Soll oder muss IPv4 und/oder IPv6 Datenverkehr *in* dem VPN transportiert werden?
- Sind andere Transportmechanismen involviert, z. B. VPN über MPLS-Netze?
- Können für den Transport – inklusive der zusätzlichen Daten (engl.: Overhead) für Verschlüsselung und VPN-Tunnel – genügend große Datenpakete übertragen werden? (Maximum Transmission Unit (MTU) ist zu prüfen und ggf. einzustellen)

### 9.2.4 Virtualisierung

Bei Betrieb von Diensten in einer Virtualisierungsumgebung ist darauf zu achten, dass auch diese Umgebung (z. B. VMware, XEN, KVM, Citrix, VirtualBox) Dual-Stack-tauglich ist und der Dual-Stack-Betrieb aktiviert ist.

Optimaler Weise sollte auch das Management der Virtualisierungslösung über IPv4 und IPv6 erfolgen können.

Falls in diesem Speicherplatz über ein IP-Netzwerk zur Verfügung gestellt wird (siehe Abschnitt 9.2.5), so sollten auch die dafür genutzten Server IPv4/IPv6-Dual-Stack unterstützen.

### 9.2.5 Dateiserver und Storage

Insbesondere in Rechenzentren werden zur Bereitstellung von gemeinsam nutzbaren Dateiablagen oder zur Bereitstellung von Speicherplatz für virtuelle Maschinen dedizierte Storage-Server genutzt, die diesen Speicherplatz über IP-Datennetze verfügbar machen. Dazu zählen:

- Dateiserver (file server) und Network Attached Storage (NAS)
    - stellen Datei-basierten Speicher zur Verfügung
    - nutzen Protokolle wie SMB/CIFS und NFS
- Storage Area Networks (SAN)
    - stellen Block-basierten Speicher zur Verfügung
    - bauen zumeist auf iSCSI [RFC3720], Fibre Channel (FC) oder Fibre Channel over Ethernet (FCoE) auf

Bei Einsatz dieser Systeme und Zugriff durch IPv6-Endsysteme ist zu gewährleisten, dass diese Server-Systeme ebenfalls IPv6-tauglich sind, d. h. per IPv6 angesprochen werden können.

Bei SANs betrifft dies nicht nur den Host und die Netzwerkumgebung, sondern auch den eingesetzten Host-Bus-Adapter (HBA), da dieser netzwerkseitig mit einem Switch der IT-Infrastruktur kommunizieren muss.

### 9.2.6 Public-Key-Infrastruktur

Public-Key-Infrastrukturen (PKI) bilden für Funktionen, die auf Zertifikaten beruhen einen wichtigen Teil einer Infrastruktur. Eine PKI ist ein System, mit dem digitale Zertifikate ausgestellt, verteilt und überprüft werden können. Die ausgestellten Zertifikate werden in der Regel zur Absicherung von Kommunikationsverbindungen und zur Authentifizierung verwendet. Eine PKI besteht aus mehreren Komponenten und besitzt eine hierarchische Struktur. In die Betrachtung bei einer Migration zu einem Dual-Stack-Betrieb sind

- Root Certification Authority (CA) online / offline,
- Sub CAs und die ausstellenden CAs,
- Sperrlisten-Verteilungspunkte (CDP) per LDAP und / oder Web,
- Zugriff auf CA-Information (AIA) per LDAP und / oder Web und optional
- OCSP-Responder (optional)
- Zertifikatsbeantragungs- und Verteilungs- API, z. B. PKCS#10
- Externe über Datennetze angebundene HSM-Module

mit einzubeziehen. Auf Grund der konkreten Strukturen der PKI, wie sie von den ÖV in Deutschland genutzt werden, betrifft dies je nach dem zu migrierenden PKI-Sever ggf. ein kommunales oder ein Landes-Rechenzentrum mit selbst betriebenen CA-Komponenten oder auch externe, außerhalb des Einfluss-bereichs der öffentlichen Verwaltungen, vorhandene CA-Komponenten.

Die externen Komponenten werden nicht in die folgenden Migrations-Betrachtungen mit einbezogen, es wird vorausgesetzt, dass diese erreichbar sind.

Für Trustcenter, die zugelassen sind, die Qualifiziert Elektronische Signatur (QES) auszustellen, muss beachtet werden, dass im Rahmen einer Migration zu IPv6 eine erneute Teilzertifizierung notwendig werden kann.

#### 9.2.6.1 Ausgangssituation

Annahme:

In der ÖV befinden sich PKI-Komponenten. Diese sind im operativen Betrieb und sind über DNS unter IPv4 (A-Record) und direkt über IPv4 erreichbar. Dabei wird eine 2 stufige-PKI- Struktur betrachtet, die die in der Einleitung zu diesem Kapitel enthaltenen Komponenten Root CA, Sub / Issuing CA, CDP, AIA und OCSP-Responder enthält. Nicht betrachtet wird eine verteilte Infrastruktur bei der sich z. B. die Root CA und mehrere Sub CAs außerhalb des Einflussbereiches der zu betrachtenden ÖV befinden, z. B. bei einem Dienstleister. Es wird davon ausgegangen, dass externe Komponenten erreichbar sind, bzw. die Erreichbarkeit gewährleistet ist .

Ziel:

Die in der ÖV vorhanden PKI müssen dahingehend migriert werden, dass sie zusätzlich unter IPv6 und DNS unter IPv6 (AAAA-Record) erreichbar sind. Das Ziel ist somit die Umstellung auf einen Dual-Stack-Betrieb der in der ÖV vorhandenen PKI Komponenten.

Optional:

Das Management und Monitoring der PKI sollte unter IPv6 möglich sein, dies kann z. B. den Zugriff via ssh, rds/rdp und Monitoring z. B. über SNMP beinhalten.

#### 9.2.6.2 Migrationsplanung

In einer Grob-Migrationsplanung sind folgende Schritte durchzuführen:

**Erfassung der IST-Situation**

Bei allen PKI-Komponenten ist als erster Schritt eine Sicherung durchzuführen. Hierzu empfiehlt sich ein vollständiges Backup zumindest der Root CA und Sub CA . Folgende Eigenschaften, gegliedert nach Komponenten einer PKI, sind zu erfassen, dabei sind einige Komponenten optional und als entsprechend gekennzeichnet:

Root CA (Offline vs. Online) und Sub / Issuing CA:

- Netzwerk
    - IPv4-Adresse
    - IPv4 Präfix und Netzmaske
    - IPv4 Default Gateway Adresse
- Routing
- bestehende ACLs oder lokale Firewall-Einstellungen (iptables oder Windows-Firewall)
- DNS-Name
- Betriebssystem
    - Typ des Betriebssystems
    - Distribution (Name und Version)
    - Bei Nicht-Windows Systemen: Version des Betriebssystem-Kernels (`uname -a`)
- Aktivierte, bzw. deaktivierte Dienste des Hosts
- Anwendung
    - Verwendete Software für die Root CA (Programm-Name und Version)
- Konfigurationseinstellungen der PKI:
    - Name der PKI
    - Verwendete Algorithmen
    - CDP-Pfad
    - AIA-Spezifika i. d. R. nur für Sub CA und auch nur wenn eingetragen
    - Zertifikatsbeantragungs- und Verteilungs- API, z. B. PKCS#10
    - HSM-Modul

CDP:

Hierbei handelt es sich um den Ort an dem die CRLs (Certificate Revocation List) gespeichert werden. Dieses kann sowohl ein LDAP-Verzeichnis (z. B. Active Directory) als auch ein Web-Server sein.

- LDAP: Der LDAP-Pfad ist zu erfassen.
- Web-Server: Die URL der CRL ist zu erfassen.

AIA (in der Regel nur für SUB-CA):

Über die AIA (Authority Information Access) wird definiert wie weitere Informationen und Dienste der ausstellenden CA genutzt werden können. Es können weitere Informationen über die CA enthalten sein oder ein Verweis auf einen Validierungsdienst / OCSP-Responder (vgl. Punkt OCSP-Responder). In der Regel ist in der AIA der Pfad zur nächsthöheren CA enthalten, bzw. der CRL der nächsthöheren CA. Dieser kann sowohl als LDAP-Pfad (z. B. Active Directory) als auch als URL enthalten sein:

- LDAP: Der LDAP-Pfad ist zu erfassen.
- Web-Server: Die URL der CRL ist zu erfassen.
- OCSP-Responder: Der Pfad unter dem der OCSP zu erreichen ist, ist zu erfassen.

OCSP-Responder (optional):

Der OCSP-Responder (Online Certificate Status Protocol) ermöglicht die Überprüfung der Gültigkeit von Zertifikaten in Echtzeit und wird als Serverdienst zur Verfügung gestellt. Hier sind die gleichen Werte wie bei einem Standard-Server zu notieren.

#### 9.2.6.3 Migration

Migrationsvoraussetzungen:

Zu den Migrationsvoraussetzungen gehören alle Punkte die gewährleistet werden müssen, damit eine nachgelagerte Migration der PKI-Komponenten reibungslos durchgeführt werden kann. In diesem Abschnitt werden nur die Voraussetzungen für die Root CA und die Sub / Issuing CA genannt, für die anderen Komponenten wird vorausgesetzt, dass diese erreichbar sind und für weitere Informationen auf die entsprechenden Abschnitte der relevanten Kapitel verwiesen:

- CDP:
  - LDAP, siehe auch Abschnitt 9.3.1.
  - Web-Server, siehe auch Kapitel 9.2.1 und 10.2.
- AIA:
  - LDAP
  - Web-Server
  - OCSP-Responder
  - Zertifikatsbeantragungs- und Verteilungs- API, z. B. PKCS#10
  - HSM-Modul

Netzwerk:

Das IP-Subnetz, in dem sich die zu migrierenden PKI-Komponenten befinden sollte IPv6 tauglich sein, damit die PKI-Komponenten über IPv6 erreichbar sind. Dies umfasst Firewalls, Router, Switches, betroffene Appliances (ALG, IDS etc.), Server und Arbeitsplatzsysteme. Folgende Werte müssen für die Firewall im IPv6 Adresskonzept und im IPv6 Netzwerkplan fixiert sein:

- IPv6-Netzmasken des Subnetzes in dem sich die Root CA befindet
- IPv6-Netzmasken des Subnetzes in dem sich die Sub/Issuing CA befindet
- Default Gateway Root CA
- Default Gateway Sub / Issuing CA
- IPv6-Adresse(n) der Root CA (mehrere für den Fall, dass es sich um ein Cluster handelt)
- IPv6-Adresse(n) der Sub / Issuing CA (mehrere für den Fall, dass es sich um ein Cluster handelt)
- IPv6-Default Gateway für die Root CA
- IPv6-Default Gateway für die Sub / Issuing CA
- Cluster-IPv6-Adresse der Root CA
- Cluster IPv6-Adresse der Sub / Issuing CA

DNS:

Der DNS-Server sollte IPv6 tauglich sein, bzw. mit AAAA-Records umgehen können.

NTP:

Der NTP Server sollte über IPv6 erreichbar sein, bzw. die Namensauflösung für den NTP Server sollte unter IPv6 funktionieren.

Migrationsvorbereitung:

Unter diesem Punkt sind die Vorbereitungen zu verstehen, die zu treffen sind, damit die Migration einer Root CA und / oder Sub / Issing CA durchgeführt werden kann. Folgende Punkte sind zu prüfen und / oder vorzubereiten.

Prüfen Migrationsvoraussetzungen:

Es ist zu überprüfen, ob die o. g. Migrationsvoraussetzungen gegeben sind.

Notieren der unter IPv6 zu konfigurierenden Parameter:

- Die Parameter die unter Voraussetzungen bzgl. des Netzwerks genannt werden sind zu notieren, so dass man diese bei der Migrations-

durchführung direkt vor Augen hat. Zusätzlich sind die IPv6-Adressen des DNS- und NTP-Servers zu notieren.

- Überprüfen des Betriebssystems:
- Die Betriebssysteme der Root CA und der Sub / Issuing CA ist dahingehend zu überprüfen ob es IPv6-tauglich ist. Sollten die Betriebssysteme nicht IPv6-tauglich sein, gibt es folgende Möglichkeiten u die die IPv6-Tauglichkeit für einen Dual-Stack-Betrieb zu gewährleisten:
- Upgrade Betriebssystem: Das Betriebssystem sollte, wenn es möglich ist, auf eine IPv6-taugliche Version aktualisiert werden.
- Patch: Einspielen von Patches, über die der Funktionsumfang der Firewall um IPv6-Tauglichkeit erweitert wird.
- Neu-Installation: Ist es nicht möglich, die IPv6-Tauglichkeit durch ein Upgrade oder patchen zu gewährleisten, dann ist bei der Migration eine Neu-Installation unter Verwendung eines IPv6 tauglichen Betriebssystems der jeweiligen zu migrierenden PKI-Komponente durchzuführen.

Überprüfen der PKI-Software / -Konfiguration:

In der Regel verwendet die PKI-Software zur Kommunikation die Parameter die über das zugrundeliegende Betriebssystem zur Verfügung gestellt werden. Das bedeutet, dass wenn das Betriebssystem IPv6 tauglich ist, dann gilt dies auch für die PKI-Software. Wichtiger ist die Konfiguration der PKI-Software. Hier ist zu überprüfen ob anstelle von DNS-Einträgen feste IPv4-Adressen konfiguriert sind, z. B. bei der Angabe von CDP-Standorten. Ist dies der Fall, ist es u. U. notwendig die PKI-Software unter Verwendung von DNS-Einträgen anstelle von IP-Adressen neu zu installieren und zu konfigurieren.

Sichern der Konfiguration (inkl. Schlüsselmaterial):

Die Konfigurationen der Root CA und der Sub / Issuing CA sind, bevor Änderungen an der Konfiguration oder Upgrades durchgeführt werden, zu sichern, hier empfiehlt sich ein Full Backup des gesamten Systems einschließlich des Betriebssystems. Das Schlüsselmaterial ist über eine sogenannte Schlüsselzeremonie zu sichern.

Durchführung der Migration

Bei den Migrationen von Root CA und Sub / Issuing CA sind mehrere Schritte durchzuführen. Ein Teil dieser Schritte ist optional. Dies hängt davon ab, ob das Betriebssystem und die Konfiguration der PKI-Software aktualisiert werden müssen und ob bestimmte optionale Parameter konfiguriert werden müssen. Folgende Schritte umfasst die Migration:

Optional: Upgrade / Patch / Neu-Installation des Betriebssystems:

Für den Fall, dass das Betriebssystem nicht IPv6 tauglich ist, sollte dieses durch ein Upgrade, das Installieren eines Patches oder durch die Neu-Installation einer IPv6 tauglichen Revision des Betriebssystems IPv6 tauglich gemacht werden.

Optional: Konfiguration / Neu-Installation der PKI-Software:

Die PKI-Software muss für den Fall, dass IPv4 Adressen anstelle von DNS Namen konfiguriert worden sind, ist die Konfiguration dahingehend zu ändern, dass die IPv4 Adressen gegen DNS-Namen ausgetauscht werden. Sollte es nicht möglich sein, dies durch einen einfachen Austausch zu gewährleisten, so ist eine Neu-Installation der PKI-Software durchzuführen. Bei der Installation sind DNS-Namen an den entsprechenden Stellen zu verwenden.

Konfiguration der IPv6-relevanten Netzwerk-Parameter:

Der Server auf dem die jeweilige PKI-Komponente installiert ist, ist mit folgenden Basis-Parametern zu konfigurieren:

- Default Gateway: Es ist ein IPv6-Default-Gateway zu konfigurieren
- IPv6-Adressen:
    - Netzwerkschnittstelle: Die IPv6-Adresse ist zu konfigurieren
    - Cluster-IP-Adressen der Netzwerkschnittstellen (optional): Handelt es sich um eine PKI-Komponente die im Cluster d. h. redundant, betrieben wird, so ist die Cluster-IP-Adresse zu konfigurieren.

#### 9.2.6.4 Prüfung des Ergebnisses

Nach Abschluss der Konfigurationsarbeiten muss überprüft werden, ob alle vorgenommenen Einstellungen persistent sind und die PKI-Dienste auf den jeweiligen Servern funktionieren, bzw. erreichbar sind. Dazu müssen der Root CA- und der Sub / Issuing-Server neu gestartet werden. Vor dem Neu-Start sollten die Konfigurationen der PKI-Dienste gesichert werden. der Server. Während des Neustarts der jeweiligen Server ist zu überprüfen, ob

- das Betriebssystem-Update (falls ein solches durchgeführt wurde) und / oder
- die Installation von Patches funktioniert hat (falls ein solches durchgeführt wurde).

Nach dem Neustart des jeweiligen Servers ist zu überprüfen ob die durchgeführten Konfigurationsänderungen, bzw. die Neu-Installation der PKI-Software gelungen sind.

Folgende Prüfungen müssen nach der Migration erfolgreich von der Root CA und der Sub / Issuing CA bestanden werden:

- IPv6-Adresse: Die Erreichbarkeit der IPv6-Adresse ist zu überprüfen. Dazu ist eine ICMP-Anfrage durchzuführen.
- Namensauflösung: Die Namensauflösung der PKI sollte getestet werden, dazu ist ein nslookup als forward und reverse lookup durchzuführen.
- Management / Monitoring (optional): Bei einem Monitoring über SNMP sollte die jeweils relevanten Parameter abgefragt werden.
- CDP: Es ist zu überprüfen ob der /die CDP erreichbar ist und ob dort die CRLs hinterlegt werden können.

### 9.2.7 ALG / Proxies

Application Level Gateways (ALG) und Proxy-Systeme müssen ebenfalls IPv6-tauglich sein, und die IPv6-Unterstützung muss aktiviert sein, sofern das IPv6 Protokoll genutzt werden soll. Da Proxy-Systeme u. U. eine Protokollumsetzung vornehmen, ist bei diesem Systemen darauf zu achten, „auf welcher Seite“ IPv6-Unterstützung benötigt wird: Nur innen, nur außen oder auf beiden Seiten.

Es kann zum Beispiel bei einer Teilmigration (siehe Abschnitt 5.1.3) vorkommen, dass nach außen durch den Proxy Zugriff auf IPv4- und IPv6-Netze möglich sein soll, nach innen aber nur IPv4-Klienten unterstützt werden sollen. Dies muss sich in der Konfiguration des Proxy auch konkret wiederspiegeln.

## 9.3. Protokolleigenschaften

Dieser Abschnitt beschäftigt sich mit einem Querschnitt an Basis- und Server-Diensten in einer ÖV und der Frage, wie stark diese durch eine Umstellung auf IPv6 oder auf IPv4/IPv6-Dual-Stack-Betrieb betroffen sind.

Für alle Dienste gleichermaßen stellt sich zuerst die Frage, ob sie betroffen sind. Wird zum Beispiel im Rahmen einer Teilmigration einer ÖV deren Web-DMZ auf Dual-Stack umgestellt, so muss in Konsequenz auch ein DNS-Server der ÖV umgestellt werden, jedoch nicht zwangsläufig auch ein Mailserver der ÖV.

Steht fest, dass ein Dienst migriert werden soll, so betrifft dies in jedem Fall auch immer:

- Das IP-Subnetz, in dem dieser Dienst angeschlossen ist
- Das Betriebssystem des Computers/der Appliance, auf der der Dienst aktiv ist
- Die Anwendung, die den Dienst bereit stellt
- Eine ggf. vorhandene Management- und Monitoring-Anwendung für diesen Dienst
- Sicherheitskomponenten zwischen Dienst und dessen Nutzern

Man kann bzgl. der Dienste-Migration zu Dual-Stack zwischen „einfachem“ und „komplexem“ Fall unterscheiden:

- Im einfachen Fall muss die Anwendung, die den Dienst realisiert nur zusätzlich zu IPv4 auch auf IPv6 auf Anfragen reagieren können (technisch: auch an einem IPv6-Port lauschen)

- Im komplexen Fall müssen zusätzlich zum einfachen Fall Anpassungen an der Anwendung und/oder von ihr genutzter Datenstrukturen (z. B. Datenbankeinträge) vorgenommen werden. Dies ist im Einzelfall zu analysieren und zu planen.

### 9.3.1 Dienste mit “einfachem” Protokoll

Als einen Dienst mit einem “einfachen” Protokoll bezeichnen wir im Zuge der Migration solche Dienste, deren Anwendungsprotokoll selbst keine Abhängigkeit von der verwendeten IP-Version im Netzwerk beinhaltet.

Technisch gesehen betrifft dies die Frage, ob *innerhalb* des Anwendungsprotokolls IP-Adressen auftreten können. Ist dies *nicht* der Fall, so lautet die entscheidende Frage für die Migration des Dienstes: Kann die Anwendung, welche den Dienst bereitstellt, so konfiguriert werden, dass sie neben IPv4 auch auf ankommende Anfragen über IPv6 reagiert? (oder gibt es eine neuere Version der Anwendung, die dies unterstützt?)

Zur Umstellung ist dann (nach der Migration der Infrastruktur und des Hosts) für die Anwendung zumeist eine „Listen“-Direktive in der Konfiguration der Anwendung umzustellen, so dass sowohl an einer IPv4-Adresse als auch an einer IPv6-Adresse auf Anfragen gewartet wird (üblicherweise auf dem gleichen Port). Für einen Webserver ist diese Umstellung in den Abschnitten 9.2.1 und 10.2 im Detail beschrieben.

Für Anwendungen/Dienste folgender Protokolle kann dieser einfachere Fall angenommen werden:

- LDAP
- SMB, NFS, CIFS
- Druckdienste (z. B. CUPS)
- Zugriff auf Datenbankserver
- SMTP / POP3 / IMAP
- SNMP
- iSCSI / Fibre Channel
- NTP
- DNS

### 9.3.2 Dienste mit “komplexem” Protokoll

Bei im Hinblick auf die Migration komplexeren Protokollen kommt es vor, dass IP-Adressen als Daten innerhalb dieser Protokolle übertragen werden. In diesem

Fall können sich im IPv6-only oder Dual-Stack-Betrieb Probleme ergeben, falls z. B. die IPv4-Adresse eines Endsystems über das Protokoll signalisiert wird, der Kommunikationspartner versucht, per IPv6 auf den Dienst zuzugreifen. Probleme dieser Art können immer dann auftreten, wenn über ein solches Protokoll dem Kommunikationspartner die *eigene* IP-Adresse übermittelt wird, damit dieser in der Gegenrichtung eine Verbindung aufbauen kann.

Bei diesen Protokollen sind in Folge der Migration genaue Prüfungen notwendig, um die korrekte Funktionalität zu gewährleisten, z. B. eine Analyse der tatsächlich zwischen den Kommunikationsendpunkten übertragenen Datenströme und übermittelten Parameter.

Folgende Protokolle und deren Dienste fallen in diese Kategorie:

- File Transfer Protocol (FTP)
- Session Initiation Protocol (SIP)
- Extensible Messaging and Presence Protocol (XMPP)
- Hypertext Transfer Protocol (http/https)
- einige Remote Procedure Call (RPC) Protokolle

*Hinweis*: Bei http / https *kann* eine alphanumerische IP-Adresse als Parameter innerhalb des Protokolls übertragen werden. Dies ist jedoch auch beim Dual-Stack-Betrieb kein Problem, das es sich um eine *Ziel*-IP-Adresse handelt und nicht wie oben angemerkt um die *eigene* IP-Adresse.

## 9.4. Routing-Protokolle

Innerhalb dieses Unterabschnitts werden Sicherheitsaspekte dargestellt, die sich durch den Einsatz der verschiedenen Routing-Protokolle ergeben, die unter IPv6 verwendet werden können.

Für IPv6 müssen z. T. neue Routing-Protokolle (oder eine neuere Version eines vorhandenen Protokolls) genutzt werden, da viele der aktuell für IPv4 eingesetzten Routing-Protokolle nicht für IPv6 genutzt werden können.

Bei den Routing-Protokollen wird in der Regel unterschieden zwischen Interior-Gateway-Protokollen (IGP) und Exterior-Gateway-Protokollen (EGP). Der wichtigste Sicherheitsaspekt im Zusammenhang mit IP-Routing ist die Gewährleistung der Integrität des Datenverkehrs zwischen zwei Routing-Instanzen.

### 9.4.1 IGP

Im Folgenden werden kurz die sicherheitsrelevanten Aspekte der einzelnen IGP dargestellt:

- **RIPng**: Die Protokolldefinition von RIPng sieht im Gegensatz zur Protokolldefinition von RIP keine Gewährleistung der Integrität vor. Aus

diesem Grund wird in [RFC2080] IPsec zur Absicherung von RIPng festgelegt.

- **OSPFv3**: In der Protokolldefinition zu OSPFv3 ist die Verwendung eines Hash-Algorithmus zur Gewährleistung der Integrität nicht enthalten. Für OSPFv3 muss daher ebenfalls IPsec zur Gewährleistung der Integrität und Authentizität nutzen.
- **IS-IS**: IS-IS verwendet den Hash-Algorithmus MD5 zur Sicherung der Integrität von Routing-Updates. Weitere Sicherheitsmechanismen sind nicht vorgesehen.
- **EIGRP**: EIGRP verwendet den Hash-Algorithmus MD5 zur Sicherung der Integrität von Routing-Updates. Weitere Sicherheitsmechanismen sind nicht vorgesehen.

Für den Einsatz in einer ÖV wird empfohlen, die genannten Sicherheitmechanismen zur Absicherung der Routing-Protokolle zu verwenden, d. h. IPsec bei RIPng und OSPF, bzw. MD5 bei IS-IS und EIGRP.

### 9.4.2 EGP

In Folgenden werden kurz die sicherheitsrelevanten Aspekte des EGP BGP-4 skizziert:

- **MD5**: Der Hash-Algorithmus MD-5 wird verwendet um die Integrität von Routing Updates zu sichern.
- **GTSM**: Über GTSM wird erreicht, dass „gespoofte“ BGP-Nachrichten verworfen werden. Dies wird unter Verwendung des Hop-Limits realisiert.
- **IPsec**: Durch die Verwendung von IPsec wird der Datenverkehr gesichert.

Für Präfixe aus dem Adressblock der LIR de.government wird der Mechanismus „RPKI“[17] eingesetzt, um das unautorisierte annoncieren von BGP Routen langfristig im Internet weltweit zu unterbinden.

Für den Einsatz in einer ÖV wird empfohlen die genannten Sicherheitsmechanismen zur Absicherung von BGP-4 zu verwenden.

## 9.5. Netzwerkmanagement und -monitoring

### 9.5.1 Netzwerkmanagement

In der heutigen IT-Landschaft einer Behörde oder eines Rechenzentrums stellen nicht nur Computer und Server, Router, Switches und Sicherheitskomponenten unverzichtbare Geräte mit Netzwerkschnittstellen dar. Ein effizienter und sicherer Betrieb der Infrastruktur ist ohne Netzwerkmanagementsysteme nicht möglich. Über das Netzwerkmanagement und -monitoring werden Vorgänge im Netz

[17] siehe https://en.wikipedia.org/wiki/Resource_Public_Key_Infrastructure und https://www.arin.net/resources/rpki.html

gesteuert und (zeitnah) sichtbar gemacht. Ohne ein Netzwerkmanagement und -monitoring würde man eine Netzwerkinfrastruktur quasi im „Blindflug“ betreiben.

Daneben gibt es noch zahlreiche „Nebendienste“ und „Geräte“, von Netzwerkdruckern bis zur Haustechnik, auf die im Folgenden ein Blick geworfen werden soll.

Das Netzwerkmanagement steht bei der Migration wie auch im Betrieb als eigener Arbeitsbereich neben dem eigentlichen Netzbetrieb. Netzwerkmanagement ist ein unverzichtbarer Bestandteil zur Konfiguration und zur Analyse des Netzes. Es muss daher frühzeitig in den Migrationsprozess zu IPv6 mit einbezogen werden. Dieses idealerweise in sich abgeschlossene System kann bspw. selbst noch auf IPv4 basieren aber schon IPv6-fähige Systeme kontrollieren und überwachen. Insofern ist beim Netzwerkmanagement zwischen dem Zugriff auf Geräte und den von diesen Geräten (z. B. Routern) behandelten Datenströmen zu unterscheiden.

#### 9.5.1.1 Ereignisverwaltung und Logging (syslog)

In mittleren und großen IT-Installationen/Rechenzentren werden standardmäßig zentrale Logserver verwendet, auf denen Log-Nachrichten anderer Dienste gesammelt und gespeichert werden. Dies ermöglicht die zentrale Sicherung und Auswertung von Nachrichten verschiedenster Dienste im eigenen Netzwerk (LAN).

Hierfür werden typischerweise Implementierungen von syslog, oder dem neueren syslog-ng verwendet. Dienste senden ihre Nachrichten hierfür standardmäßig über UDP/IP, Port 514. Die Basis für Syslog wurde 2001 in [RFC3164] und [RFC3195] definiert.

In einer IT-Infrastruktur mit Dual-Stack- oder IPv6-only-Systemen muss ein syslog Dienst Nachrichten ebenfalls per IPv6 empfangen können. Ferner sollte der Zugang zum syslog Server zum Zweck der Auswertung oder Abfrage gesammelter Log-Daten auch per IPv6 möglich sein, da dieser zumeist auch über das lokale Netzwerk erfolgt.

#### 9.5.1.2 Netzwerkmanagement und Alarmsignale

Sehr viele vorhandene Geräte – von Messgeräten bis hin zu Switches und Routern – lassen sich über das Simple Network Management Protokoll (SNMP, [RFC1157] und weitere) abfragen und zum Teil auch konfigurieren. Dazu ist auf dem Gerät ein sogenannter SNMP Agent aktiv, mit dem Managementsysteme Daten über den Zustand des Geräts austauschen können. Über sogenannte SNMP Traps kann ein SNMP-fähiges Gerät außerdem von sich aus Signale asynchron an das Management-System senden, z. B. um auf einen Alarm-Zustand aufmerksam zu machen.

In einer Dual-Stack-Umgebung muss ein Managementsystem, dass Geräte über SNMP abfragt, sowohl IPv4 als auch IPv6 zur Kommunikation nutzen können. Auf SNMP-fähigen Geräten in einer solchen Umgebung sollte der SNMP-Agent

zusätzlich zu IPv4 über IPv6 erreichbar sein (im Fall von IPv6-only-Netzen: muss).

Im Fall von IPv6-Geräten sollte geprüft werden, ob diese auch IPv6-spezifische Informationen per SNMP bereit stellen können (z. B. IPv6-Paket- und Byte-Zähler pro Netzwerkschnittstelle). Dazu ist es unter Umständen notwendig, weitere SNMP MIBs (Management Information Base; Datenbank) auf den Geräten zu aktivieren. Gegebenenfalls ist dazu auch zuerst die Router-Firmware zu aktualisieren.

Im IPv6-Profil für die öffentliche Verwaltung sind mehrere Standard-MIBs zur Verwaltung der Netzwerk- und Transportschicht aufgeführt. Allerdings spielen in diesem Bereich Hersteller-spezifische Lösungen eine große Rolle. Es ist daher bei der Migration zu prüfen, ob für die eingesetzten Geräte entsprechende IPv6-MIBs bereit stehen, so dass zu IPv4 vergleichbare oder bessere Informationen über den Netzzustand bereit stehen.

### 9.5.2 Monitoring

In größeren IT-Netzwerken kommen oft Geräte zum Netzwerkmonitoring zum Einsatz, in erster Linie, um das Verkehrsaufkommen in und zwischen den Netzen zu ermitteln. Das Monitoring kann aber auch installiert sein, um die Qualität der Datenübertragung zu ermitteln oder um die Nutzung bestimmter Dienste zu protokollieren (und hier Trends zu erkennen). Netzwerk-Monitoring in IP-Netzwerken wir zumeist von IP-Routern (Verkehrsaufkommen) und durch dedizierte Monitoringsysteme durchgeführt (letztere für komplexere Metriken oder zum Zweck der Abrechnung von Ressourcennutzung (Accounting)).

Es ist üblich, dass solche Systeme ihre Messdaten in regelmäßigen Abständen an weitere Systeme (Analyse, Datenbank) exportieren. Für den Export haben sich einige Standardprotokolle etabliert, z. B. sFlow [RFC3176], NetFlow [RFC3954] und IPFIX [RFC5101]. In einer Dual-Stack-Umgebung sollte der Export (Senden und Empfangen) von Messergebnissen über IPv4 und über IPv6 möglich sein. NetFlow unterstützt IPv6 ab der Version 9.

In den Datensätzen selbst können auch IP-Adressinformationen enthalten sein, was bedeutet, dass zukünftig dann auch Datenfelder für IPv6 vorhanden sein müssen. Wie bei den MIBs werden die entsprechenden Datensatzformate für das Monitoring zumeist durch die Hersteller zur Verfügung gestellt.

Eine weitere Herausforderung stellen die Speicherung und Darstellung von IPv6-Datensätzen dar. Hierbei ist zu beachten, dass die (im Vergleich zu IPv4 vierfach längere) IP-Adresse entsprechend größeren Speicherbedarf bzw. Platzbedarf in der Darstellung benötigt.

#### 9.5.2.1 Nachrichten-Weiterleitungen / Messaging

Eine dedizierte Betrachtung der IPv6-Tauglichkeit ist auch für in einer ÖV oder einem Rechenzentrum eingesetzte Messaging-Systeme notwendig, und zwar sowohl solche, die nur im Intranet eingesetzt werden, als auch ÖV- oder Standort-übergreifende Anwendungen. Dabei können je nach Anwendung auch

Zwischensysteme, z. B. Proxy-Server, betroffen sein. Einige Beispiele für mögliche Messaging-Systeme sind:

- Instant Message (z. B. Skype oder XMPP-basierte Systeme wie Jabber)
- Message-Gateway-Systeme (z. B. E-Mail nach SMS)
- Bei Nutzung von Voice-over-IP (VoIP) Telefonie
    - VoIP Endgeräte
    - VoIP Proxies
    - Gateways (z. B. Übergang zur ISDN-Telefonie)
- E-Mail (siehe Abschnitt 9.2.2)

Sofern es sich um kritische Systeme handelt, sollten vor einer möglichen Nutzung in einer Dual-Stack-Umgebung unbedingt unabhängige Labortests durchgeführt werden.

#### 9.5.2.2 Weitere IT-Systeme in IP-Netzwerken

Auf Grund des anhaltenden Trends, immer mehr technische Systeme mit IP-basierten Kommunikations-Schnittstellen auszustatten, finden vermehrt Geräte Anschluss an das Intranet/LAN, die früher andere, dedizierte Kommunikations-wege genutzt haben. Im Zuge der Nutzung von IPv6 ist auch für diese Geräte die Funktionstauglichkeit zu testen und weiterhin zu gewährleisten. Beispiele für solche Systeme sind:

- Netzwerk-Drucker
- externe Massenspeicher mit Netzwerkanschluss
- Sensor-Systeme
- Haus- und Alarmtechnik

Nicht immer ist bei diesen Systemen ein Upgrade der Firmware möglich, so dass ggf. sogar einige IPv4-Netzwerke noch auf sehr lange Sicht weiter bestehen müssen.

# 10. Praktische Migrationsbeispiele

Aufbauend auf der Migrations-Referenzarchitektur aus Abschnitt 3.6 wurden konkrete Migrationsbeispiele in Form von realistischen Szenarien durchgeführt. Diese Szenarien wurden für diesen Migrationsleitfaden in einem Testbed migriert. Sie dienten einerseits dazu, die in diesem Leitfaden enthaltenen Checklisten (siehe Anhang II) zu entwickeln, andererseits können diese Beispiele auch direkt als Vorlage für eigene Migrationsprojekte genutzt werden. Mit der Migration eines Web-Portals, einer Kommunalen Anwendung und von Arbeitsplatznetzen werden weit verbreitete und vordringliche Szenarien abgedeckt.

Im Folgenden werden sowohl das Testbed für diese Migrationsbeispiele als auch die Migration selbst dargestellt. Zur Dokumentation eines Migrationsbeispiels finden sich die ausgefüllten Web-Server-Checklisten im Anhang.

## 10.1. Migrations-Testbed

Das Migrationstestbed wurde mithilfe einer Virtualisierungsumgebung aufgesetzt. Dabei wurden die verschiedenen logischen Komponenten der Migrations-Referenzarchitektur unter VMware vSphere realisiert. Die Details des Migrations-testbeds sind:

- Hardware: Dell PowerEdge Bladecenter mit 6 Blades
- VMware vSphere 4.1 Enterprise
- Simulation der Netzwerkinfrastruktur mittels vSwitches
- Storage mittels NFS durch eine NetApp FAS 304x
- Erstellung neuer Images mittels NetApp SnapClone

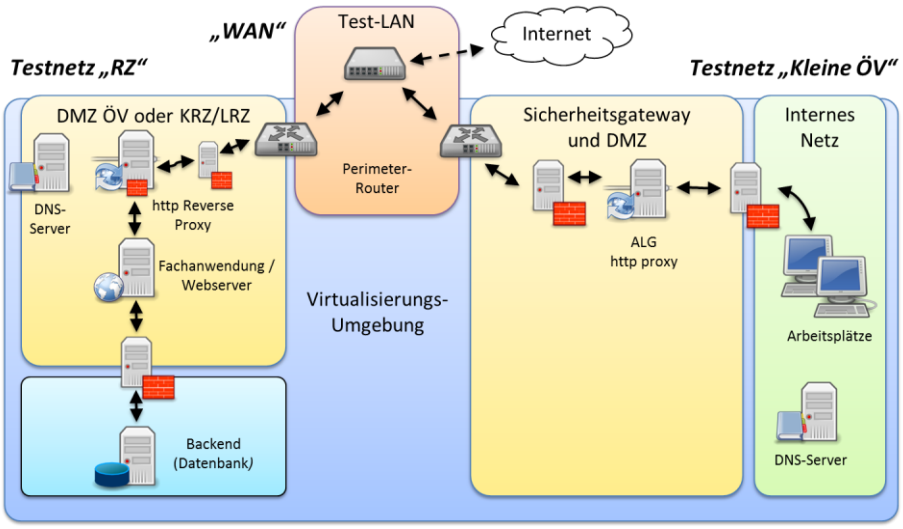


*Abbildung 30: Migrations-Testbed*

Die Abbildung zeigt die Teilnetze entsprechend der Migrations-Referenz-architektur auf logischer Sicht: Das Testnetz „RZ“ steht hier für eine Einrichtung die Dienste anbietet, das Testnetz „Kleine ÖV“ steht für eine Einrichtung die über Arbeitsplätze auf diese Dienste zugreift. Die Netzverbindungen sind innerhalb der Virtualisierungsumgebung mit VLANs und vSwitches realisiert. Dabei wurde darauf geachtet, später weitere Server integrieren zu können, aufbauend auf der Referenz-Architektur. Eine Verbindung zum Internet und zur (zukünftigen) Einbindung von externen Hardware-Komponenten ist vorhanden.

Zur Migration wurden zunächst die entsprechenden Komponenten des Szenarios im Testbed realisiert und miteinander über IPv4 zu einem betriebsfähigem Gesamtnetz verbunden. Im nächsten Schritt fanden dann die Migrationsarbeiten zu IPv4/IPv6 Dual Stack entsprechend der Checklisten dieses Migrations-leitfadens statt. Abgeschlossen wurden die Migrationen dann jeweils mit den in den Checklisten vorgeschlagenen Funktionstests.

Zum besseren Verständnis sind die Migrationsbeispiele sind in zwei Szenarien von unterschiedlicher Komplexität zusammengefasst:

- Migration eine Web-Servers, mit der Migration der Netzinfrastruktur
- Migration einer web-basierten kommunalen Fachanwendung, mit der Migration von Arbeitsplatznetzen bei Nutzung von (stateful) DHCPv6.

Beide Szenarien sind so konzipiert, dass sie nicht nur eine (lokale) Migration einer Komponente darstellen, sondern dass ein Dienst oder eine Fachanwendung in einer typischen Umgebung migriert wird. Die Funktionsfähigkeit wird anhand des logischen Ende-zu-Ende-Zugriffs getestet, also einer realistischen Nutzung des Dienstes.

## 10.2. Migration „Web-Server“

Bei diesem einführenden Migrationsszenario soll ein Webserver auf IPv6 umgestellt werden, in der typischen Konfiguration der ÖV mit vorgeschaltetem Reverse-Proxy. Es könnte sich um ein kleines Informationsangebot handeln oder aber auch um eine andere web-basierte-Anwendung. Der Web-Server muss nicht notwendigerweise von außerhalb erreichbar sein.

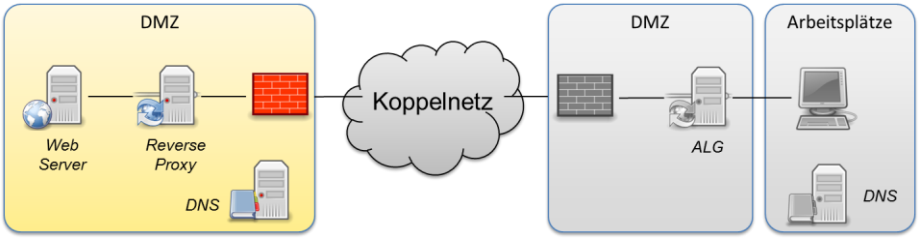


*Abbildung 31: Migrations-Beispiel „Web-Server“*

Die Abbildung zeigt die logische Ende-zu-Ende-Sicht auf dieses Szenario. Im Mittelpunkt steht dabei der Web-Server auf der linken Seite. In diesem Szenario wurde auf der Seite der Arbeitsplätze nur die Netzinfrastruktur, analog zur Server-

Seite migriert, ein Arbeitsplatz wurde anschließend zur Durchführung der Tests statisch konfiguriert. Eine sinnvolle Teilmigration in diesem Szenario ist beispielweise die Migration des Zugangs von außen bis hin zum Reverse-Proxy auf IPv4/IPv6-Dual-Stack-Betrieb.

Die folgende Tabelle stellt die in diesem Szenario genutzten Komponenten vor:

| Komponenten Web-Server | Software / Version |
|---|---|
| Web-Server | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>Apache 2.2.14 |
| Reverse-Proxy | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>Apache 2.2.14 + mod_proxy |
| Paketfilter | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>iptables 1.4.4-2 |
| Router | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>UFW, iptables |
| DNS-Server | Windows Server 2008 R2 Standard SP1<br>DNS-Server 6.1.7601.17514 |

*Tabelle 9: Komponenten im Migrationsszenario „Web-Server“*

Die Migration wurde entsprechend der IPv6-Leitlinie und den Checklisten dieses Leitfadens durchgeführt. Die ausgefüllten Checklisten für dieses Migrationsszenario finden sich in Abschnitt 0 ab Seite 177.

## 10.3. Migration „Kommunale Anwendung“

Nachdem bei dem ersten Migrationsbeispiel die Netzinfrastruktur und ein (Web-)Server umgestellt wurden, wird im Folgenden ein darauf aufbauendes, komplexeres Szenario vorgestellt. Es soll dabei die typische Umgebung für eine Web-basierte Fachanwendung migriert werden. Serverseitig ist dazu die Migration eines Web- oder Applikationsservers nötig, der wiederum durch einen Datenbank-Server unterstützt wird. Aus Sicherheitsgründen befindet sich der Datenbank-Server in einem separaten Netz. Eine Reihe von Fachanwendungen sind auf diese Weise realisiert, beispielhaft wurde in diesem Szenario die Anwendung VISkompakt von PDV-Systeme (siehe unten) migriert. Zudem werden in diesem Szenario realistische Arbeitsplatz-Netzwerke betrachtet. Diese nutzen für die Konfiguration der einzelnen Systeme stateful DHCPv6, d. h. es werden die Endsystem-Adresse und DNS-Server-Adresse mittels DHCP konfiguriert.

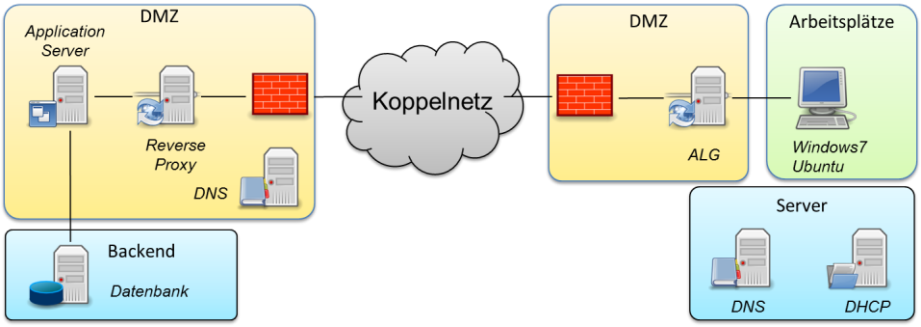


*Abbildung 32: Migrations-Beispiel „Kommunale Anwendung“*

Dieses Szenario kann in zwei Teilen betrachtet werden: Serverseitig besteht es aus der Migration der Web-Anwendung (vergleiche mit dem vorherigen Szenario), und auf der Seite der Arbeitsplätze findet eine Migration von DHCP-konfigurierten Arbeitsplatznetzen statt. Auch in diesem Szenario ist die Teilmigration von außen bis hin zum Reverse-Proxy möglich, hinzu kommt eine mögliche Teilmigrationen rund um das ALG auf der Arbeitsplatzseite. Da die Verbindungen von den Arbeitsplätzen nach außen an dieser Stelle terminiert und neu aufgebaut werden, ist hier eine ideale Schnittstelle um alle möglichen Zugriffskombinationen zu realisieren: Noch nicht migrierte IPv4-only Arbeitsplätze können auf IPv6-only-Angebote zugreifen, aber auch neue, IPv4/IPv6-Duals-Stack- und IPv6-only-Arbeitsplatznetze können bestehende IPv4-only-Fachanwendungen nutzen.

In diesem Beispiel wurde die Anwendung „VISkompakt“ von PDV-Systeme (http://www.pdv.de) als eine typische Anwendung der ÖV betrachtet und migriert. Es handelt sich dabei um ein Vorgangsbearbeitungs- und Dokumenten-management-System, welches mit einem Applikationsserver und einem Datenbank-System realisiert ist. Diese Fachanwendung ist in zwei Versionen erhältlich, einer J2EE-Version basierend auf ORACLE-Technologien und einer .NET-Version basierend auf Microsoft-Technologien. In dem vorgestellten Beispiel wurde die Version VISkompakt J2EE 4.8(027) eingesetzt. Das Server-Betriebssystem ist Windows 2008 mit Java 1.4.2 Update 19, als Datenbank wurde MS SQL 2008 eingesetzt.

Die folgende Tabelle stellt die in diesem Szenario auf der Seite der Web-Anwendung genutzten Komponenten vor.

| Komponenten Fachanwendung | Software / Version |
|---|---|
| Applikationsserver | Windows Server 2008 R2 Standard SP1 64-Bit<br>PDV-Systems VISkompakt J2EE 4.8(027) |
| Reverse-Proxy | Ubuntu Server 10.04.3 LTS<br>Apache 2.2.14 + mod_proxy |
| Paketfilter | Ubuntu Server 10.04.3 LTS<br>iptables 1.4.4-2 |
| Router | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae) |
| DNS-Server | Windows Server 2008 R2 Standard SP1<br>DNS-Server 6.1.7601.17514 |
| DB-Server | Windows Server 2008 R2 Standard SP1 64-Bit<br>Microsoft SQL Server 2008 R2 64-Bit |

*Tabelle 10: Komponenten im Migrationsszenario „Web-Anwendung“ – Serverseite*

Die auf der Seite der Arbeitsplatz-Netze genutzten Komponenten vor sind in dieser zweiten Tabelle zusammengefasst.

| Komponenten Arbeitsplatzseite | Software / Version |
|---|---|
| Arbeitsplätze | Windows 7<br>Ubuntu Desktop 12.04 development branch (3.2.0-10-generic) |
| DNS-Server | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>Bind9 1:9.70.df |
| ALG | Ubuntu Server 11.10 (3.0.0-14-generic-pae)<br>Squid 3.1.14 |
| Router | Ubuntu Server 10.04.3 LTS (2.6.32-21-generic-pae)<br>Radvd 1:1.3-1.1u |
| DHCP-Server (auf Router) | Dhcp3-server 3.1.3-2ubu |
| DHCPv6 Server (auf Router) | Wide-dhcpv6-server 20080615-7 |

*Tabelle 11: Komponenten im Migrationsszenario „Kommunale Anwendung“ - Arbeitsplatznetze*

Die Migration wurde entsprechend der Empfehlungen und Checklisten dieses Leitfadens durchgeführt. Als Beispiel dient die ausgefüllte Checkliste aus der Web-Server-Migration.

# 11. Spezielle Migrationsaspekte

## 11.1. Neue Eigenschaften von IPv6

Die folgenden Abschnitte zeigen einige Eigenschaften und Optionen auf, welche unter IPv6 möglich sind und, sofern sie eingesetzt werden sollen, eine noch detailliertere Betrachtung erfahren müssen. In den folgenden Absätzen werden kurz die wichtigsten Aspekte dieser Optionen unter IPv6 aufgezeigt.

### 11.1.1 Multipräfix-Umgebung

Als IPv6-Multipräfix-Umgebung wird ein Netzwerkaufbau bezeichnet, bei dem ein Knoten (Klient, Server, Router) auf *einer* Schnittstelle IPv6-Adressen aus mindestens zwei verschiedenen IP-(Sub-)Netzen besitzt. Solch ein Fall tritt z. B. auf bei:

- „host centric multihoming“
- Netzrenummerierungen
- Nutzung von IPv6-Adressen mit verschiedenen Scopes auf einer Schnittstelle, z. B. unique local und globally unique Adressen zusammen.

In jedem dieser Fälle ist es wichtig, zu definieren, wann welche der konfigurierten IPv6-Adressen für den Aufbau einer Datenkommunikation verwendet wird. Dies kann zum Teil von der Anwendung auf dem System bestimmt sein, aber auch vom Betriebssystem/IP-Stack und von der Konfiguration der Adressen (und deren Prioritäten). Für technische Details dazu siehe auch [RFC3633]. Dieses Dokument definiert auch das Standardverhalten eines Betriebssystems zur IPv6-Adressauswahl.

*Hinweis*: Die standardmäßige Nutzung einer *link local* IPv6-Adresse und einer weiteren IPv6-Adresse mit einem anderen Scope wird nicht als Multipräfix-Fall angesehen, da hier trotz zweier Adressen nur ein Default Gateway existiert.

### 11.1.2 Multihoming

Als Multihoming wird jede Art von Netzwerkaufbau bezeichnet, bei dem ein Knoten mehr als eine Verbindung (engl.: uplink) zum nächsten, übergeordneten Netzwerk besitzt. Dieser Knoten kann dabei ein Endsystem sein („host centric multihoming“) oder ein Gateway oder Router („site multihoming“).

Ziel des Multihoming ist die Erhöhung der Ausfallsicherheit der Anbindung bestimmter Netze durch den Einsatz redundanter Netzverbindungen. Die typischste Variante für Multihoming ist die Verbindung des Intranets einer Institution an dritte Netze (z. B. das Internet) über zwei physikalisch getrennte Netzverbindungen. Diese terminieren am Zugangsrouter der Institution und führen zu zwei verschiedenen Routern auf Providerseite. Diese Router können zum selben Provider oder zu zwei verschiedenen Providern gehören. Unabhängig davon kann auch noch der Zugangsrouter der Institution selbst redundant ausgelegt sein. Das folgende Bild zeigt ein vereinfachtes Schema für Site-Multihoming (ohne redundanten Zugangsrouter):

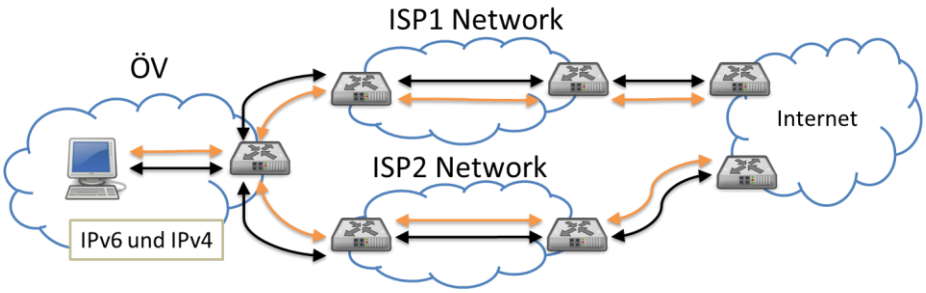


*Abbildung 33: Site Multihoming mit zwei Providern*

Für die technische Umsetzung des Multihoming existieren verschiedene Techniken[18]. Diese unterscheiden sich hinsichtlich der verwendeten IP-Adressen (IP-Adressen vom Provider versus provider independant (PI) Adressen), der Art der Umschaltung der genutzten Verbindung (im Falle eines Ausfalls einer Leitung) und der Frage, ob das Multihoming auch auf Klienten in der Institution sichtbar ist (in Form mehrerer IPv6-Adressen bzw. sich ändernder IPv6-Präfixe).

Weiterführende Informationen zu IPv6-Multihoming finden sich z. B. in [RFC3582] und in [MIG_GUIDE].

### 11.1.3 Renummerierung

Durch technische oder organisatorische Veränderungen kann es vorkommen, dass eine Verwaltung oder eine Liegenschaft ihr IP-Präfix für ihre IT-Infrastruktur ändern muss. Bei einem Dual-Stack-Betrieb bedeutet dies, ein neues IPv4- und ein neues IPv6-Präfix in Betrieb zu nehmen. Ausnahme: Bei Verwendung von providerunabhängigen (provider independant (PI)) IPv6 Adressen kann auch bei einer Reorganisation einer ÖV im Allgemeinen das IPv6-Präfix behalten werden.

IPv6 besitzt durch den Aufbau des Protokolls und durch den Verzicht auf NAT eine andere Herangehensweise an Netzwerk-Renummerierung als IPv4. Ein IPv4-basiertes Netzwerk wird zumeist mit privaten IP-Adressen für Arbeitsplatzrechner betrieben, so dass hier in erster Linie die extern sichtbaren Systeme (Zugangsrouter/Gateway, ALGW, Proxy, Reverse Proxy) von einer Renummerierung betroffen sind. Bei einer IPv6-Infrastruktur in einer ÖV gilt dies nur dann analog, wenn die IPv6-Arbeitsplatzrecher *ohne* globale Adressen arbeiten, z. B. bei Verwendung von unique local IPv6-Adressen hinter einem (http-)Proxy.

Aber auch bei Verwendung von global unicast Adressen im Intranet ist eine Renummerierung von IPv6-Subnetzen relativ einfach durchführbar, da eine „sanfte“ Migration der Präfixe möglich ist (siehe [RFC4192]). Ferner besteht unter IPv6 bei einer Renummerierung nicht die Problematik von kollidierenden IP-Adressbereichen wie bei IPv4 (typisch: Kollision von mehreren privaten 10.0.0.0/8 oder 192.168.0.0/16 Subnetzen).

[18] siehe z. B. http://ipv6.com/articles/general/IPv6_Multihoming.htm

Eine Renummerierung muss jedoch in jedem Fall als eigenständiges Projekt sorgfältig geplant, durchgeführt und überwacht werden.

### 11.1.4 Mobile IPv6

Durch die Nutzung von Notebooks und Smartphones von unterwegs wird die Unterstützung von nahtloser Datenkommunikation während der Bewegung (z. B. auf einer Zugfahrt) immer wichtiger für den geschäftlichen Alltag. Diese Art der Mobilität für Endsysteme muss gewährleisten, dass auch bei Wechsel der Verbindung zu einer anderen Basisstation laufende IP-Datenströme nicht unterbrochen werden. Dazu darf sich die IP-Adresse des Endsystems nicht ändern.

Für IPv4 wird dies ermöglicht durch den Einsatz von „mobile IP“ [RFC5944]. Für IPv6 ist „mobile IP“ definiert in [RFC6275]. Für IPv4 wurde die Unterstützung für Mobilität erst nach dem Protokoll definiert. Für IPv6 jedoch wurde dies bereits bei der Standardisierung des Protokolls selbst berücksichtigt. Mobile IP für IPv6 ist daher mit anderen, z. T. einfacheren, Mechanismen realisiert[19].

Mobile IPv6 ist für mobile Netze der vierten Generation (LTE, Long Term Evolution) verpflichtend. Für den Einsatz von Notebooks und Smartphones in LTE Netzen ist daher die Unterstützung von Mobile IPv6 verpflichtend.

## 11.2. Einbindung bestehender IPv4-only Komponenten

Vorhandene IPv4-only-Komponenten, welche nicht um IPv6-Unterstützung erweitert werden können (z. B. bestehende Appliances) , werden voraussichtlich noch viele Jahre im Einsatz sein, da sie in bestehenden Infrastrukturen oft wichtige Aufgaben erfüllen. Für diese Komponenten ist es sinnvoll, über eine koordinierte Weiternutzung in einer zukünftigen Dual-Stack-bzw. IPv6-only-Umgebung nachzudenken.

Mit „IPv4-only-Komponenten“ sollen im Folgenden solche Geräte bezeichnet sein, für die es nicht möglich ist - oder z. B. auf Grund der Kosten nicht sinnvoll ist:

- ein Software-Update auf IPv4/IPv6 Dual Stack durchzuführen
- ein Firmware-Upgrade auf Dual Stack durchzuführen
- per Beschaffung einen Dual-Stack-fähigen Ersatz einzukaufen
- das Anmieten eines Dual-Stack-fähigen Ersatzes oder
- das Outsourcing des Dienstes an einen externen Dienstleister nicht möglich ist (z. B. auf Grund von Sicherheitsbestimmungen)

Dies trifft oft zu auf hoch integrierte Geräte (embedded devices) mit Netzwerkanschluss und fest installierter Firmware. Es kann auch zutreffen auf

[19] eine Beschreibung von Mobile IPv6 findet sich zum Beispiel unter http://wwwlehre.dhbw-stuttgart.de/~schulte/doc/MobileIP.pdf

Fachanwendungen, für die es keinen Nachfolger mit IPv6-Unterstützung gibt bzw. geben wird.

Die zukünftige Einbindung solcher Komponenten muss insbesondere dann überdacht werden, wenn *IPv6-only-Systeme* mit ihnen interagieren müssen.

Wichtig sind hierfür folgende Fragen zu klären:

- Gibt es wirklich in absehbarer Zeit keinen Update-Pfad (neue Software, Firmware oder Ersatz-Gerät)?
- Muss diese Komponente nur im Intranet kommunizieren oder auch über das Internet bzw. über Koppelnetze?

Es werden im Folgenden drei Kategorien betrachtet:

(1) Die Komponente ist ein Gerät, Dienst oder Server welcher über http(s) angesprochen wird, aber aus einem der o. g. Gründe nicht IPv6-tauglich gemacht werden kann. Dies kann z. B. ein webbasiertes Management-Interface einer IT-Appliance sein.

In diesem Fall empfiehlt es sich, für den Zugang von IPv6-only Systemen aus vor der Server-Komponente einen http(s)-Reverse-Proxy zu installieren (siehe Abschnitt 7.3.3). Dieser wird dem Dienst logisch gesehen vorgeschaltet und wandelt http-Anfragen über IPv6 in solche über IPv4 um.

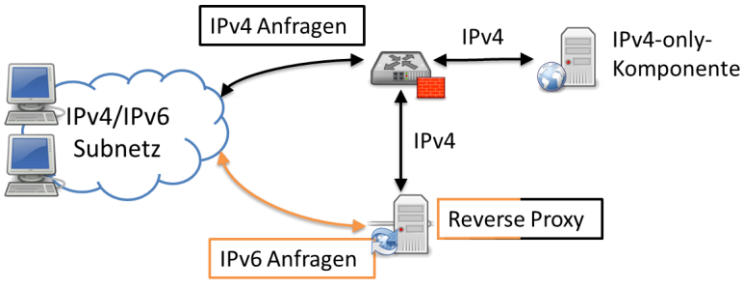


*Abbildung 34: Reverse-Proxy für Anbindung einer IPv4-only-Komponente*

Diese Lösung ist sowohl für Systeme im Intranet anwendbar, als auch für solche, die öffentlich sichtbar sein sollen.

Für SIP-Server kann es u. U. auch eine Lösung vom Typ (1), also durch Zwischen-Schalten eines (SIP-)Reverse-Proxy geben. Dies hängt jedoch von den Details der vorhandenen SIP-Installation ab.

(2) Die Komponente ist ein *nicht-http*-Dienst, -Gerät oder -Server, welcher nur IPv4-only verfügbar ist und von IPv6-only-Klienten genutzt werden können soll.

In diesem Fall ist es u. U. möglich, durch einen 6-zu-4-Protokoll-Umsetzer (6-to-4-Gateway) eine Verbindung zwischen den IPv6-only-Klienten und dem Dienst bzw. Server herzustellen. Siehe hierzu für eine technische Beschreibung in Abschnitt 7.3.4. Falls die IPv4-only-Komponente nur ausgehende Verbindungen benötigt und selbst keinen Dienst anbietet, ist auch die NAT64-Technik eine Option. Siehe dazu Abschnitt 7.3.1.

Ein Protokoll-Umsetzer kann auf der Netzwerkebene IPv6-Pakete in IPv4-Pakete konvertieren. Jedoch ist diese Umsetzung nicht vollkommen transparent und funktioniert daher nicht für alle Anwendungen. Zur Klärung der Realisierbarkeit ist zu untersuchen, welche Protokolle und Verbindungen von dem Dienst genutzt werden.

Protokolle, die intern auch IP-Adressen zur Identifizierung eines Kommunikationspartners benutzen und/oder selbsttätig Verbindungen zu Klienten aufbauen, funktionieren nur eingeschränkt oder gar nicht über einen 6-zu-4-Umsetzer. Beispiele hierfür sind SIP oder FTP.

(3) IPv4-only-fähige Geräte, bei denen weder (1) noch (2) eine Lösung darstellt, sind von *IPv6-only-Klienten* nicht erreichbar. In diesem Fall sollte geprüft werden, ob als Klienten (ggf. dedizierte) IPv4- bzw. Dual-Stack-Klienten genutzt werden können. Dies kann z. B. ein Dual-Stack-fähiges, virtuelles System auf einem Terminal-Server sein, welches remote von einem IPv6-only-Rechner genutzt wird. Auf diese Art kann etwa eine IPv4-only-Management-Anwendung einer Telefonanlage von einem IPv6-only-Arbeitsplatz aus genutzt werden.

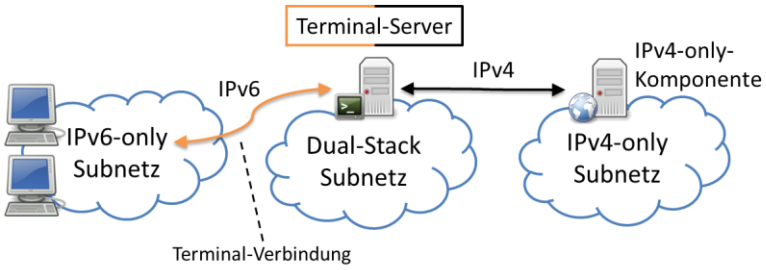


*Abbildung 35: Terminal-Server für Zugriff auf eine IPv4-only-Komponente*

Im Fall von IPv4-only-Geräten, welche nur im Intranet genutzt werden (z. B. IP-fähige Haustechnik, wie IP-Kameras) besteht zudem die Möglichkeit, ausschließlich private IPv4-Adressen zu nutzen. So können diese Geräte noch im Intranet genutzt werden, in dem Fall, dass einmal nur noch ein IPv6-WAN-Anschluß an einem Standort verfügbar ist. Dies setzt jedoch (auch ohne IPv4-Internet-Zugang) weiterhin den Betrieb einer lokalen IPv4-Infrastruktur parallel zur IPv6 Infrastruktur am Standort voraus.

## 12. Zusammenfassung und Ausblick

Wie in der einleitenden Motivation in diesem Dokument ausgeführt wurde, wird IPv6 auf Grund der akuten IPv4-Adressknappheit in naher Zukunft eine starke Verbreitung finden. ISPs beginnen Internetanschlüsse auszurollen, welche IPv4 nur noch mit Einschränkungen bereitstellen und Hosting-Anbieter nehmen mittlerweile extra Gebühren für IPv4 Adressen. Durch Sensornetze, Smart Grids und LTE-Funknetze wird IPv6 auch immer öfter in der Form „IPv6-only-Netzwerk“ anzutreffen sein.

Es ist daher für die öffentlichen Verwaltungen in Deutschland essentiell, ihre Dienste – zumindest die von „außen“ erreichbaren – auch über IPv6 erreichbar zu machen. Dies betrifft sowohl Fachanwendungen, welche ausschließlich von anderen Verwaltungen genutzt werden, als auch Bürger-Dienste (z. B. ELSTER) und öffentliche Informationen, welche über das Internet bereit gestellt werden.

Spätestens, wenn die ersten Internetanschlüsse ausgerollt werden, welche einem Bürger IPv4 nur noch über Hilfstechniken zur Verfügung stellen, wird es zur Pflicht werden, Bürgerdienste auch über IPv6 anzubieten, um diese in gewohnter Qualität sichtbar zu machen.

Bei der Einführung von IPv6 bietet sich zudem für Organisationen die Chance, gewachsene Strukturen aufzuräumen. Auch wenn noch auf absehbare Zeit Dienste über IPv4 zur Verfügung gestellt werden müssen, so hilft eine sorgfältige Vorbereitung auch, die Netze leistungsfähiger und sicherer zu machen.

Mit den vorliegenden Dokumenten ist eine Reihe an Hilfsmitteln geschaffen worden, die die öffentliche Verwaltung sowohl im Kontext von Beschaffungsmaßnahmen als auch bei der Bestandsaufnahme und der aktiven IPv6-Migrationsplanung unterstützen können.

Vorrangiges Ziel ist, die zu leistenden Aufgaben bei der Umstellung auf IPv6 in Bezug zur Öffentlichen Verwaltung und deren Netzstrukturen zu setzen. Es wurde bei der Erstellung, insbesondere beim Migrationsleitfaden, darauf geachtet, die unterschiedlichen Aufgaben, Funktionen und Größen der Öffentlichen Verwaltung zu berücksichtigen. Gleichwohl ist den Autoren bewusst, dass es ein "one size fits all" nicht gibt und dass im Einzelfall Entscheidungen anders ausfallen können, als hier vorgeschlagen.

Das begleitende Profildokument orientiert sich an bereits bestehenden und eingeführten Profilen auf internationaler Ebene und strukturiert diese weiter, so dass eine thematische Vergleichbarkeit der unterschiedlichen Geräteklassen in dem Tabellenwerk möglich wird. Da auch hier die Entscheidung für oder gegen eine Anforderung von den konkreten Einsatzszenarien abhängt, ist das Tabellenwerk um ein Profildokument ergänzt, welches Szenarien beschreibt und die Entscheidungsfindung erleichtert.

Da alle Arbeiten vor dem Hintergrund einer Laborinfrastruktur entstanden sind und dort praktisch überprüft wurden, stehen dem Leser und Anwender eine Reihe von Prüflisten zur Verfügung. Mit Hilfe dieser Listen kann der IST-Zustand

erhoben werden, die Migration für verschiedene Komponenten schrittweise durchgeführt werden. Eine weitere Liste beschreibt weiterhin Tests, sich durchzuführen sind, um das Ergebnis zu verifizieren. Durch die Möglichkeiten, in einem Laboraufbau zu arbeiten und anschließend Teilmigrationen durchzuführen, bietet sich in der Praxis die Gelegenheit, inkrementell Wissen und Erfahrung mit IPv6 aufzubauen.

Alle diese Dokumente geben dem Netzwerker und Administrator Hilfsmittel an die Hand, wenn aus Netz- oder Anwendungssicht ein Dienst unter IPv6 bereitzustellen ist. Im Beschaffungsprozess können die Profildokumente wertvolle Unterstützung bieten, wenn es um die Auswahl von Eigenschaften geht, die ein neu zu beschaffendes Gerät aufweisen soll. Ebenso kann auch eine Bewertung von Angeboten unter Einbeziehung der Tabellen vorgenommen werden.

Damit liegt erstmalig eine Sammlung von Dokumenten vor, die die Umstellung auf IPv6 unter Beachtung der Anforderungen der Öffentlichen Verwaltung beschreibt und durch praktische Anleitung unterstützt.

Bitte senden Sie Fragen, Anregungen und Verbesserungsvorschläge an:

ipv6@bva.bund.de

# 13. Anhang I: IPv6-Migrations-Checklisten

Für die praktische Migration sind im Folgenden mehrere Checklisten zusammengestellt, welche die in diesem Migrationsleitfaden vorgestellten, notwendigen Arbeitsschritte und Hinweise zusammenfassen. Im Vordergrund stehen auch bei diesen Checklisten die Besonderheiten von IPv6, die Wechselwirkungen mit IPv4 durch die Einführung von IPv6 bzw. die Migration zu IPv4/IPv6-Dual-Stack.

Zur Vorbereitung eines konkreten Migrationsprojekts finden sich ab Seite 152 mehrere Checklisten für die praktische Umsetzung. In diesen Checklisten sind alle grundlegenden Schritte zur Migration zusammengefasst.

Aufgrund der mannigfaltigen Konfigurationen in verschieden ÖV-Netzen können diese Checklisten nicht jeden Einzelfall hundertprozentig abdecken. Sie können aber als ein stabiles Grundgerüst dienen und als roter Faden durch die Migration führen.

Die Checklisten können (und sollen) bei Bedarf ergänzt werden. Diese Erweiterungen (zusätzliche Fragen, Datenfelder, etc.) sollten für die zukünftige Nutzung zusammen mit den Listen abgelegt werden.

In den Checklisten werden wichtige Informationen zur vorhandenen Netzinfrastruktur gesammelt, wie z. B. Angaben zu Netzen und Servern. Es können dabei alle Felder frei ausgefüllt werden. Auch beliebige weitere Angaben können notiert werden. Vorhandene Wahlmöglichkeiten in den Fragen sind dabei nicht ausschließlich zu verstehen. Sind die Checklisten durchgearbeitet, kann daran anschließend die Migration durch die Konfiguration der einzelnen Infrastrukturkomponenten schrittweise durchgeführt werden.

Es stehen die folgenden vier Migrations-Checklisten zur Verfügung:

- **Migrationsplanung** – Einstieg in die Migration inklusive Erfassung des Ist-Zustandes, Zielsetzung und Planung der Migrationsreihenfolge.
- **Netzinfrastruktur** – Migration des Netzzugangs, Migration von Subnetzen, und Netzinfrastrukturdiensten wie DNS und DHCP.
- **Webserver** – Exemplarische Umstellung eines Webservers/Portals.
- **Klienten** – Umstellung von Klientennetzen und Klienten auf Dual-Stack-Betrieb.

Die Checklisten bauen aufeinander auf und bilden eine natürliche Reihenfolge der Migration von außen nach innen ab. Das Migrationsprojekt muss mit einer Planungsphase beginnen, in der die vorhandene IT-Infrastruktur und die Ziele der Migration erfasst werden. Die Umsetzung beginnt zunächst mit der Netzinfrastruktur der betroffenen Netzbereiche, z. B. dem Zugang zu einem oder mehreren IPv6-Weitverkehrsnetzen (Wide Area Networks (WAN)) und den darin befindlichen Infrastruktur-Komponenten. Aufbauend auf diesem Schritt können anschließend Server(netze) und Klienten(netze) migriert werden.

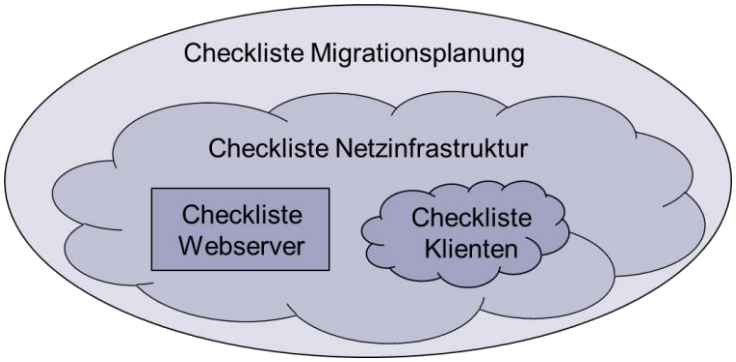


*Abbildung 36: Übersicht über die Checklisten*

Die Checklisten selbst sind jeweils in drei Abschnitte gegliedert:

- **Erfassung der Ist-Situation (Abschnitt E)** – Zusammenstellung von wichtigen Informationen der bestehenden Netzkonfiguration
- **Migration (Abschnitt M)** – Angaben zur geplanten Netzkonfiguration in logischer Reihenfolge
- **Prüfung (Abschnitt P)** – Wichtige Tests, die während und nach der tatsächlichen Migration durchgeführt werden sollten

Ergänzt werden die Checklisten um eine Übersicht typischer Kommandos zur Prüfung der vorhandenen Netzkonfiguration. Diese Kommandos wiederholen sich oftmals bei verschiedenen Prüfungen während der Migration und dienen zur schnellen Orientierung in einem existierenden Netzwerk. Sie sind hier am Ende als separater Anhang nach den Checklisten aufgeführt.

## 13.1. Migrationsplanung.E - Erfassung der Ist-Situation

Die Migration zu IPv6 ist eine wichtige Aufgabe, die entsprechend sorgfältig geplant werden muss. Die Planung selbst ist ein Teil der Migration und sollte möglichst frühzeitig begonnen werden. Dann ist genug Zeit um die Migrationsarbeiten mit anderen, bereits geplanten Infrastruktur-Arbeiten zu koordinieren, Ressourcen bereitzustellen und Mitarbeiter vorzubereiten, z. B. durch dedizierte Schulungen zu IPv6.

### Angaben zum Migrationsprojekt

| | |
|---|---|
| **Projekt-Ziel / -Inhalt** | **Welche (Teil-)Netze sollen migriert werden?** |
| **Zeitraum** | |
| **Mitarbeiter** | **Wer (intern/extern) muss involviert werden bei Planung und Umsetzung?** |
| **Ressourcen** | **Welche Aufwände sind zu erwarten und wo abzurechnen?** |
| **Projektleiter** | |
| **Auftraggeber** | |
| **Weitere Abhängigkeiten / relevante Maßnahmen**<br><br>(z. B. geplante Investitionen, Austausch-Zyklen, Neu-anschaffungen, Wartungsfenster, …) | |

***Es sollte ferner ein schematisches Architekturbild vorliegen**, in dem alle relevanten Netze und interne/externe Dienste* eingezeichnet *sind. Wichtige Infrastruktur-Komponenten, Server und sicherheitsrelevante Systeme müssen eingezeichnet sein.*

## Bereitgestellte Dienste / Anwendungen

Zusammenstellung relevanter Dienste und netzbasierter Anwendungen, die von der Organisationseinheit für Dritte zur Verfügung gestellt werden.

| Dienst /Anwendung | Beschreibung, ggf. Ansprechpartner |
|---|---|
| Externes Web-Portal | |
| FA | |
| FA2 | |
| FA3 | |
| | |

## Genutzte Dienste / Anwendungen

Zusammenstellung relevanter Dienste und netzbasierter Anwendungen, die in den betroffenen Netzen bzw. über diese Netze durch interne Nutzer verwendet werden. In dieser Liste sollten sowohl die von der ÖV intern genutzten Dienste aufgelistet werden, als auch externe Dienste, die über das Internet oder über Koppelnetze verwendet werden.

| Dienst / Anwendung | Beschreibung, ggf. Ansprechpartner |
|---|---|
| Internet-Zugriff | |
| E-Mail-Dienst | |
| FA[20] | |
| FA2 | |
| FA3 | |

[20] FA = Fachanwendung

## 13.2. Migrationsplanung.M - Migrations-Schritte

### Vorgehen/Reihenfolge bei der Migration:

- WAN/Gateway Router (siehe Migrationscheckliste Netzinfrastruktur)
- Netzinfrastruktur (siehe Migrationscheckliste Netzinfrastruktur)
- Infrastrukturdienste (siehe Migrationscheckliste Netzinfrastruktur)
- Subnetze (siehe Migrationscheckliste Klienten oder Webserver)

*Das generelle **Vorgehen bei einer Migration** wird in diesem Leitfaden detailliert in Kapitel 4 beschrieben. Die empfohlene Reihenfolge der Umstellung wird genauer erläutert in Abschnitt 5.1 und im Anhang II - IPv6-Migrationsleitlinie im Unterabschnitt 14.1*.

*Bei der Migrationsplanung sollte auch die Möglichkeit einer **Teilmigration** berücksichtigt werden. Weitere Details hierzu sind im Abschnitt 5.1.3 in diesem Dokument zu finden.*

Technische ***Empfehlungen zur Migration** („Welche Techniken muss oder sollte ich nutzen“) und zur Nutzung von IPv6 finden sich in Anhang II: IPv6-Migrationsleitlinie.*

***Es sollte ein detaillierter Projekt-Ablaufplan vorliegen**, in dem die **Arbeitsschritte und Meilensteine** des* Migrationsprojekts*, incl. der Abhängigkeiten zwischen Teilaufgaben und Meilensteinen, festgelegt sind.*

*Falls es dabei zu erwarteten Ausfallzeiten einzelner Netzsegmente kommen sollte, so müssen diese* „Wartungsfenster“ *geplant werden und Nutzer mit hinreichend Vorlauf über die Arbeiten informiert werden. (Idealerweise sollten Arbeiten, welche die Funktion wichtiger Infrastrukturdienste oder Netzsegmente beeinträchtigen, außerhalb der normalen Büroarbeitszeiten stattfinden).*

Es wird empfohlen, ein IPv6-Testnetz aufzubauen, in dem praktische Erfahrungen mit IPv6 und dem Verhalten von Geräten bzw. typischen Implementationen gesammelt werden können. Insbesondere bei der schrittweisen Migration bzw. Teilmigration kann ein Testnetz auch als Vorläufer für den Wirkbetrieb aufgesetzt werden, beispielsweise indem ein zusätzlicher (Web-)Server zu Testzwecken aufgesetzt wird oder ein einzelnes, typisches Arbeitsplatz-System testweise migriert wird.

## 13.3. Migrationsplanung.P - Prüfung der Migration

*Dieser Abschnitt beschreibt einfache Wege zur Prüfung der Konsistenz des Migrationskonzepts vor dem Beginn der eigentlichen Migration. An dieser Stelle kann daher noch keine Überprüfung von tatsächlichen Zugriffen erfolgen, sondern ein prüfender Blick auf die geplante Umsetzung ermöglicht werden.*

- Sind alle notwendigen Personen über das Migrationsvorhaben informiert?
- Ist der aufgestellte Zeitplan realistisch?
- Müssen Neuanschaffungen getätigt werden? (Hardware, Software)
- Ist Migrations-Support durch Dritte gewährleistet?
- Sind entsprechende Prüfungen für die erfassten Dienste geplant? (siehe ausgefüllte Tabellen)

Bei der Migration einzelner Fachanwendungen liegt die Herausforderung in der Berücksichtigung aller Infrastruktur- und Querschnittsdienste, die zum Betrieb notwendig sind.

Die Software-Matrix im „IPv6-Profil der ÖV“ [IPv6_PROFILE] stellt diese Art von Zusammenhängen dar und sollte genutzt werden, um mögliche Abhängigkeiten im Vorfeld zu erkennen.

## 13.4. Netzinfrastruktur.E - Erfassung der Ist-Situation

**WAN-Zugang**

| | | |
|---|---|---|
| Anbieter / Kontakt für den WAN-Zugang | = | |
| IPv4-Präfix (der ÖV) | = | |

**Infrastruktur-Geräte**

| | | |
|---|---|---|
| *Switches (incl. DHCP-Relay)* | = | Name, Hersteller, Modell, Firmware |
| *Router* | = | Name, Hersteller, Modell, Firmware |
| *Sicherheitskomponenten (ALG, Firewall, Proxy, CryptoBox)* | = | Name, Hersteller, Modell, Firmware |

**Infrastruktur-Dienste**

| | | |
|---|---|---|
| *DNS* | = | Name, Hersteller, Software, Version |
| *DHCP* | = | Name, Hersteller, Software, Version |
| *NTP* | = | Name, Hersteller, Software, Version |
| *LDAP* | = | Name, Hersteller, Software, Version |
| *Exchange/Groupware Server* | = | Name, Hersteller, Software, Version |
| *E-Mail Server* | = | Name, Hersteller, Software, Version |

## Erfassung der Netzstruktur

| IPv4-Subnetz (zzgl. Typ, „Name“) | Beschreibung, und ggf. Ansprechpartner (DMZ, Servernetz, Klientennetz, …) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |

(siehe auch Adressplan in Migrationsplanung.M auf Seite 155)

## Zugriffsmatrix

*In der* folgenden *Übersicht sollen die erlaubten Netzübergänge zur Nutzung der oben genannten Dienste und Anwendungen dargestellt werden.*

| Ziel | | Arbeitsplätze | | | Server | | WAN | |
|---|---|---|---|---|---|---|---|---|
| Quelle | | | | | | | | |
| Arbeits-plätze | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| Server | | | | | | | | |
| | | | | | | | | |
| WAN | | | | | | | | |
| | | | | | | | | |

**Netzwerkmanagement und Monitoring**

In dieser Checkliste wird nicht im Detail auf das Netzwerkmanagement und Monitoring eingegangen. Es ist aber generell zu beachten, dass einerseits die Systeme des Netzwerkmanagement auch unter IPv6 betrieben werden sollten und andererseits die IPv6-Teile des Netzes im Netzwerkmanagement abgebildet werden. Bei der jeweiligen Prüfung eines Migrationsschritts sollte anschließend auch das Netzwerkmanagement mit einbezogen werden.

## 13.5. Netzinfrastruktur.M - Migrations-Schritte

**WAN-Zugang**

| | | |
|---|---|---|
| Genutzter WAN-Zugang (Internet-Zugang) ist bereits Dual-Stack fähig (IPv4/IPv6) | = | ja / nein |

*Falls nein, beginnen Sie zuerst für den WAN-Zugang mit der Migrationsplanung:*

1) Falls Ihnen noch kein IPv6-Adressbereich (IPv6-Präfix) für ihre Verwaltung zugeteilt worden ist, so wenden Sie sich an ihre übergeordnete Verwaltung oder direkt an die Local Internet Registry (LIR) des Bundes www.lir.bund.de um ein eigenes IPv6-Präfix zu bekommen. Siehe auch 6.2.1.

2) Kontaktieren Sie dann ihren Netzprovider (DSL-Provider, NdB, DOI, ggf. Ländernetze) und klären Sie die Möglichkeiten, ihr neues IPv6-Präfix in seinen Netzen zu routen.

3) Informieren Sie sich über die korrekte Aktivierung von IPv6 auf ihrem Gateway-Router.

| | | |
|---|---|---|
| Zugeteiltes IPv6-Präfix | = | |

**Dienste und Geräte**

Analysieren Sie für jedes der zuvor identifizierten Geräte bzw. Dienste der Netzwerkinfrastruktur die folgenden Fragen:

- Ist dieses Gerät/dieser Dienst direkt von der Migration betroffen?
- Ist dieses Gerät/dieser Dienst indirekt von der Migration betroffen, muss es also aufgrund von Abhängigkeiten zu direkt betroffenen Geräten / Diensten ebenfalls migriert werden?

Falls eine dieser beiden Fragen mit ja zu beantworten ist, dann muss geklärt werden:

- Ist das Gerät / der Dienst in der vorhandenen Version theoretisch IPv6-fähig? (abhängig von Baureihe, Software/Firmware-Version und Patch-Level)
    - Falls nein, so ist zuerst ein Upgrade oder ggf. ein Austausch zu planen.
      *Diese Arbeiten sind im Rahmen der IT-Wartung als separates Projekt zu planen und durchzuführen*.

  - Alternativ: Falls die Migration eines Teils der Infrastruktur nicht möglich erscheint (z. B. wirtschaftlich nicht sinnvoll ist), so besteht die Möglichkeit einer Teilmigration bzw. die Bildung eines IPv4-only-Subnetzes; siehe auch Abschnitt 7.3.2.

- Wie kann auf diesem Gerät IPv6-Unterstützung eingeschaltet werden?
- Wie kann dies in der Konfiguration so verankert werden, dass die IPv6-Unterstützung auch nach einem Neustart wieder automatisch eingeschaltet ist?

  - Bei einigen Diensten ist über das „Einschalten“ von IPv6 hinaus eine erweiterte Konfiguration zu erstellen, z. B. auf IP-Routern für die neuen IPv6-Routen und die Einstellungen zur IP-Adressvergabe. Diese Konfiguration muss pro Gerät/Dienst an der entsprechenden Stelle dokumentiert werden.

Entscheidend bei der Umsetzung der Migrationsschritte ist für einen reibungslosen Ablauf die Reihenfolge, in der auf Geräten, in IP-Subnetzen und für Dienste IPv6 eingeschaltet wird. Siehe dazu die Ausführungen im Abschnitt 14.1 diesem Dokument.

**Adresskonzept**

| | | |
|---|---|---|
| Liegt ein IPv6-Adresskonzept bereits vor? | = | ja / nein |

*Falls nein, so stellen sie ein passendes Adresskonzept auf. Die Tabelle **„Adressplan“** auf der folgenden Seite ermöglicht es, den vorhandenen und den geplanten (IPv6-)Adressplan zu dokumentieren.* Hilfestellung *bei der Definition der neu zu vergebenden IPv6-Adressen und der Auswahl des Adressvergabe-Verfahrens geben die Abschnitte 6.2 und 14.2 in diesem Leitfaden.*

| **vorhandenes Subnetz:** | | **Zugehöriges IPv6-Präfix / Länge** | **IPv6 - Adressvergabe (statisch, SLAAC, DHCPv6)** | **Adress-typ (ULA, GUA, link local)** | **Routing / Erreichbarkeit /ACLs wo dokumentiert?** | **Netz-Beschreibung / ggf. Ansprechpartner (intern/ ggf. extern)** |
|---|---|---|---|---|---|---|
| **IPv4-Subnetz** | **VLAN-ID** | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Adressplan**

## 13.6. Netzinfrastruktur.P - Prüfung der Migration

Zu prüfende Infrastruktur-Komponenten und -Dienste:

- WAN-Zugang (Internet oder Koppelnetze) über IPv6 funktioniert?
- IPv6-Adressvergabe funktioniert?
- Erreichbarkeit von Gateways und Infrastruktur-Diensten über IPv6? (siehe ausgefüllte Tabelle)
- Sind die Infrastruktur-Dienste wie geplant erreichbar?
- Optional: Sind die Dienste auch bzgl. IPv6 im Netzwerkmonitoring und -management erreichbar/sichtbar?

Wurden bei der Erstellung des Adressplanes folgende Punkte berücksichtigt:

- Ist definiert, wie sich die verfügbaren Bits der Subnetz-ID (typischerweise 8 oder 16 Bits) im Adressschema auf die Netztypen aufteilen?
- Mögliche Zusammenfassung von Subnetzen?
- Aggregierung von Subnetz-Routen?
- Wurden freie Adressbereiche für eine mögliche zukünftige Netzerweiterungen reserviert?

## 13.7. Webserver.E - Erfassung der Ist-Situation

**Netzwerk**

| | | |
|---|---|---|
| IPv4 Präfix und Netzmaske | = | |
| IPv4 Default Gateway Adresse | = | |
| ggf. Name des Subnetzes | = | |
| ggf. VLAN Tag | = | |
| spezielle Routen | = | |
| bestehende ACLs | = | |

**Betriebssystem**

| | | |
|---|---|---|
| Betriebssystem-Typ | = | Windows \| Linux \| MacOS \| … |
| Distribution (Name und Version) | = | |
| Kernel-Version (bei UNIX-Systemen) | = | |

**Host**

| | | |
|---|---|---|
| Öffentliche IPv4-Adresse des Webservers | = | |
| private IPv4-Adresse des Webservers | = | |
| optional: weitere IP-Adresse | = | |

**DNS**

| | | |
|---|---|---|
| Namen der vom Webserver gehosteten Domains [21] | = | |
| IP Adresse(n) der betroffenen „authorative“ DNS Server | = | |
| DNS-Namen des Webservers (intern / extern) | = | |

**Applikation**

| | | |
|---|---|---|
| Webserver-Software | = | |
| Version/Patchlevel der Software | = | |
| Konfiguration ist gesichert unter | = | |

**Sicherheitskomponenten auf dem Kommunikationspfad zum Gateway-Router**

| | | |
|---|---|---|
| ALG / Proxy | = | |
| PF / Firewall | = | |

[21] Bitte den FQDN (Fully Qualified Domain Name) eintragen.

## 13.8. Webserver.M - Migrations-Schritte

**WAN-Zugang**

| | | |
|---|---|---|
| Vom Webserver genutzter WAN-Zugang (Internet-Zugang) ist bereits Dual-Stack fähig (IPv4/IPv6) | = | ja / nein |

*Falls nein, führen Sie zuerst dort eine Migration durch.* Siehe dazu **Checkliste Netzinfrastruktur**.

**Adresskonzept**

*Falls kein Adresskonzept vorhanden ist, sollte zunächst eins erstellt werden.* Siehe dazu die **Checkliste Netzinfrastruktur**.

Folgende neue Werte sind zu definieren und zu notieren:

| | | |
|---|---|---|
| IPv6-Präfix des IPv6-Netzwerkes für den Webserver | = | |
| IPv6 Default Gateway Adresse (kann auch link-lokal sein) | = | |
| Art der Verteilung bzw. Konfiguration der IPv6 Adressen | = | statische Konfiguration / stateful DHCP |

**Netzwerk**

| | | |
|---|---|---|
| alle IP-Subnetze zwischen WAN-Zugang und dem Netzwerk, in dem sich der Webserver befindet, sind IPv4-IPv6 Dual-Stack-fähig | = | ja / nein |

*Falls nein, führen Sie zuerst dort eine Migration durch.* Siehe dazu die vorangegangene **Checkliste Netzinfrastruktur**.

**Betriebssystem**

| | | |
|---|---|---|
| Dual-Stack-Betrieb ist vom vorhandenen Betriebssystem in der installierten Version bereits unterstützt und aktiviert | = | ja / nein |
| IPv6 ist auf dem Webserver-Host konfiguriert und aktiviert | = | ja / nein |

*Hinweis: Falls der Webserver auf einer virtuellen Maschine läuft, muss auch die Virtualisierungsumgebung für IPv4/IPv6-Dual-Stack-Betrieb frei geschaltet werden.*

**Host**

| | | |
|---|---|---|
| öffentliche IPv6-Adresse des Webservers | = | |
| interne IPv6-Adresse des Webservers | = | |
| optional: weitere IPv6-Adresse | = | |

*Hinweis: Je* nach *gewählter Technik zur Verteilung der IPv6-Adressen muss diese Adresse noch auf dem Webserver selbst oder auf dem entsprechenden System (z. B. DHCPv6 Server oder Management-System) eingetragen werden.*

**DNS**

Der Webserver sollte unter IPv6 genauso wie unter IPv4 heißen, z. B. www.example.com. Damit sind beide IP-Adressen (IPv4 und IPv6) für denselben Hostnamen abzuspeichern.

| | | |
|---|---|---|
| Für die vom Webserver gehosteten Domains sind zusätzlich neue AAAA Records mit der neuen IPv6-Adresse auf dem entsprechenden „authorative“ DNS-Server(n) angelegt (beachte ggf. vorhandene DNS Zone Files oder mehrere DNS Server!) | = | ja / nein |
| Auf dem DNS-Server ist zusätzlich zum A-Record ein AAAA-Record für den **Hostnamen** des Webservers eingetragen. | = | ja / nein |
| Auf dem Webserver sind die IPv6-Adressen der zu nutzenden DNS-Server konfiguriert. | = | ja / nein |

**Webserver-Applikation**

| | | |
|---|---|---|
| Ist die für den Webserver verwendete Software Dual-Stack-fähig und IPv6-Unterstützung durch entsprechende Konfiguration aktiviert? | = | ja / nein |
| Erlaubt die Webserver-Konfiguration eingehende Verbindungen über IPv4 und über IPv6? | = | ja / nein |
| Bei mehreren gehosteten Domains: Erlauben die vHosts-Einträge der Webserver-Konfiguration eingehende Verbindungen über IPv4 und über IPv6? | = | ja / nein |

**(ALG-)Firewall und IDS**

| | | |
|---|---|---|
| Vorhandene Filterregeln für IPv6-Datenverkehr zum/vom Webserver sind so konfiguriert, dass sie ein zu IPv4 analoges Verhalten für IPv6-Anfragen aufweisen? | = | ja / nein |

## 13.9. Webserver.P - Prüfung der Migration

**Migration IPv4-only Webserver zu Dual Stack**

*Empfehlung:* Starten *Sie den Webserver **Host** nach Abschluss aller Migrationsschritte einmal neu.*

Zu überprüfen sind:

- Sind die erwarteten IPv4- und IPv6-Adressen korrekt konfiguriert? (GUA; Default-GW; DNS usw.)
- Können sowohl über die IPv4- als auch die IPv6-Adresse Verbindungen zu anderen IPv4/IPv6-Hosts aufgebaut werden?
- Werden DNS-Anfragen für IPv4- und IPv6-Domänen beantwortet?
- Können Webseiten (IPv4-only und IPv6-only) erreicht werden?
- Funktionieren die genutzten Programme/Anwendungen noch wie gewohnt?
- Verbindungen zum migrierten Webserver überprüfen:
- Von Extern („über das Internet“) und von Intern (aus dem Intranet)
    - „IPv4-only“-Klient/„IPv6-only“-Klient/IPv4-IPv6 Dual-Stack-Klient
    - Mit diversen Web-Browsern
    - Mit diversen Betriebssystemen
    - Für jede von dem Webserver gehostete Domain
    - Für mehrere wichtige URLs („/“ und ausgewählte Unterverzeichnisse; ggf. einen „Web-Crawler“ nutzen)
    - Funktionalität von Webseiten überprüfen, z. B. Formularseiten
- Dabei ist es sinnvoll, mehrere Kombinationen von Webbrowser, Betriebssystem und mehrere verschiedene IP-Subnetze (intern und extern) für Test-Anfragen an den Webserver zu nutzen.

Weitere Hinweise können dem Anhang IV - Technische Hinweise entnommen werden.

**Performance** überprüfen (z. B. Herunterladen der kompletten Startseite):

| | | |
|---|---|---|
| mit IPv4-only-Klient | = | |
| mit IPv6-only-Klient | = | |
| mit Dual-Stack-Klient | = | |

Für den Fall von Fehlern bei o.g. Prüfungen werden folgende Tests empfohlen:

| | | |
|---|---|---|
| ping6 auf die IPv6 Adresse des Webservers | = | ja / nein |
| traceroute6 auf die IPv6 Adresse des Webservers | = | ja / nein |
| nslookup/ dig -6 auf die DNS Namen der gehosteten Websites | = | ja / nein |
| TCP connect über IPv6,<br>z. B. via “telnet6 <IPv6-Adresse> 80” | = | ja / nein |
| Ausgaben von „ipconfig“ und „route“ auf dem Webserver ansehen | = | ja / nein |
| wget/curl/telnet zum Server und herunterladen einzelner Webseiten | = | ja / nein |

## 13.10. Klienten.E - Erfassung der Ist-Situation

Die folgenden Angaben können für mehrere Subnetze oder Gruppen von Arbeitsplatzrechnern zusammengefasst werden.

Die Migration von Arbeitsplatzrechnern baut auf der Netzinfrastruktur-Checkliste auf.

**Netzwerk(e):**

| | | |
|---|---|---|
| IPv4-Präfix und Netzmaske | = | |
| IPv4 Default Gateway Adresse | = | |
| spezielle Routen | = | |
| bestehende ACLs | = | |

**Betriebssystem:**

| | | |
|---|---|---|
| Betriebssystem-Typ | = | Windows \| Linux \| MacOS \| . . . |
| Distribution (Name und Version) | = | |
| bei UNIX: Kernel-Version | = | |

*Hinweis:* Verschiedene *Betriebssysteme sollten ggf. in Gruppen zusammengefasst werden (eine Checkliste pro Gruppe von Klientensystemen).*

**DNS:**

| | | |
|---|---|---|
| Domain | = | |
| DNS-Server | = | |

**IPv4-Adressvergabe:**

| | | |
|---|---|---|
| Methode | = | statisch \| DHCP |
| DHCP-Server | = | |
| DHCP-Relay | = | |

**Weitere Infrastrukturdienste:**

Diese Checkliste berücksichtigt nur die Besonderheiten in Bezug auf IPv6, d. h. eine Reihe von weiteren Konfigurationen werden vorgenommen, sollten aber normalerweise keine Schwierigkeiten machen. Es sollte aber überprüft werden, ob alle Dienste über Namen erreichbar sind (oder im Fall von Dual-Stack weiterhin über ihre ggf. verwendete IPv4-Adresse).

| | | |
|---|---|---|
| Zeitsynchronisation / NTP | = | |
| | | |
| | | |
| speziell Windows | | z. B. Domain-Controller |
| | | |
| | | |
| speziell Linux | | z. B. NIS |
| | | |
| | | |

## 13.11. Klienten.M - Migrations-Schritte

**Netzwerk:**

| | | |
|---|---|---|
| Ist das Netzwerk, in dem sich die Klienten befinden, inklusive aller Netzwerkgeräte und -dienste IPv4-IPv6-Dual-Stack-fähig? | = | ja / nein |

Falls nein, führen Sie zuerst dort eine Migration durch. Siehe dazu die **Checkliste Netzwerkinfrastruktur**.

| | | |
|---|---|---|
| IPv6-Präfix | = | |
| Subnetz-ID | = | |

**IPv6-Adressvergabe:**

| | | |
|---|---|---|
| Methode der Adressvergabe | = | statisch \| dynamisch |

**Statische Adresskonfiguration:**

| | | |
|---|---|---|
| Adressbereich | = | |
| Default-Gateway | = | |
| Domainnamen | = | |
| DNS-Server | = | |
| NTP-Server | = | |

**Dynamische Adresskonfiguration:**

| | | |
|---|---|---|
| Methode der Adressvergabe | = | SLAAC \| stateful DHCPv6 |

**Stateless Address Autoconfiguration (SLAAC):**

| | | |
|---|---|---|
| Erzeugung der Host-ID | = | zufällig erzeugt (PEX) \| EUI-64 |
| Default-Gateway | = | |
| Methode DNS-Server Konfiguration | = | statisch \| DHCPv4 \| stateless DHCPv6 \| RDNSS |
| Domainnamen | = | |
| DNS-Server | = | |
| NTP-Server | = | |
| DHCP-Server | = | |
| ggf. DHCP-Relay | = | |

Hinweis: Der Recursive DNS Servers Standard (RDNSS; RFC 6106) wird derzeit nur von wenigen Betriebssystemen (aktuellen Linux Distributionen) unterstützt. Des Weiteren können keine weiteren Dienste wie z. B. NTP, mit Hilfe von RDNSS konfiguriert werden.

**Stateful DHCPv6:**

| | | |
|---|---|---|
| DHCPv6-Server | = | |
| Adresspool für Klienten | = | |
| DNS-Server | = | |
| NTP-Server | = | |
| ggf. DHCP-Relay | = | |

*Hinweise*:

- DHCPv6 unterstützt derzeit keine Konfiguration von Default-Gateways auf den Klienten.
- Falls Stateful DHCPv6 verwendet wird, so muss autonomous address configuration in RAs deaktiviert sein.

**Betriebssystem:**

| | | |
|---|---|---|
| Dual-Stack-Betrieb ist vom vorhandenen Betriebssystem in der installierten Version bereits unterstützt und aktiviert? | = | ja / nein |
| IPv6 ist auf dem Host konfiguriert und aktiviert? | = | ja / nein |

**Software auf den Klienten:**

An dieser Stelle sollte überprüft werden, ob die verwendete Software und Anwendungen IPv6 bzw. den Dual-Stack Betrieb unterstützt.

| | | |
|---|---|---|
| Wichtige/kritische Software: | = | |
| | | |
| | | |

**Sicherheitskomponenten:**

| | | |
|---|---|---|
| Dual-Stack-Betrieb ist von der vorhandenen Firewall in der installierten Version bereits unterstützt und aktiviert/konfiguriert? | = | ja / nein |
| Paket Filter und Proxy-Server unterstützen den Betrieb von Dual-Stack und sind dementsprechend konfiguriert und aktiviert? | = | ja / nein |

## 13.12. Klienten.P - Prüfung der Migration

Empfehlung: Starten Sie die Hosts nach Abschluss aller Migrationsschritte einmal neu.

Zu überprüfen ist:

- Sind die erwarteten IPv4 und IPv6 Adressen konfiguriert?
  (GUA, Default-Gateway, DNS usw.)
- Können über die IPv4 als auch die IPv6 Adresse Verbindungen zu benachbarten Hosts aufgebaut werden?
- Werden DNS-Anfragen für IPv4- und IPv6-Hosts/Domänen beantwortet?
- Können Webseiten (IPv4- und IPv6-only) geöffnet werden?
- Funktionieren die genutzten Programme und Anwendungen noch wie gewohnt?

Bei einem Dual-Stack-Host kann nicht zuverlässig vorausgesagt werden, ob für eine Verbindung IPv4 oder IPv6 verwendet wird, da dies von der Kombination aus Netzinfrastruktur, Betriebssystem und Anwendungssoftware anhängt.

Bei der Durchführung von Test mit Netzwerktools sollte daher wenn möglich explizit ein IP-Protokoll angegeben werden (durch Auswahl des Tools oder entsprechende Parameter).

Weitere Hinweise können dem Anhang III: Technische Hinweise entnommen werden.

## Webserver.E (Beispiel) - Erfassung der Ist-Situation

**Netzwerk**

| | | |
|---|---|---|
| IPv4-Präfix und Netzmaske | = | 10.0.150.0/24<br>255.255.255.0 |
| IPv4 Default Gateway Adresse | = | 10.0.150.1 |
| ggf. Name des Subnetzes | = | rz_web |
| ggf. VLAN Tag | = | 475 |
| spezielle Routen | = | route add –net 10.0.99.0 netmask 255.255.255.0 gw 10.0.100.110 |
| bestehende ACLs | = | Keine |

**Betriebssystem**

| | | |
|---|---|---|
| Betriebssystem-Typ | = | Windows \| ~~Linux~~ \| ~~MacOS \| ...~~ |
| Distribution (Name und Version) | = | Windows Server 2008 R2 Standard Service Pack 1 |
| Kernel-Version (bei UNIX-Systemen) | = | |

**Host**

| | | |
|---|---|---|
| öffentliche IPv4-Adresse des Webservers | = | 193.175.132.91 per SNAT |
| private IPv4-Adresse des Webservers | = | 10.0.150.2 Anbindung über reverse Proxy, auf eth0 |
| optional: weitere IP-Adresse | = | 10.0.100.100 Anbindung DB-Backend über PF, auf eth1 |

**DNS**

| | | |
|---|---|---|
| Namen der vom Webserver gehosteten Domains [22] | = | ipv6.rz |
| IP-Adresse(n) der betroffenen „authorative“ DNS Server | = | 10.0.200.3 intern<br>193.175.132.89 extern |
| DNS-Namen des Webservers (intern / extern) | = | Intern: dnssrv-rz.ipv6.rz<br>Extern: mars.ipv6.rz |

**Applikation**

| | | |
|---|---|---|
| Webserver-Software | = | Microsoft IIS 7.0 |
| Version/Patchlevel der Software | = | PDV-Systems VISkompakt J2EE 4.8 (build 027) |
| Konfiguration ist gesichert unter | = | C:\Program Files (x86)\PDV-Systeme\VIS\ |

**Sicherheitskomponenten auf dem Kommunikationspfad zum Gateway-Router**

| | | |
|---|---|---|
| ALG / Proxy | = | 10.0.150.2 Anbindung Webserver<br>10.0.200.3 Anbindung Firewall |
| Paketfilter / Firewall | = | 10.0.200.1 Anbindung Proxy<br>193.175.132.83 Anbindung Internet |

[22] FQDN, Fully Qualified Domain Name.

## 13.13. Webserver.M (Beispiel) - Migrations-Schritte

**WAN-Zugang**

| | | |
|---|---|---|
| Vom Webserver genutzter WAN-Zugang (Internet-Zugang) ist bereits Dual-Stack fähig (IPv4/IPv6) | = | ja / ~~nein~~ |

*Falls nein, führen Sie zuerst dort eine Migration durch.* Siehe dazu **Checkliste Netzinfrastruktur**.

**Adresskonzept**

*Falls kein Adresskonzept vorhanden ist, sollte zunächst eins erstellt werden.*
Siehe dazu die **Checkliste Netzinfrastruktur**.

Folgende neue Werte sind zu definieren und zu notieren:

| | | |
|---|---|---|
| IPv6-Präfix des IPv6-Netzwerkes für den Webserver | = | 2001:638:806:f3a1::/64 |
| IPv6 Default Gateway Adresse (kann auch link-lokal sein) | = | 2001:638:806:f3a1::1 |
| Art der Verteilung bzw. Konfiguration der IPv6 Adressen | = | Statische Konfiguration / ~~Stateful DHCP~~ |

**Netzwerk**

| | | |
|---|---|---|
| alle IP-Subnetze zwischen WAN-Zugang und dem Netzwerk, in dem sich der Webserver befindet, sind IPv4-IPv6 Dual-Stack-fähig | = | ja / ~~nein~~ |

*Falls nein, führen Sie zuerst dort eine Migration durch.* Siehe dazu die vorangegangene **Checkliste Netzinfrastruktur**.

**Betriebssystem**

| | | |
|---|---|---|
| Dual-Stack-Betrieb ist vom vorhandenen Betriebssystem in der installierten Version bereits unterstützt und aktiviert | = | ja / ~~nein~~ |
| IPv6 ist auf dem Webserver-Host konfiguriert und aktiviert | = | ja / ~~nein~~ |

*Hinweis: Falls der Webserver auf einer virtuellen Maschine läuft, muss auch die Virtualisierungs-Lösung für IPv4/IPv6 Dual-Stack-Betrieb frei geschaltet werden.*

**Host**

| | | |
|---|---|---|
| öffentliche IPv6-Adresse des Webservers | = | 2001:638:806:f3f1::2 |
| interne IPv6-Adresse des Webservers | = | 2001:638:806:f3a1::2 auf eth0, Anbindung über reverse Proxy |
| optional: weitere IPv6-Adresse | = | 2001:638:806:f311::100 auf eth1,Anbindung DB-Backend über PF |

*Hinweis: Je nach gewählter Technik zur Verteilung der IPv6-Adressen muss diese Adresse noch auf dem Webserver selbst oder auf dem entsprechenden System (z. B. DHCPv6 Server oder Management-System) eingetragen werden.*

**DNS**

Der Webserver sollte unter IPv6 genauso wie unter IPv4 heißen, z. B. www.example.com .

Damit sind beide IP-Adressen (IPv4 und IPv6) für denselben Hostnamen abzuspeichern.

| | | |
|---|---|---|
| Für die vom Webserver gehosteten Domains sind zusätzlich neue AAAA Records mit der neuen IPv6-Adresse auf dem entsprechenden „authorative“ DNS-Server(n) angelegt. (beachte ggf. vorhandene DNS Zone Files oder mehrere DNS Server!) | = | ja / ~~nein~~ |
| Auf dem DNS-Server ist zusätzlich zum A-Record ein AAAA-Record für den **Hostnamen** des Webservers eingetragen. | = | ja / ~~nein~~ |
| Auf dem Webserver sind die IPv6-Adressen der zu nutzenden DNS-Server konfiguriert. | = | ja / ~~nein~~ |

**Webserver-Applikation**

| | | |
|---|---|---|
| Ist die für den Webserver verwendete Software Dual-Stack-fähig und IPv6-Unterstützung durch entsprechende Konfiguration aktiviert? | = | ja / ~~nein~~ |
| Erlaubt die Webserver-Konfiguration eingehende Verbindungen über IPv4 und über IPv6? | = | ja / ~~nein~~ |
| Bei mehreren gehosteten Domains: Erlauben die vHosts-Einträge der Webserver-Konfiguration eingehende Verbindungen über IPv4 und über IPv6? | = | ja / ~~nein~~ |

**(ALG-)Firewall und IDS**

| | | |
|---|---|---|
| Vorhandene Filterregeln für IPv6-Datenverkehr zum/vom Webserver sind so konfiguriert, dass sie ein zu IPv4 analoges Verhalten für IPv6-Anfragen aufweisen? | = | ja / ~~nein~~ |

## 13.14. Webserver.P (Beispiel) - Prüfung der Migration

**Migration IPv4-only Webserver zu Dual Stack**

*Empfehlung: Starten Sie den Webserver **Host** nach Abschluss aller Migrationsschritte einmal neu.*

Zu überprüfen ist:

- Sind die erwarteten IPv4 und IPv6 Adressen korrekt konfiguriert? (GUA; Default-GW; DNS usw. )
- Können sowohl über die IPv4- als auch die IPv6-Adresse Verbindungen zu anderen IPv4/IPv6-Hosts aufgebaut werden?
- Werden DNS-Anfragen für IPv4- und IPv6-Domänen beantwortet?
- Können Webseiten (IPv4-only und IPv6-only) erreicht werden?
- Funktionieren die genutzten Programme/Anwendungen noch wie gewohnt?
- Verbindungen zum migrierten Webserver überprüfen:
    - Von Extern („über das Internet“) und von Intern (aus dem Intranet)
    - „IPv4-only“-Klient/„IPv6-only“-Klient/IPv4-IPv6-Dual-Stack-Klient
    - Mit diversen Web-Browsern
    - Mit diversen Betriebssystemen
    - Für jede von dem Webserver gehostete Domain
    - Für mehrere wichtige URLs („/“ und ausgewählte Unterverzeichnisse; ggf. einen „Web-Crawler“ nutzen)
    - Funktionalität von Webseiten überprüfen, z. B. Formularseiten
- Dabei ist es sinnvoll, mehrere Kombinationen von Webbrowser, Betriebssystem und mehrere verschiedene IP-Subnetze (intern und extern) für Test-Anfragen an den Webserver zu nutzen.

Weitere Hinweise können dem Anhang III - Technische Hinweise entnommen werden.

**Performance** überprüfen (z. B. Herunterladen der kompletten Startseite):

| | | |
|---|---|---|
| mit IPv4-only-Klient | = | funktioniert |
| mit IPv6-only-Klient | = | funktioniert |
| mit Dual-Stack-Klient | = | funktioniert |

Für den Fall von Fehlern bei o.g. Prüfungen werden folgende Tests empfohlen:

| | | |
|---|---|---|
| ping6 auf die IPv6 Adresse des Webservers | = | ja / ~~nein~~ |
| traceroute6 auf die IPv6 Adresse des Webservers | = | ja / ~~nein~~ |
| nslookup / dig -6 auf die DNS Namen der gehosteten Websites | = | ja / ~~nein~~ |
| TCP connect über IPv6, z. B. via “telnet6 <IPv6-Adresse> 80” | = | ja / ~~nein~~ |
| Ausgabe von „ipconfig“ und „route“ auf dem Webserver ansehen | = | ja / ~~nein~~ |
| wget/curl/telnet zum Server und herunterladen einzelner Webseiten | = | ja / ~~nein~~ |

# 14. Anhang II: IPv6-Migrationsleitlinie

Im Forschungsprojekt „IPv6 für die Öffentliche Verwaltung“ wurden neben der Entwicklung von Profilen in den Bereichen Hardware und Software auch Migrationsexperimente durchgeführt, die sich an den Netzwerkstrukturen der Öffentlichen Verwaltung (ÖV) orientieren. Darüber hinaus wurde hierbei auch das Softwareportfolio der ÖV beachtet. Mit den gewählten Anwendungen werden im kommunalen Umfeld Fachverfahren betrieben, die mittelfristig in eine IPv6-fähige Umgebung überführt werden sollen.

In diesem Anhang werden Empfehlungen zur technischen Einführung von IPv6 in der öffentlichen Verwaltung zusammenfassend dargestellt. Der Schwerpunkt liegt dabei auf der Migration zu einer IPv4/IPv6-Dual-Stack-Netzinfrastruktur und dem Betrieb wichtiger Dienste darin.

Ein Dual-Stack-Betrieb wird auf absehbare Zeit notwendig sein im DMZ-Server-Bereich, um IPv4- und IPv6-Anfragen gleichermaßen beantworten zu können und für interne Systeme, um sowohl neue Klienten als auch Legacy-Komponenten zu unterstützen, bis deren Lebenszyklus abgelaufen bzw. bis sie durch IPv6-fähige Versionen ersetzt worden sind. Der langfristige Umstieg auf IPv6-only-Netzwerke steht bei diesen Empfehlungen nicht im Mittelpunkt.

Der folgende Text fasst daher die wichtigsten Ergebnisse dieses Projektes und der oben genannten Experimente so zusammen, dass sie als generelle Leitlinien und technische Empfehlungen im Rahmen einer IPv6-Migration dienen können. Detaillierte Informationen und Motivationen zu den einzelnen Themenbereichen finden sich in den vorhergehenden Kapiteln dieses Migrationsleitfadens.

Die in diesem Dokument gewählten Kategorisierungen ***muss***, ***sollte*** und ***darf*** weichen bewusst von der Bedeutung in Normen und Beschaffungsvorgängen ab und werden hier aus einer sowohl technisch als auch zum Teil administrativ motivierten Perspektive heraus definiert.

Im Folgenden stellen wir hier die Definition der verschiedenen Empfehlungs-Stufen gegenüber, um möglichen Fehlinterpretationen vorzubeugen:

**muss (verpflichtend)**

Die beschriebene Eigenschaft oder das Vorgehen muss in dieser Form oder Abfolge aus technischen oder aus administrativen Gründen umgesetzt werden, da anderenfalls das gewollte Verhalten nicht erreicht werden kann. Es handelt sich dann hierbei um eine absolut gültige und normative Festlegung bzw. Anforderung.

[Negation: „darf nicht“]

**sollte (empfohlen)**

Aus den technischen Experimenten heraus hat sich diese Konfiguration oder Vorgehensweise als sicher und sinnvoll erwiesen. In Abhängigkeit der Gegebenheiten und Anforderungen vor Ort kann hiervon auch abgewichen werden.

[Negation: „sollte nicht“]

**darf (optional)**

Dieses Wort bedeutet, dass die Eigenschaften oder Vorgehensweisen fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

[Negation: keine, da ‘optional‘ auch schon die Möglichkeit beinhaltet, etwas nicht umzusetzen oder anzuwenden]

[In anderen deutschen Übersetzungen wird auch „kann“ verwendet; dies wird in diesem Dokument nicht verwendet, da es mehrdeutig ausgelegt werden kann].

Die generellen Vorgehensweisen und Regelungen zu Netz-Architekturen und Sicherheit aus [ISI_LANA] und [ISI_S] sind, wo erforderlich, weiterhin anzuwenden und werden hier nicht weiter ausgeführt.

Die hier zu IPv6 ausgesprochenen Empfehlungen sind in verschiedene Gebiete gruppiert und werden jeweils kurz eingeleitet oder erläutert. Die eigentlichen Empfehlungen sind mittels der Anforderungsgrade („muss“, „sollte“, „darf“) formuliert und kursiv hervorgehoben. Der strikte Anforderungsgrad („muss“) wird in diesen Empfehlungen nur verwendet, wenn es technisch oder administrativ unbedingt notwendig ist, die Empfehlung einzuhalten.

Generell sollten die genannten Empfehlungen so wie beschrieben berücksichtigt werden, allerdings kann es aus organisatorischen, wirtschaftlichen oder anderen Gründen in Einzelfällen notwendig sein, andere Lösungen einzusetzen. In einem solchen Fall sind die Hintergründe für das Abweichen von der vorliegenden Empfehlung sorgfältig zu analysieren und zu dokumentieren. Es dürfen in begründeten Fällen Ausnahmen von einzelnen Empfehlungen gemacht werden.

Für die Ausarbeitung der Empfehlungen wurden eine Migrationsarchitektur und eine Zielarchitektur entwickelt, die den Notwendigkeiten und Möglichkeiten von IPv6 Rechnung tragen:

***Migrationreferenzsarchitektur:***
Umfasst einen Vorschlag in Hinblick auf den aktuellen Stand und die speziellen Ziele und Vorgaben in der öffentlichen Verwaltung Deutschlands. Die Migrationsarchitektur spiegelt eine bestehende ÖV wieder, ergänzt um den IPv6-Transport.

***Zielarchitektur:***
Umfasst eine IPv6-Netz-Architektur unter Ausnutzung neuer technischer Möglichkeiten des IPv6-Protokolls. Die Zielarchitektur stellt ein neu aufgebautes bzw. restrukturiertes System dar, in dem IPv4 im Wesentlichen nur noch in nicht migrierbaren Inseln verwendet wird.

Für Details zu diesen Architekturen siehe Abschnitt 3.6 „IPv6-Migrationsreferenzarchitektur“ in diesem Dokument.

IPv6 besitzt ein Potenzial zur Vereinfachung bestimmter Aspekte, z. B. durch den Wegfall von NAT und die nicht mehr vorhandene Adressknappheit bei globalen Adressen. Des Weiteren kann durch die gezielte, strukturierte Einführung von IPv6 ein Sicherheitsgewinn erzielt werden, indem z. B. ein übersichtlicheres Adress-Schema genutzt wird (siehe Abschnitt 6.3), als es aktuell mit IPv4 und Netzwerk-Adress-Umsetzung (Network Address Translation, NAT) möglich ist.

*Die nachfolgenden Empfehlungen beziehen sich, ausgehend von der Migrations-referenzarchitektur, auf die verschiedenen Schritte im Migrationsprozess.*

## 14.1. Vorgehen bei der Migration

Für die Vorbereitung und Durchführung der Migration sind die Checklisten in diesem Leitfaden von zentraler Bedeutung, beginnend mit der Checkliste „Migrations-Planung“ aus Anhang I. Die im Folgenden genannten Empfehlungen unterstützen diese Migrations-Prozesse für eine sichere und strukturierte Umstellung der IT-Infrastruktur. Es wird empfohlen, sich im Vorfeld einer Migration mit diesen Empfehlungen und den Auswirkungen auf die eigene Infrastruktur auseinander zu setzen, um sich wichtiger Fragen, etwa zu den möglichen Arten der Adressvergabe, bewusst zu werden.

- *Eine Migration von IP-Netzen (IPv4-only nach Dual-Stack, ebenso wie IPv4-only nach IPv6-only) **sollte** immer stufenweise vom WAN-Anschluss her (z. B. DOI, Internet) über die DMZ-Netze hin zu den Netzwerken mit Arbeitsplätzen (Klienten) erfolgen.*

- Folgende Reihenfolge wird dafür empfohlen:

    1. *Zuerst **sollte** IPv6 am WAN-Anschluss bereitgestellt werden.*
        - *IPv6 **sollte** dringend in der Form „native IPv6“ bereitgestellt werden.*
        - *Alternativ **darf** IPv6 auch über sichere Tunnelbroker bezogen werden.*
            - *Dabei **müssen** feste Adressen für die beiden Tunnelendpunkte (typisch: Tunnel-Server und ÖV-Gateway) verwendet werden.*
            - *Als Tunneltechnik **sollte** eine 6in4-Encapsulierung (IP-in-IP-Tunnel) verwendet werden.*
            - *Andere Tunneltechniken wie 6to4 und Teredo **dürfen** aus Sicherheitsgründen **nicht** verwendet werden.*
    2. *Nach diesem Schritt **sollten** die DMZ-Netze und die internen Server-Netze eines nach dem anderen migriert werden.*
    3. *Danach **muss** eine Migration des DNS-Dienstes erfolgen, damit auch AAAA-Records verarbeitet und an Klienten ausgeliefert werden können.*
    4. *Danach **sollten** die vorhandenen Klienten-Netze migriert werden.*
        - *DNS-Antworten mit IPv6-Adressen (AAAA-Records) **sollten** nur in bereits zu IPv4/IPv6-Dual-Stack oder zu IPv6-only migrierte Subnetze ausgeliefert werden.*
    5. *Als Letztes **sollten** die Management-Netze umgestellt werden.*

- *„Isolierte IPv6-Inseln“ mit globalen IPv6-Adressen **sollten** vermieden werden.*

  - Mit isolierten IPv6-Inseln sind IP-Subnetze gemeint, in denen bereits IPv6-Präfixe verteilt werden, aber deren Klienten mit IPv6 noch nicht dritte Netze oder das Internet erreichen können. In solchen Subnetzen kann es auf Klienten zu langen Timeouts beim Zugriff auf Dual-Stack-Server kommen, bevor ein Rückgriff auf eine IPv4-Verbindung versucht wird.
  - *Werden IPv6-Inseln explizit gewünscht, so **sollten** dort nur Link-lokale IPv6-Adressen verwendet werden.*

- *Paketbasierte IPv4/IPv6-Protokollumsetzer (protocol translation, PT) **sollten nicht** eingesetzt werden.*

  - *Eine Umsetzung zwischen IPv4 und IPv6 **sollte**, wo es notwendig ist, durch Proxies erfolgen, vorausgesetzt, das verwendete Dienst-Protokoll lässt sich über einen Proxy betreiben (wie z. B. bei http).*
    - Siehe für Details auch im Glossar zu den Unterschieden zwischen Protokollumsetzer und Proxy (trennt IP-Verbindung auf).

- Empfohlen wird nach Umstellung von WAN und DMZ auf Dual-Stack-Betrieb auch im LAN die Migration zu IPv4/IPv6-Dual-Stack.

  - *IPv4-Datenpakete und IPv6-Datenpakete **sollten** auf denselben Netzen (insbesondere auf den vorhandenen VLANs) transportiert werden.*
    - IPv4- und IPv6-Daten können technisch auch auf separate VLANs in derselben Infrastruktur verteilt werden; hierfür müssten jedoch alle beteiligten Switches protocol-based VLAN-tagging unterstützen, und der Verwaltungsaufwand für die Dopplung der VLANs ist deutlich höher. *Separate VLANs für IPv4 und IPv6 werden daher **nicht empfohlen***.
    - *Physikalisch separate LANs für IPv4 und IPv6 werden auf Grund des dafür notwendigen Aufwandes ebenfalls **nicht empfohlen**.*
    - *In Konsequenz wird auch der Betrieb eines großen Layer2-VLANs für IPv6 mittels der in Abschnitt 7.1.2 beschriebenen Technik **nicht empfohlen**.*

- *VLAN-Tagging (802.1q) direkt auf Endsystemen (insbesondere auf Arbeitsplätzen) **sollte nicht** genutzt werden.*

  - Es erhöht den Aufwand für das Netzwerk-Management, und potenzielle Fehlkonfigurationen im Zusammenhang damit sind nur schwer einzugrenzen.
  - Ausnahmen sind ausgewählte *Server-Systeme*, bei denen eine Konfiguration mit VLAN-Tagging direkt auf dem Server Sinn machen kann. Dies ist im Einzelfall zu entscheiden.

- *Ein IPv6-only-Betrieb wird zurzeit für die Verwendung in vorhandenen operativen Netzwerken noch **nicht empfohlen**.*

    - Bei der Vielzahl an vorhandenen Komponenten, Diensten und Software in einer gewachsenen IT-Umgebung ist nur mit sehr hohem Aufwand sicher zu stellen, dass alle o. g. Elemente komplett ohne IPv4 auskommen können. *Es wird daher trotz des höheren Verwaltungsaufwandes ein Dual-Stack-Betrieb **empfohlen**.*
        - Bei speziellen Anwendungen, z. B. für die Voice-over-IP (VoIP) Sprachkommunikation kann es mit aktuellen Geräten sinnvoll sein, ein IPv6-only Netzwerk für diesen Zweck zu nutzen.
            - *Solch ein IPv6-only Netzwerk **sollte** als separates Netzwerk aufgebaut werden* (separates VLAN, oder physikalisch separates Netzwerk).
    - Bei komplett neu aufzubauenden Netzwerken ist es generell sinnvoll, über einen *IPv6-only-Betrieb* nachzudenken um ggf. den Verwaltungsaufwand für den IPv4-Betrieb solcher neuen Netze zu vermeiden.

## 14.2. Netzstruktur und Adressierung

### 14.2.1 Netzwerksegmentierung

Der große Adressraum von IPv6 ermöglicht eine sehr strukturierte, semantische Aufteilung der Subnetz-Nummern (siehe dazu Abschnitt 6.1). Jedes einzelne der möglichen /64 Subnetze in IPv6 stellt genug Adressen für $2^{64}$ Klienten (genauer: Schnittstellen) bereit. Ferner können mit einem typischen, 48 Bit langen IPv6-Präfix (/48) an einem Standort $2^{16} = 65536$ solcher IPv6-Subnetze genutzt werden. Für kleine Standorte sind mit einem 56 Bit langen Präfix (/56) immer noch $2^8 = 256$ IPv6-Subnetze möglich.

- *Es **sollte** bei der Migration darauf geachtet werden, dass die Komplexität eines einzelnen Migrationsvorganges nicht zu groß wird.*
    - Ggf. bietet sich eine Untergliederung in mehrere Migrationsvorgänge an (z. B. je IP-Subnetz)
- *Zur Vereinfachung der Migration **dürfen** IPv4-Netze neu strukturiert werden.*
    - Dies kann z. B. durch Zusammenfassung semantisch äquivalenter IP-Subnetze, und Konsolidierung von Adressbereichen geschehen.
    - *Diese mögliche Neustrukturierung der IPv4-Netze ist ein eigener Arbeitsschritt und **muss** sorgfältig geplant und getestet werden.*
        - *Dieser Schritt **sollte** vor einer Migration von IP-Subnetzen zu IPv4/IPv6-Dual-Stack-Betrieb durchgeführt werden.*
    - *Eine Neustrukturierung von IP-Subnetzen unter IPv6 ohne gleichzeitige Neustrukturierung auch unter IPv4 wird **nicht empfohlen.***
    - *IPv4-Netze und IPv6-Netze **sollten** möglichst semantisch deckungsgleich sein*.
        - Dadurch werden die für IPv4/IPv6 Dual-Stack-Betrieb parallel zu konfigurierenden Regeln auf Routern und auf Sicherheitskomponenten verständlicher und leichter zu warten und damit die Sicherheit erhört.
- *Große IPv6-Subnetze mit deutlich mehr als 254 Klienten **dürfen** bei IPv6 verwendet werden.*
    - *In IPv6-Subnetzen mit Klienten (Arbeitsplatzrechnern) **muss** ein /64 Präfix vergeben werden, da die niederwertigen 64 Bits der IPv6-Adresse für die Schnittstellen-Adresse (interface identifier) reserviert sind.*

- *Die Klienten in einem IP-Subnetz **müssen** semantisch gleichberechtigt sein, da Zugriffs-Regeln (ACLs) üblicherweise je Subnetz definiert werden.*

- Hinweis: Im Enterprise-Bereich sind häufig bis zu 12.000 Geräte für ein Layer-2-Subnetz möglich; entscheidend hierfür ist die Größe der MAC-Adress-Tabellen der verwendeten Switches.

- *Eine Segmentierung des Netzes einer ÖV in viele, kleine Subnetze **darf** entfallen, sofern die Klienten (je Subnetz) den gleichen Schutzbedarf besitzen.*

    - Dies reduziert die Anzahl an Subnetzen und damit den Management-Aufwand für Netze, Router und ACLs.

- *Es **sollten** die gleichen VLANs für IPv4 und IPv6 verwendet werden.*

    - Getrennte VLANs für IPv4 und IPv6 erhöhen den Wartungsaufwand und die Fehlersuche, und es müssen bei der Einführung von Netzfunktionen und Regeln immer zwei verschiedene VLANs berücksichtig werden.

- *Es **sollten** für das Routing nach Möglichkeit Protokolle der gleichen Familie (z. B. OSPF) unter IPv6 wie unter IPv4 verwendet werden.*

    - *Es **muss** für IPv6 eine Version des Routing*-Protokolls eingesetzt werden, die IPv6 unterstützt. Insbesondere ist zu prüfen, ob die verwendeten Geräte mit Routing-Funktionalität die notwendige Version unterstützen können.

- *Unterschiedliche Routing-Wege für IPv4 und IPv6 **sollten** vermieden werden.*

### 14.2.2 Adressvergabe für IPv6

#### 14.2.2.1 Für Klienten / Arbeitsplätze

- *Die IPv6-Adresskonfiguration in Klienten-Netzen **sollte** mittels Stateful DHCPv6 erfolgen.*

    - *Insbesondere wenn für Klienten die Adressvergabe für IPv4 per DHCP stattfindet, so **sollte** auch die Vergabe der IPv6-Adressen per DHCP (Stateful DHCPv6) erfolgen.*
    - *Nur in kleinen, einfach strukturierten Netzen **darf** zur Vereinfachung der IT-Infrastruktur stattdessen Stateless Address Autoconfiguration (SLAAC) verwendet werden.*
    - *Falls SLAAC eingesetzt wird, so **sollte** dieses zusammen mit Stateless DHCPv6 betrieben werden, mit dem weitere Konfigurations-Daten verteilt werden können, wie z. B. der von den Klienten zu nutzende DNS-Server.*

- *Router/Layer3-Switches **müssen** für die IPv6-Adressverteilung die IPv6-DHCP-Relay-Funktion unterstützen, wenn ein zentraler DHCP-Server eingesetzt wird.*

  Zufällige Schnittstellenadressen (interface identifier) können zusammen mit SLAAC über IPv6 Privacy Extensions (PEX) realisiert werden. Wenn kein SLAAC verwendet wird, sondern Stateful DHCPv6, so kann durch eine entsprechende Konfiguration auf dem DHCP-Server eine Pseudo-Randomisierung der Schnittstellenadressen nachgebildet werden (kurze Adress-Lease-Zeit, Vergabe der Adressen aus einem genügend großen IPv6-Adress-Pool).

- *Für Klienten **sollten** Privacy Extensions (PEX) standardmäßig aktiviert sein, falls SLAAC als Technik zur Generierung der IPv6-Adressen gewählt wurde.*
  - *Für Klienten, die aus technischen Gründen eine feste Adresse nutzen sollen, **müssen** Privacy Extensions deaktiviert sein.*

- *Von der MAC-Adresse oder einer Geräte-ID abgeleitete (EUI-64) IPv6-Adressen **sollten nicht** verwendet werden.*

  Falls Klienten auch im DNS registriert sein sollen, so ermöglicht Stateful DHCP hierfür eine vereinfachte zentrale Steuerung (Updates) der DNS-Einträge für Klienten auf dem DNS-Server, da die Einträge in diesem Fall zentral durch den DHCP-Server aktualisiert werden können, anstatt durch die Klienten selbst.

#### 14.2.2.2 Für Server

- *Server **müssen** für jede Schnittstelle in einem IPv6-Subnetz eine festgelegte, unveränderliche[23] IPv6-Adresse verwenden.*
  - *Die IPv6-Adressvergabe für Server **sollte** per DHCPv6 erfolgen.*
    - *Alternativ **darf** die IPv6-Adresse auch direkt auf dem Server statisch konfiguriert werden.*
  - *Die vergebenen IP-Adressen **müssen** im DNS-Server als A- und AAAA-Records eingetragen werden.*
    - *AAAA-Records **sollten** erst dann für einen Server im DNS eingetragen werden, wenn der Server, dessen Dienste und der Zugang zum Servernetz bereits alle IPv6 unterstützen.* Damit werden unnötige Timeouts beim Zugriff durch IPv6-fähige Klienten vermieden.

- *Dienste **sollten** nur an die IPv6-Adresse gebunden werden, über die der Dienst erreichbar sein soll.*

[23] Unveränderlich, bis auf eine mögliche Renummerierung von ganzen Netzen.

- *Das Multihoming von Servern, also der Anschluss des Servers in mehreren IP-Subnetzen, **sollte** vermieden werden.*
- *Server **sollten** unter IPv4 und IPv6 unter dem gleichen Namen zu erreichen sein.*
- *Server **sollten** zur Namensauflösung auch die IPv6-Adressen der lokalen DNS-Server kennen (sobald letztere auch über IPv6 DNS-Anfragen entgegen nehmen können).*

#### 14.2.2.3 Für Endsysteme im Allgemeinen

- *Dual-Stack-Endsysteme **sollten** (je Schnittstelle) neben der IPv4-Adresse und der Link-lokalen IPv6-Adresse nur eine weitere aktive Unicast-IPv6-Adresse haben.*
    - *Diese IPv6-Adresse **sollte** vom Typ GUA oder ULA sein (siehe Kapitel 6.1).*
    - *Es **dürfen** jedoch auch mehrere zusätzliche IPv6-Adressen auf einer Schnittstelle konfiguriert werden (z. B. eine GUA und eine ULA oder zwei GUA)*
        - *In solch einem Fall **müssen** alle diese IPv6-Adressen zur gleichen Sicherheitszone gehören.*
        - *Diese IPv6-Adressen **müssen** unterschiedliche Präfixe besitzen.*
        - *Der Subnetz-Teil der Präfixe (siehe Kapitel 6) **darf** jedoch übereinstimmen.*

#### 14.2.2.4 ICMP6

- Für ICMPv6 sind nicht alle Regeln von ICMPv4 eins-zu-eins anwendbar.
    - *Insbesondere ICMPv6-Nachrichten für die Erkennung der maximal möglichen Paketgröße auf einem Datenpfad (path MTU[24] discovery) und Neighbor Detection (ND) Nachrichten **dürfen nicht** generell blockiert werden.*
    - Technische Details hierzu sind in [ISI-LANAv6] und in [RFC4890] zu finden.

### 14.2.3 Namensauflösung (DNS)

Das Domain Name System (DNS) ist ein zentraler Bestandteil des Internet-Kommunikationssystems. Im DNS-System wurde für IPv6 ein neuer Eintrag definiert: Anstatt A-Records werden für IPv6 die größeren AAAA-Records verwendet. Das DNS-Protokoll erlaubt die Abfrage von IP-Adressen über das IPv4- und das IPv6-Protokoll, unabhängig vom abgefragten Adresstyp (A oder AAAA).

[24] Maximum transmission unit, maximal in einem Datagramm transportierbare Datenmenge in Bytes

- *DNS-Server **müssen** AAAA-Records verwalten, lesen und ausliefern können.*
- *DNS-Server **müssen** Anfragen sowohl über IPv4 als auch über IPv6 annehmen und beantworten.*
    - Hinweis: Es ist für den DNS-Server nicht direkt sichtbar, wie ein Klient angebunden ist, da Klienten selbst entscheiden, über welche IP-Version sie den DNS-Server ansprechen.
- *Für bereits im DNS eingetragene und nach der Migration Dual-Stack-fähige Hosts **müssen** sowohl IPv4- als auch IPv6-Adressen im DNS-Server hinterlegt sein.*
- *Im DNS eingetragene Hosts **sollten** unter IPv4 und IPv6 unter demselben Hostnamen abgelegt sein.*
- *DNS-Server **sollten nicht** mit AAAA-Records an Klienten antworten, die bekanntermaßen nur in einem IPv4-only Subnetz angeschlossen sind*.
    - Auf einem Klienten mit einem IPv6-aktivierten Betriebssystem könnten ansonsten Timeout-Probleme auftreten.
- *DNS-Server **müssen** so für IPv4 und für IPv6 konfiguriert sein, dass sie ein korrektes Reverse Lookup ermöglichen.*
    - Dies ist z. B. zwingend notwendig für die korrekte Kommunikation zwischen Mail-Servern (genauer: zwischen Mail Transfer Agents (MTA)).

## 14.3. Sicherheitskomponenten

### 14.3.1 Proxies / ALGs

- *Proxies (für HTTP, HTTPS, SMTP, etc.) **müssen** überall dort genutzt werden, wo es aus Gründen der Sicherheit, Performanz (z. B. durch Caching) und/oder Protokollierung des Datenverkehrs notwendig ist.*
- *Eingesetzte Proxies und ALGs **müssen** Dual-Stack-fähig sein.*
- *Der Aufbau von IP-Verbindungen vom Internet aus zu Klienten **muss** für IPv4 und für IPv6 gleichermaßen überall dort unterbunden werden, wo dies nicht erlaubt ist.*
    - Für betrieblich notwendige Tunnel-Verbindungen (z. B. LAN-zu-LAN-Kopplung zu Netzen mit Fachanwendungen) **muss** u. U. an den Tunnel-Endpunkten von der Regel „keine direkte Ende-zu-Ende-Verbindung“ abgewichen werden.
- Die weitere Verbreitung von IPv6 eröffnet in der Zukunft das Potential für neue, innovative Internetanwendungen. Diese werden möglicherweise

auch direkte IP-Verbindungen benötigen. *Hierfür **muss** im Einzelfall entschieden werden, ob diese Verbindungen zugelassen werden dürfen*.

### 14.3.2 Paketfilter / Firewalls

- Aktuell sind bei fast allen Firewalls und Paketfiltern für IPv4 und IPv6 zwei unabhängige Regelwerke zu pflegen, welche nicht automatisch synchronisiert werden.
    - *Es **müssen** für IPv6 Regeln erstellt werden, die semantisch zu den vorhandenen Regeln für IPv4 äquivalent sind.*
    - *Es **müssen** Regeln definiert werden, die das gleiche Sicherheitsniveau unter IPv6 gewährleisten wie unter IPv4.*
- Es dürfen aus Sicherheitsgründen außer von vorhandenen IPv6-Tunnel-Routern keine anderen Hosts Tunnel in das IPv6-Internet aufbauen.
    - *Nicht erlaubte Tunneltechniken (6to4, Teredo) **müssen** spätestens am Perimeter-Router blockiert werden.*
- *Datenpakete mit IPv6-Adressen, welche nur zur internen Verwendung in einer ÖV verwendet werden sollen, **müssen** am Perimeter-Router verworfen werden.*
- *Die gewünschte globale Erreichbarkeit (oder Nicht-Erreichbarkeit) von Servern, Diensten und Klienten **muss** durch Zugriffsregeln (Access Control Lists, ACLs) gesteuert werden.*
    - Dies betrifft in erster Linie die Filter-Regeln auf vorhandenen Paketfiltern, aber auch den Einsatz von Filter-Regeln auf den Endsystemen, sofern dort Paketfilter („personal firewall“) zum Einsatz kommen.

### 14.3.3 Switches und Router

Ein unterschiedliches Routing von IPv4-Datenpaketen im Vergleich zu IPv6-Datenpaketen kann zu Störungen in Form von Timeouts auf Klienten führen.

- *Ein unterschiedliches Routing von IPv4- und IPv6-Datenpaketen **sollte** vermieden werden.*
- *Ein asymmetrisches Routing von IP-Datenpaketen **sollte** vermieden* werden.

### 14.3.4 Sicherheitsmechanismen im Endsystem

Zusätzlich zu sicheren Netzen müssen sichere Endsysteme bereitgestellt werden. Dies gilt jetzt und in Zukunft umso mehr, da sich ein Paradigmenwechsel von ortsbezogener Sicherheit zur gerätebezogener Sicherheit vollzieht und dieser durch die Einführung von IPv6 beschleunigt wird.

Zusätzlich kann es aus administrativen Gründen sinnvoll oder notwendig sein, dass ein Klienten-System immer über die gleiche IP-Adresse erreichbar ist, unabhängig von seinem Aufenthaltsort.

- *IPv6-Tunnel-Protokolle und -Mechanismen **müssen** auf Klienten deaktiviert sein.*
    - Durch von Klienten selbst ins Internet aufgebaute Tunnel (z. B. 6to4 oder Teredo) entstehen Sicherheitslücken, und es könnten Daten über unerwünschte Netze geleitet werden.
- *IPv6 auf Klienten **sollte** vor Beginn der Migration deaktiviert werden.*
- *Auf Klienten **sollte** eine lokale Firewall genutzt werden.*
    - *Wenn vorhanden, so **muss** diese Firewall auch mit IPv6-Datenströmen umgehen können.*
    - Bei Standardbetriebssystemen für Klienten ist oft die mitgelieferte Firewall des installierten Betriebssystems in der Standard-Konfiguration bereits Dual-Stack-tauglich und sinnvoll konfiguriert.
    - *Für einige ausgewählte Systeme und Konfigurationen **sollte** exemplarisch überprüft werden, ob die installierten Regelwerke der Firewall auf dem Klienten die gleichen Schutzregeln für IPv4 und IPv6 aktiviert haben.*
- *Es **darf** auf den Klienten zusätzlich ein Intrusion-Prevention-System (IPS) eingesetzt werden.*
    - *Ist ein solches System vorhanden, so **muss** es IPv6 unterstützen.*

## 14.4. Netzwerk-Management und -Monitoring

### 14.4.1 Allgemeines

- *Die verwendeten Management-Server und die Management-Software (z. B. Nagios, Icinga, HP OpenView) **sollte** IPv6-fähig sein.*
- *Die Managementschnittstelle einer Komponente (Router, Switches, Appliances etc.) **sollte** auch über IPv6 erreichbar sein.*
    - *Management-Systeme und -Schnittstellen können nach den operativen Netzwerken (DMZ- und Klienten-Netze) auf IPv4/IPv6-Dual-Stack migriert werden.*
- *Zuerst **sollte** der Management-Server migriert werden, dann die zu managenden Komponenten.*
- *Wird ein IP-Adress-Management-System (IPAM) verwendet, so **muss** dieses IPv4 und IPv6 unterstützen.*
- *Monitoring-Systeme **müssen** auf ihre IPv6-Tauglichkeit überprüft werden.*

- *Es **sollten** alle genutzten Monitoring-Funktionen für aktive und passive Prüfungen, die bisher IPv4 nutzen, auch über IPv6 ausgeführt werden können*.
- *Wenn vom Monitoring überwachte Dienste auf IPv4/IPv6-Dual-Stack-Betrieb migriert werden, dann **sollte** auch eine zusätzliche IPv6-Prüfung im Monitoring-System hinzugefügt werden.*

### 14.4.2 SNMP

- *Es **muss** geprüft werden, ob SNMP Agenten auch über IPv6 erreichbar sind.*
  - *SNMP Agenten **sollten** auch über IPv6 erreichbar sein.*
  - Dies gilt auch für einen ggf. geforderten sicheren, verschlüsselten SNMP Zugang mittels SNMPv2c und SNMPv3.
- *In operativen IPv6-Netzwerken **sollten** von den SNMP-Agenten (insbes. auf Switches und auf Routern) auch IPv6-spezifische MIBs unterstützt werden.*

## 14.5. Infrastruktur-Dienste

### 14.5.1 Zeitsynchronisation / NTP

- *Alle lokalen NTP Server einer ÖV **müssen** über IPv4 und IPv6 erreichbar sein.*
- *Die Zeit auf einem NTP-Server **darf** durch Techniken wie GPS, DCF77 oder durch Abfrage eines ausgewählten übergeordneten NTP-Servers erfasst werden.*
- *Falls zum Zweck der Redundanz mehrere NTP Server betrieben werden, so **sollten** auf Hosts einer der ÖV alle diese NTP-Server mit ihrer IPv4- und IPv6-Adresse als mögliche Zeit-Quellen konfiguriert werden.*
  - Die ist auch zentral über geeignete Protokolle wie DHCP möglich.
- *Die Hosts einer ÖV **sollten** ihre Zeit **nicht** direkt mit externen NTP-Servern synchronisieren.*[25]

### 14.5.2 E-Mail / SMTP

- *Zur Migration vom E-Mail-Infrastrukturen auf IPv4/IPv6-Dual-Stack-Betrieb **muss** die vorhandene Software, welche für Mailserver (Mail Transfer Agent, MTA) und für Mail-Klienten eingesetzt wird, auf IPv6-Tauglichkeit überprüft werden.*

[25] Ausnahme: ausgewählte NTP-Server der ÖV selbst dürfen ihre Zeit auch von externen NTP-Servern synchronisieren.

- *Nach außen hin **muss** ein MTA auch IPv6-tauglich sein, wenn der Nachrichtenaustausch mit E-Mail-Domains in einem geografischen Raum vorkommen kann, in dem IPv6-only-MTAs zu erwarten sind (z. B. Asien).*

### 14.5.3 Verzeichnisdienste / LDAP

- *Verzeichnisdienste (z. B. LDAP-Server) einer ÖV **sollten** IPv6-tauglich sein, wenn mindestens ein nutzender Klient im IPv4/IPv6-Dual-Stack-Betrieb aktiv ist.*

    - *Diese Verzeichnisdienste **müssen** IPv6-tauglich sein, wenn mindestens ein nutzender Klient IPv6-only betrieben wird.*

# 15. Anhang III: Technische Hinweise

Dieser Anhang enthält Beispiele für die Überprüfung der IPv6-Konfiguration auf Endsystemen sowie Konfigurationsbeispiele für Infrastrukturdienste.

Das Dokument geht davon aus, dass IPv6 vom dem zu überprüfenden Host unterstützt wird und auch aktiviert ist.

## 15.1. Statische Konfiguration von IPv6-Adressen

**Debian Host** /etc/network/interfaces

```
       iface eth0 inet6 static
        address 2001:638:806:f200::3
        netmask 64
        gateway 2001:638:806:f200::1
```

**RedHat/CentOS Host** /etc/sysconfig/network-scripts/ifcfg-eth0

```
IPV6INIT=yes
IPV6ADDR=YOURIPV6ADDRESS
IPV6_DEFAULTGW=YOURGATEWAY

#IPv6 configuration
IPV6INIT=yes
IPV6ADDR=2001:638:806:f200::3/64
IPV6_DEFAULTGW=2001:638:806:f200::1
```

## 15.2. Anzeigen der IPv6-Adressen

Grundsätzlich kann man sich IPv6-Adressen mit den gleichen Kommandos wie bei IPv4 anzeigen lassen (z. B. ipconfig/ifconfig).

Das folgende Kommando zeigt ausschließlich IPv6-Adressen aller Interfaces an:

```
root@ipv6-ext-router-oev:~# ip -6 addr show
       1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
              inet6 ::1/128 scope host
          valid_lft forever preferred_lft forever
       2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
              inet6 2001:638:806:f200::3/64 scope global
                 valid_lft forever preferred_lft forever
              inet6 fe80::250:56ff:fe80:74aa/64 scope link
                 valid_lft forever preferred_lft forever
```

## 15.3. Anzeigen von IPv6-Routen und Gateways

Die folgenden Kommandos zeigen statisch konfigurierte Routen sowie das statisch vergebene Default-Gateway an:

```
root@ipv6-ext-router-oev:~# route -A inet6
Kernel IPv6 routing table
Destination                    Next Hop                   Flag Met Ref
Use If
2001:638:806:f200::/64         ::                         U    256 0
1 eth0
#Statische Routen
```

```
2001:638:806:f201::/64         2001:638:806:f2a1::2       UG   1024 0
4000 eth1
2001:638:806:f211::/64         2001:638:806:f2a1::2       UG   1024 0
16 eth1
2001:638:806:f2a1::/64         ::                         U    256 0
3 eth1
2001:638:806:f2a2::/64         2001:638:806:f2a1::2       UG   1024 0
9 eth1
2001:638:806:f300::/64         ::                         U    256 0
2 eth4
2001:638:806:f300::/56         2001:638:806:f300::3       UG   1024 0
1742 eth4
fe80::/64                      ::                         U    256 0
0 eth0
fe80::/64                      ::                         U    256 0
0 eth2
fe80::/64                      ::                         U    256 0
0 eth4
fe80::/64                      ::                         U    256 0
0 eth1
#Statisch konfiguriertes Default Gateway
::/0                           2001:638:806:f200::1       UG   1    1
6238 eth0
::/0                           ::                         !n   -1  1
13298 lo
```

Alternativ:

```
root@ipv6-ext-router-oev:~# ip -6 route show
2001:638:806:f200::/64 dev eth0  proto kernel  metric 256  mtu 1500
advmss 1440 hoplimit 0
2001:638:806:f201::/64 via 2001:638:806:f2a1::2 dev eth1  metric 1024
mtu 1500 advmss 1440 hoplimit 0
2001:638:806:f211::/64 via 2001:638:806:f2a1::2 dev eth1  metric 1024
mtu 1500 advmss 1440 hoplimit 0
2001:638:806:f2a1::/64 dev eth1  proto kernel  metric 256  mtu 1500
advmss 1440 hoplimit 0
2001:638:806:f2a2::/64 via 2001:638:806:f2a1::2 dev eth1  metric 1024
mtu 1500 advmss 1440 hoplimit 0
2001:638:806:f300::/64 dev eth4  proto kernel  metric 256  mtu 1500
advmss 1440 hoplimit 0
2001:638:806:f300::/56 via 2001:638:806:f300::3 dev eth4  metric 1024
mtu 1500 advmss 1440 hoplimit 0
fe80::/64 dev eth0  proto kernel  metric 256  mtu 1500 advmss 1440
hoplimit 0
fe80::/64 dev eth2  proto kernel  metric 256  mtu 1500 advmss 1440
hoplimit 0
fe80::/64 dev eth4  proto kernel  metric 256  mtu 1500 advmss 1440
hoplimit 0
fe80::/64 dev eth1  proto kernel  metric 256  mtu 1500 advmss 1440
hoplimit 0
default via 2001:638:806:f200::1 dev eth0  metric 1  mtu 1500 advmss 1440
hoplimit 0
```

## 15.4. Konfiguration statischer Routen

```
ip -6 route add 2001:638:806:f2a2::/64 via 2001:638:806:f2a1::2 //Netz
zwischen Proxy und Router intern
ip -6 route add 2001:638:806:f201::/64 via 2001:638:806:f2a1::2 //Netz
Klienten
ip -6 route add 2001:638:806:f211::/64 via 2001:638:806:f2a1::2 //Netz
interne Server
```

Hinweis: Statische Routen sind nach einem Reboot nicht mehr existent. Daher müssen Sie z. B. beim Aktivieren der Interfaces geladen werden. Der folgende Abschnitt zeigt einen beispielhaften Auszug aus der Datei /etc/network/interfaces:

```
iface eth1 inet6 static
address 2001:638:806:f2a2::2
netmask 64
post-up route -A inet6 add 2001:638:806:f3f1::/64 gw 2001:638:806:f300::3
pre-down route -A inet6 del 2001:638:806:f3f1::/64 gw
2001:638:806:f300::3
```

## 15.5. Überprüfung der IPv6-Konnektivität

Erreichbarkeit des Gateways mit dem Kommando ping überprüfen:

```
root@ipv6-ext-router-oev:~# ping6 –c 1 2001:638:806:f200::1
PING 2001:638:806:f200::1(2001:638:806:f200::1) 56 data bytes
64 bytes from 2001:638:806:f200::1: icmp_seq=1 ttl=64 time=0.349 ms

--- 2001:638:806:f200::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.349/0.349/0.349/0.000 ms
```

Hinweis: Bei Klienten, die Ihr Default-Gateway per Router Advertisements konfigurieren, handelt es sich bei der IPv6-Adresse des Gateways um die Link-lokale-Adresse des Routers (Präfix beginnt mit fe80::/64).

Folgendes Kommando zeigt die IP-Adressen der benachbarten Hosts:

```
root@ipv6-ext-router-oev:~# ip -6 neigh show
2001:638:806:f2a1::2 dev eth1 lladdr 00:50:56:80:32:58 STALE
2001:638:806:f200::1 dev eth0 lladdr 00:11:13:93:00:12 router REACHABLE
2001:638:806:f300::3 dev eth4 lladdr 00:50:56:80:00:97 router STALE
```

Hinweis: STALE bedeutet, dass der Host erreichbar war, aber die Adresse länger nicht genutzt wurde.

Zur Kontrolle des Routings eignen sich Tools wie tracert, traceroute6 oder tracepath6. Mit Hilfe von tcpdump können IPv6-Pakete auf einem Netzwerkinterface anzeigt werden:

```
tcpdump -n icmp6      //Zeigt nur ICMPv6 Pakete
tcpdump -n -i <dev> ip6      //Zeigt sämtlichen IPv6 Traffic auf dem
Interface an
```

## 15.6. Überprüfung von DNS

Mit folgendem Kommando wird ein AAAA-Record über IPv4 abgefragt:

```
root@ipv6-ext-router-oev:~# nslookup -q=aaaa ipv6.google.com
Server:         10.147.9.3
Address:        10.147.9.3#53

Non-authoritative answer:
ipv6.google.com canonical name = ipv6.l.google.com.
ipv6.l.google.com       has AAAA address 2a00:1450:4001:c01::68
```

Falls der DNS-Server auch über IPv6 zu erreichen ist sollte dies explizit überprüft werden:

```
root@ipv6-ext-router-oev:~# dig aaaa ipv6.google.com @2001:638:806:9::3

; <<>> DiG 9.7.0-P1 <<>> aaaa ipv6.google.com @2001:638:806:9::3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23628
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;ipv6.google.com.               IN      AAAA

;; ANSWER SECTION:
ipv6.google.com.        421432  IN      CNAME   ipv6.l.google.com.
ipv6.l.google.com.      300     IN      AAAA    2a00:1450:4001:c01::67

...
;; Query time: 41 msec
;; SERVER: 2001:638:806:9::3#53(2001:638:806:9::3)
```

## 15.7. RADVD

Folgender Abschnitt zeigt eine beispielhafte Konfiguration des radvd (Router Advertisment Daemon), in der die wesentlichen Optionen hervorgehoben und erklärt sind:

```
root@ipv6-int-router-oev:~# vim /etc/radvd.conf
interface eth1
{
        AdvSendAdvert on;      #activates the RAs on the interface

        AdvManagedFlag on;     #Flag to receive IP address through dhcpv6
        AdvOtherConfigFlag on; #Flag to receive e.g. DNS through dhcpv6

        MinRtrAdvInterval 5;
        MaxRtrAdvInterval 15;

# example of RA
#
        prefix 2001:638:806:f201::/64
        {
                AdvOnLink on;
                AdvAutonomous off;      #Autonomous address-configuration
                AdvRouterAddr off;
        };
};
```

## 15.8. DHCPv6-Server und -Klient

Konfigurationsbeispiel für einen stateful DHCPv6-Server (wide-dhcpv6-server):

```
root@ipv6-int-router-oev:~# vim /etc/wide-dhcpv6/dhcp6s.conf

option domain-name-servers 2001:638:806:f211::3;
option domain-name "ipv6.oev";

interface eth1 {
        address-pool pool1 3600;
};

pool pool1 {
        range 2001:638:806:f201::1000 to 2001:638:806:f201::2000 ;
};
```

Konfigurationsbeispiel für einen DHCPv6-Klienten (wide-dhcpv6-client): Mit den folgenden Einstellungen erhält der Klient eine IPv6-Adresse aus dem o. g. Adresspool, sowie den Domainnamen und die IPv6-Adresse des DNS-Servers.

```
administrator@ClientUU:~$ vim /etc/wide-dhcpv6/dhcp6c.conf
# default gw has to be set through router advertisements.
interface eth0
{
  send ia-na 0;

  request domain-name-servers;
  request domain-name;

  script "/etc/wide-dhcpv6/dhcp6c-script";
};
```

```
id-assoc na 0 {
};
```

## 15.9. IPv6-Konfigurationen für DNS, Apache, MySQL

Konfigurationsdateien können in Abhängigkeit vom verwendeten Betriebssystem im Pfad und Namen abweichen.

**DNS Bind9**

Konfigurationsdatei: /etc/bind/named.conf.options

```
options {
        # sure other options here, too
        listen-on-v6 { any; };
};
```

**Apache Webserver**
Konfigurationsdatei: /etc/apache2/ports.conf

```
NameVirtualHost *:80
Listen *:80
```

**MySQL**

Konfigurationsdatei: /etc/mysql/my.cnf

```
[mysqld]
bind-address = ::
```

## 15.10. Erreichbarkeit von Diensten

Mit folgendem Befehl kann man sehen, ob ein Dienst Verbindungen über IPv4 und IPv6 ermöglicht:

```
root@ipv6-dnsserver-oev:~# netstat -tulpen
udp 0 0 :::53        :::*      1234/named  // Lauscht auf IPv4 und v6
Adresse
```

## 15.11. Deaktivieren der Tunneladapter bei Windows 7

Die benötigten Kommandos für Microsoft Windows 7 sind:

```
       netsh interface ipv6 6to4 set state disabled default
       netsh interface ipv6 isatap set state disabled
       netsh interface ipv6 set teredo disabled
```

# 16. Anhang IV: Fallstricke

Dieses Kapitel zeigt mögliche „Fallstricke“, die im Zusammenhang mit der Migration zu IPv6 bzw. zum Dual-Stack-Betrieb auftreten können. Fallstricke sind Eigenschaften von Hard- oder Software oder Ereignisse, welche während der Migration ans Licht kommen können. Trotz sorgfältiger Planung sind sie oft nicht vorhersehbar und können die Funktionsfähigkeit der Komponenten oder des Netzes beeinträchtigen.

Netzwerk:

- Es existieren DNS-Implementationen und Betriebskonzepte, die mit einem AAAA-Record nur dann antworten, wenn die Anfrage von einer IPv6-Adresse kommt. Dies kann problematisch sein, weil Klienten auch über IPv4 nach einem AAAA-Record fragen können, diesen aber nicht erhalten würden.
- Klienten können DNS-Einstellungen über verschiedene Mechanismen (Router Announcements, DHCPv6) erhalten. Um Konflikte zu vermeiden, sollte in jedem IP-Subnetz immer nur ein Mechanismus hierfür verwendet werden. Ferner werden RAs für DNS (RDNSS) derzeit noch nicht von allen Betriebssystemen unterstützt.

Verbindungen:

- Automatische IPv6-Funktionalitäten (z. B. Teredo-Tunnel) könnten bereits vorkonfiguriert sein und ein Sicherheitsrisiko darstellen. Diese müssen aktiv blockiert werden (an der Firewall) bzw. auf dem Host deaktiviert werden.
- Sobald ein Klient eine routbare IPv6-Adresse bekommen hat, wird er versuchen über diese IPv6-Verbindungen aufzubauen. Diese Adressen sollten daher erst vergeben werden, wenn IPv6-fähige Dienste auch per IPv6 aus dem IP-Subnetz der Klienten erreichbar sind (siehe Abschnitt 14.1 zur Migrationsreihenfolge). Ansonsten kann es zu Timeouts für den Rückgriff auf eine IPv4-Verbindung kommen.
- Es ist nicht vorhersehbar, über welche IP-Version ein Dual-Stack-Host Verbindungen aufbaut. Daher müssen Verbindungen und Sicherheitsregeln explizit für beide Protokolle verifiziert werden. Zum Beispiel verwenden einige Webbrowser bei Verwendung eines HTTP-Proxies vorzugsweise IPv4 bis zum Proxy, auch wenn der gewünschte Dienst per IPv6 erreichbar ist.
- Dual-Stack-Router: IPv6-Forwarding und IPv6-Routen müssen unabhängig von den IPv4-Funktionen auf einem Router aktiviert oder deaktiviert werden.
- Falls durch Blockierung von ICMPv6 auf einem IPv6-Ende-zu-Ende-Pfad zu viele oder alle ICMPv6-Nachrichten verworfen werden, so funktioniert die IPv6-Path-MTU-Erkennung nicht. Dies hat zur Folge, dass es zu

massiven Paketverlusten kommt, nämlich immer dann, wenn ein (nicht fragmentierbares) IPv6-Paket mit einer Größe gesendet wird, die nicht den kompletten Pfad passieren kann. Die Einhaltung der empfohlenen Filterregeln für ICMPv6 aus [RFC4890] ist daher auf allen Paketfiltern/Firewalls auf dem genutzten Pfad sicher zu stellen.

- Die erlaubte Größe von Layer-2-Datenpaketen ist in einigen Anwendungsszenarien (z. B. MPLS) möglicherweise zu gering. Bei jeder verwendeten Layer-2-Technologie muss daher zur Nutzung von IPv6 gesichert sein, dass IPv6-Pakete der garantierten Mindestgröße von 1280 Bytes transportiert werden können. Bei LAN-Technologien wie z. B. Ethernet ist dies gewährleistet (1500 Bytes sind möglich). Bei WAN-Technologien – wie z. B. MPLS – muss (in Zusammenarbeit mit dem MPLS-Anbieter) gewährleistet werden, dass Datenpakete von 1280 Bytes zzgl. eventuell vorhandener Header für darüber genutzte Tunneltechniken (z. B. IP-in-IP-Tunnel, IPsec) von der darunter liegenden Technologie transportiert werden können.

- Weitere Hinweise zu potentiellen Verbindungsproblemen im Dual-Stack-Betrieb sind zum Beispiel zu finden in [Meyer11].

Host:

- Klienten können leicht „unerwartet“ bereits IPv6-Konnektivität nutzen, wenn in einem LAN IPv6 Router Advertisements (RA) versendet werden (geplant oder auch ungeplant) und Klienten sich über IPv6-Autokonfiguration eine IPv6-Adresse erstellen. Eine explizite Deaktivierung von IPv6 auf Klienten, die dies noch nicht nutzen sollen, ist daher sinnvoll.

- Grafischen Bedienoberflächen zur Netzwerkkonfiguration arbeiten nicht immer fehlerfrei mit Systemfunktionen zur Konfiguration des IPv6-Netzwerkes zusammen (z. B. Ubuntu Desktop 10.04 Network Manager (GUI) schaltet bei Einstellung von IPv6 auf „automatisch“ die lokale Schnittstelle ab).

- Bei der IP-Adressvergabe können Funktionen und Einstellungen fest vorkonfiguriert sein. Zum Beispiel sind IPv6-Privacy-Extensions bei einigen Betriebssystemen in der Grundeinstellung aktiv und bei anderen deaktiviert.

- Beim Duplizieren von Hosts (klonen) kann es vorkommen, dass die so erstellten Systeme einen identischen DHCP unique identifier (DUID) erhalten. Da dieser als ID bei der Adresskonfiguration mittels DHCPv6 verwendet wird, kommt es zu Adresskonflikten, wenn die DUID nicht eindeutig im Netz ist.

Anwendung:

- Für die Umstellung eines Dienstes auf IPv6 ist zu prüfen, ob die eingesetzte Version (einer Software) IPv6 tatsächlich unterstützt. Bei

einigen (UNIX-)Software-Paketen kann es vorkommen, dass der aktuelle Source Code einer Server-Anwendung zwar prinzipiell IPv6 unterstützt, das für eine bestimmt UNIX/Linux-Distribution verfügbare Anwendungs-Paket aber ohne IPv6-Unterstützung übersetzt wurde. Falls es sich dabei um eine Open Source Software handelt, kann IPv6-Support ggf. durch Kompilieren einer eigenen Version dieser Software aktiviert werden. Allerdings entfällt bei einer selbst übersetzten Anwendung die Möglichkeit, Sicherheits-Updates automatisch über die Paketverwaltung einzuspielen – daher muss dieser Schritt wohl überlegt werden.

- Nach [RFC5952] ist es vorgeschrieben, *eine alphanumerische* IPv6-Adresse als Teil einer URI / URL in „[ ]“ einzuschließen, wie zum Beispiel in http://[::1] oder https://[::1]:80/index.html. Für alphanumerische IPv6-Adressen, die nicht Teil einer URI sind (z. B. ::1) sind die „[ ]“ laut o. g. RFC nicht verpflichtend. Wird unter Windows jedoch ein http/https-Proxy *mit einer alphanumerischen IPv6-Adresse* konfiguriert, so *muss* diese IPv6-Adresse in eckige Klammern ( „[ ]“ ) eingeschlossen werden. Schreibt man die IPv6-Adresse in der Proxy-Konfiguration nicht in eckige Klammern, so wird die Einstellung nicht übernommen.

- Bei Implementierungen für IP-Adress-Parser, Eingabefeldern oder Datenbankeinträgen für IP-Adressen ist nicht immer garantiert, dass diese auch für IPv6 geeignet sind; u. U. existiert keine Unterstützung für mehrere IP-Adressen (unterschiedlicher Protokollversion) für ein Interface in einer Anwendung. Die Lauffähigkeit wichtiger Anwendungen mit IPv6-Adressen muss daher explizit getestet werden.

- Bei der Konfiguration eines Servers (z. B. Webserver) muss darauf geachtet werden, dass die Annahme von Verbindungen sowohl über IPv4 als auch über IPv6 aktiviert wird. Eine Direktive wie „listen *“ oder „listen localhost“ führt nicht immer dazu, dass sowohl IPv4- als auch IPv6-Verbindungen akzeptiert werden. Ferner müssen mögliche Regeln, welche beschreiben, aus welchen Netzen eingehende Verbindungen akzeptiert werden, auch für IPv6 korrekt konfiguriert werden.

- Je nach Server-Anwendung bzw. Dienst muss in der Konfiguration nicht nur eine „Listen“-Direktive hinzugefügt werden, sondern weitere Parameter gesetzt werden (z. B. „IPv6_enable=yes“). Dies hängt von der jeweiligen Anwendung ab und sollte aus deren Betriebsanleitung/Manual in Erfahrung gebracht werden.

- In vielen Anwendungen sind IP-Adressen direkt („hart“) konfiguriert, z. B. in Webanwendungen, in Webservices, auf einigen Webseiten. Wo immer möglich, sollten statt dessen Hostnamen verwendet werden, die dann bei der Anwendung per DNS aufgelöst werden.

- Vorhandene Zertifikate sind ggf. neu oder zusätzlich zu erstellen, falls diese bisher (z. B. für die Authentisierung von Tunnelendpunkten) auf IP-Adressen ausgestellt sind

- IPv6 ist schon lange standardisiert, IPv6-Basisdienste werden aber immer noch erweitert. Implementierungen sind daher oft nicht ausreichend implementiert bzw. enthalten nicht alle bereits standardisierten Funktionen. Daher muss Hardware und Software mit Updates aktuell gehalten werden. Diese Updates bedürfen jedoch auch einer fortlaufenden Prüfung, da neue Fehler enthalten sein können.

- Es kann vorkommen, dass eine Software offiziell ab Version x.y IPv6 unterstützt, ein vorkompiliertes Paket dieser Software aber dennoch im Einzelfall ohne IPv6-Unterstützung übersetzt wurde (dies ist scheinbar bei Squid 3.1 unter Ubuntu 10.04 der Fall). In solch einem Fall sollte überlegt werden, ob ein Upgrade der verwendeten Distribution möglich ist, so dass verwendete Pakete bereits in einer IPv6-tauglichen Version als Pakete vom Distributor vorliegen.

- Ein DHCPv6-Klient benötigt ggf. eine komplexere Konfiguration, als dies für einen DHCPv4-Klienten der Fall ist. Mit den Default-Einstellungen des wide-dhcpv6-Klienten unter Linux werden zum Beispiel nur der Domainname und der DNS-Server abgefragt. Daher muss die Konfiguration dieses Klienten angepasst werden, um zusätzlich auch eine IPv6-Adresse zu erhalten.

- Kommt es nach der Einführung von IPv6 zu Problemen mit dem E-Mail-Empfang in einer Organisation, so *kann* dies auch ein DNS-Problem aufzeigen. E-Mail-Server (Mail Transfer Agents, MTA) müssen – genau wie bei IPv4 auch – Reverse DNS Lookups korrekt auflösen können (z. B. für PTR[26]-Checks durch die MTAs). Es muss sichergestellt sein, dass diese Anfragen sowohl für (DNS-)Domänen mit IPv4-Adressen, als auch solche die (auch) auf IPv6-Adressen aufgelöst werden, korrekt beantwortet werden. Siehe auch [Tanger11].

- Der Betrieb eines Split-DNS zum Verstecken interner Systeme ist auch unter IPv6 möglich, jedoch ist hier die Konfiguration und der Aufbau komplexer als bei IPv4. Siehe ebenfalls in [Tanger11], am Ende des Artikels für einige Hinweise.

IPv6-only:

- Erfahrungen aus einem IPv6-only-Betrieb sind detailliert in [RFC6586] beschrieben. Dieser Einsatzfall deckt besonders schnell Schwächen in einer Implementierung auf, da kein Rückgriff auf IPv4 möglich ist. Ein Test von vorhandenen Anwendungen unter IPv6-only-Laborbedingungen bietet sich an, denn Programme, die IPv4-only und IPv6-only funktionieren sind später im praktischen Einsatz auch Dual-Stack-tauglich (und zudem zukunftstauglich).

[26] PTR = Pointer Resource Record

# 17. Anhang V: Weiterführende Informationen zu IPv6

Zu IPv6 sind eine Reihe von Informationen in Buchform oder online verfügbar. Die folgende Liste soll einen ersten Überblick geben und stellt eine subjektive Auswahl an Material vor.

Bei der Online-Suche sollte auf die Aktualität der Information geachtet werden. IPv6 wurde über einen langen Zeitraum in Präsentationen vorgestellt und in Forschungsprojekten eingesetzt, so dass z. T. in IPv6-Dokumenten im Internet veraltete Referenzen oder veraltete Informationen zu finden sind.

Beim Nachschlagen von RFC (Request for Comments) Dokumenten sollte auf die IETF-Tools-Webseite[27] zurück gegriffen werden, da dort immer Verweise auf eine aktuellste Version jedes RFC-Dokuments vorhanden sind, falls dieses verbessert wurde („Errata", „Updated by …") oder durch eine neuere Version ersetzt wurde („Obsoleted by …").

| | |
|---|---|
| | Wilhelm Boeddinghaus, Christoph Meinel, Harald Sack:<br>Einführung von IPv6 in Unternehmensnetzen – ein Leitfaden<br>Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam, Nr. 52, ISBN 978-3-86956-156-1, 2011,<br>http://www.ipv6council.de/fileadmin/documents/HPI_52_ipv6_leitfaden.pdf<br><br>*Der Leitfaden stammt aus dem Umfeld des Deutschen IPv6 Rat und ist insbesondere für Entscheider gedacht, die hier eine leicht verständliche Einführung in die Thematik der Migration zu IPv6 finden. Eingegangen wird auf die Motivation zum Umstieg auf IPv6 und einige technische Details, insbesondere zu IPv6-Adressen. Der Schwerpunkt liegt auf dem Einstieg in den Prozess der Migration für kleinere und mittlere Unternehmen.* |
| | |
| | Silvia Hagen: IPv6. Grundlagen - Funktionalität – Integration<br>Verlag Sunny Edition, 2. Auflage Oktober 2009, ISBN-13 978-3952294222<br><br>*Ein gut verständliches Standardwerk in Deutsch, das übersichtlich die IPv6-Funktionen anhand der Netzwerkschichten und Protokolle erläutert. Anhand der Protokolle werden dann die grundlegenden IPv6-Konzepte erläutert. Das umfangreiche Buch ist übersichtlich aufgebaut und gestaltet und ermöglicht sowohl einen leichten Zugang zu IPv6-Funltionen als auch ein einfaches Nachschlagen von benötigten Informationen. Auch die Integration von IPv6 in bestehende Netze wird besprochen.*<br><br>Außerdem: Silvia Hagen: Planning for IPv6<br>Silvia Hagen: IPv6 Essentials |
| | |

[27] http://tools.ietf.org/rfc/ oder nach dem Muster http://tools.ietf.org/html/rfc2460

| | |
|---|---|
| | Benedikt Stockebrand: IPv6 in Practice<br>Springer, ISBN 978-3-540-24524-7<br><br>*Dieses Buch in Englisch orientiert sich an dem praktischen Betrieb von IPv6 unter verschiedenen Unix-Betriebssystemen. Im Vordergrund steht dabei ein betriebsorientiertes Konzept, dabei sind auch Übersichten und Erläuterungen oft an Kommandozeilen bzw. Konfigurationsdateien orientiert. Generelle Konzepte und Hintergründe werden an passender Stelle im Text eingestreut.* |
| | |
| | Lawrence E. Huges: The Second Internet<br>Online Ausgabe Oktober 2010, ISBN-13: 978-0-9828463-0-8<br>Das Buch ist vollständig verfügbar unter<br>http://www.secondinternet.org/<br><br>*Diese online verfügbare Buch stellt ist eine aktuelle Informationsquelle zu IPv6 und die Kernprotokolle des Internets. Es werden auch Migrationsmechnismen vorgestellt, sowie in einem weiteren Schwerpunkt Kryptografie und PKI. Abgeschlossen wird das Buch mit einer Reihe von IPv6-Projekten, bei denen es um das Aufsetzen Anwendungen und Diensten mittels Dual Stack geht.* |
| | |
| | Martin Dunmore (Hrsg.): 6NET: An IPv6 Deployment Guide.<br>Online verfügbar unter http://www.6net.org/book/deployment-guide.pdf<br><br>*Ein IPv6-Buch aus dem EU-Projekt 6NET. Gutes und praxisnahes Werk mit sehr vielen konkreten Beispielen, teilweise nicht mehr aktuell.* |
| | |
| | Tutorial des Projekts 6DEPOLY (IPv6 Deployment and Support)<br>http://www.6deploy.eu/index.php?page=tutorials<br><br>*Verschiedene Tutorials in Form von Foliensätzen zu Funktionen und Eigenschaften von IPv6, von wechselnder Qualität. Zusätzlich ist ein E-Learning-Modul für den ersten Einstieg verfügbar.* |
| | |
| [RFC6434] | RFC 6434 – IPv6 Node Requirements<br>Dezember 2011, http://tools.ietf.org/html/rfc6434<br><br>*Ein guter und leicht lesbarer Einstieg in die Standards und weitere RFCs der IETF rund um IPv6. Das Ziel des Dokuments ist eine Zusammenfassung der Anforderungen an ein IPv6-fähiges Endsystem oder einen Router, damit die Interoperabilität der Systeme gewährleistet ist. Dazu werden in den funktionalen Gruppen bzw. zu IP, Sub-IP und Anwendungsschicht die relevanten RFCs genannt und ggf. weiter analysiert, insbesondere in Hinblick auf Anforderungsgrade.* |
| | |

| | |
|---|---|
| | BSI-Standard zur Internet-Sicherheit (ISi-Reihe)<br>https://www.bsi.bund.de/ISi-Reihe/<br><br>*Das Bundesamt für Sicherheit in der Informationstechnik stellt mit der ISi-Reihe Informationen zur Verfügung, mit denen Behörden und Unternehmen ihre Internet-Aktivitäten möglichst eigenständig neu aufbauen, erweitern oder umbauen können. Das modulare Konzept bietet Informationen für Fach- und Führungskräfte. Im Rahmen der IPv6-Migration relevante Sicherheitsaspekte werden vor allen in den Dokumenten der ISi-Reihe zur sicheren Anbindung von lokalen Netzen an das Internet (ISi-LANA) behandelt, Informationen speziell zu IPv6 sind auch verfügbar (ISi-L-IPv6).* |
| | |
| | http://de.wikipedia.org/wiki/IPv6<br><br>*Der schnelle Überblick und Einstieg. Zu weiterführenden Information zu einzelnen IPv6-spezifschen Funktionen und Protokollen sind teilweise die englischen Seiten hilfreich und sollten nicht außer Acht gelassen werden.* |
| | |
| | http://ipv6.com/index.htm<br><br>*Einführung und Übersicht zu allen Themen und Techniken rund um IPv6.* |
| | |
| | http://ipv6.net/<br><br>*Ein Sammelsurium an Folien, Büchern, Terminen, …* |

*Tabelle 12: Weiterführende Informationen und Bücher zu IPv6*

## 18. Quellenverzeichnis


| | |
|---|---|
| [6PE_6VPE] | "IPv6 over MPLS ; 6PE and 6VPE", http://lacnic.net/documentos/seminarios/6PE_6VPE_LACNIC.pdf |
| [BUT-DEPLOY] | Deploying IPv6 in University Campus Network - Practical Problems, https://2011.jres.org/archives/141/paper141_article.pdf |
| [Donn11] | Lutz Donnerhacke: „Kommentar: IPv6 und der Datenschutz", Online-Artikel auf Heise Netze, 10. November 2011, http://heise.de/-1375692 |
| [ICDPPC11] | „Die Verwendung eindeutiger Kennungen bei der Nutzung von Internet Protokoll Version 6 (IPv6)", Entschließung der 33. Internationale Konferenz der Beauftragten für den Datenschutz und für die Privatsphäre, 1. Nov 2011, Mexiko Stadt |
| [IPv6_PROFILE] | siehe unter http://www.ipv6.bva.bund.de |
| [IPv6_PROFILE-DOK] | siehe unter http://www.ipv6.bva.bund.de |
| [IPV6_REF] | IPv6 Referenzhandbuch, Version 1.0 |
| [ISi-L-IPv6] | „Leitfaden für eine sichere IPv6-Netzwerkarchitektur (ISi-L-IPv6)", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_leitfaden_IPv6_pdf |
| [ISi-LANA] | „Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA)", https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_lana_studie_pdf |
| [Kaps12] | Reiko Kaps: „Tarnkappen-Router für IPv6", c't, Heft 3 / 2012, http://www.heise.de/ct/inhalt/2012/03/160/ |
| [Meyer11] | "IPv6 und das Dual-Stack-Problem", Frank Meyer, iX Magazin 07/2011, Seite 48 ff., http://www.heise.de/ix/inhalt/2011/07/48/ |
| [MIG_GUIDE] | „Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks, Marc Blanchet, John Wiley & Sons, December 2005. also on Google books: http://books.google.de/books?id=9_Qn3LSD2t8C |
| [NIST-800-119] | National Institute of Standards and Technology – Special Publication 800-119 – "Guidelines for the Secure Deployment of IPv6", Sheila Frankel, Richard Graveman, John Pearce, Mark Rooks, December 2010 |
| [RFC1661] | The Point-to-Point Protocol (PPP), W. Simpson, July 1994, http://www.rfc-editor.org/rfc/rfc1661.txt |
| [RFC2080] | RIPng for IPv6 G. Malkin, R. Minnear, January 1997, http://www.rfc-editor.org/rfc/rfc2080.txt |

| | |
|---|---|
| [RFC2460] | Internet Protocol, Version 6 (IPv6) Specification, S. Deering, R. Hinden, December 1998, http://www.rfc-editor.org/rfc/rfc2460.txt |
| [RFC2463] | Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, A. Conta, S. Deering, December 1998, http://www.rfc-editor.org/rfc/rfc2463.txt |
| [RFC2637] | Point-to-Point Tunneling Protocol (PPTP), K. Hamzeh, G. Pall, W. Verthein, J. Taarud, W. Little, G. Zorn, July 1999, http://www.rfc-editor.org/rfc/rfc2637.txt |
| [RFC2784] | Generic Routing Encapsulation (GRE), D. Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, March 2000, http://www.rfc-editor.org/rfc/rfc2784.txt |
| [RFC2845] | Secret Key Transaction Authentication for DNS (TSIG), P. Vixie, O. Gudmundsson, D. Eastlake 3rd, B. Wellington, May 2000, http://www.rfc-editor.org/rfc/rfc2845.txt |
| [RFC3056] | Connection of IPv6 Domains via IPv4 Clouds, B. Carpenter, K. Moore, February 2001, http://www.rfc-editor.org/rfc/rfc3056.txt |
| [RFC3068] | An Anycast Prefix for 6to4 Relay Routers, C. Huitema, June 2001, http://www.rfc-editor.org/rfc/rfc3068.txt |
| [RFC3176] | InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks, P. Phaal, S. Panchen, N. McKee, September 2001, http://www.rfc-editor.org/rfc/rfc3176.txt |
| [RFC3582] | Goals for IPv6 Site-Multihoming Architectures, J. Abley, B. Black, V. Gill, August 2003, http://www.rfc-editor.org/rfc/rfc3582.txt |
| [RFC3633] | IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6, O. Troan, R. Droms, December 2003, http://www.rfc-editor.org/rfc/rfc3633.txt |
| [RFC3720] | Internet Small Computer Systems Interface (iSCSI), J. Satran, K. Meth, C. Sapuntzakis, M. Chadalapaka, E. Zeidner, April 2004 http://www.rfc-editor.org/rfc/rfc3720.txt |
| [RFC3756] | IPv6 Neighbor Discovery (ND) Trust Models and Threats, P. Nikander, J. Kempf, E. Nordmark, May 2004, http://www.rfc-editor.org/rfc/rfc3756.txt |
| [RFC3776] | Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, J. Arkko, V. Devarapalli, F. Dupont, June 2004, http://www.rfc-editor.org/rfc/rfc3776.txt |
| [RFC3954] | Cisco Systems NetFlow Services Export Version 9, B. Claise, Ed., October 2004, http://www.rfc-editor.org/rfc/rfc3954.txt |

| | |
|---|---|
| [RFC3964] | Security Considerations for 6to4, P. Savola, C. Patel, December 2004, http://www.rfc-editor.org/rfc/rfc3964.txt |
| [RFC4007] | IPv6 Scoped Address Architecture, S. Deering, B. Haberman, T. Jinmei, E. Nordmark, B. Zill, March 2005, http://www.rfc-editor.org/rfc/rfc4007.txt |
| [RFC4033] | DNS Security Introduction and Requirements, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005, http://www.rfc-editor.org/rfc/rfc4033.txt |
| [RFC4034] | Resource Records for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005, http://www.rfc-editor.org/rfc/rfc4034.txt |
| [RFC4035] | Protocol Modifications for the DNS Security Extensions, R. Arends, R. Austein, M. Larson, D. Massey, S. Rose, March 2005, http://www.rfc-editor.org/rfc/rfc4035.txt |
| [RFC4192] | Procedures for Renumbering an IPv6 Network without a Flag Day, F. Baker, E. Lear, R. Droms, September 2005, http://www.rfc-editor.org/rfc/rfc4192.txt |
| [RFC4193] | Unique Local IPv6 Unicast Addresses, R. Hinden, B. Haberman, October 2005, http://www.rfc-editor.org/rfc/rfc4193.txt |
| [RFC4213] | Basic Transition Mechanisms for IPv6 Hosts and Routers, E. Nordmark, R. Gilligan, October 2005, http://www.rfc-editor.org/rfc/rfc4213.txt |
| [RFC4214] | Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), F. Templin, T. Gleeson, M. Talwar, D. Thaler, October 2005, http://www.rfc-editor.org/rfc/rfc4214.txt |
| [RFC4225] | Mobile IP Version 6 Route Optimization Security Design Background, P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark, December 2005, http://www.rfc-editor.org/rfc/rfc4225.txt |
| [RFC4285] | Authentication Protocol for Mobile IPv6, A. Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury, January 2006, http://www.rfc-editor.org/rfc/rfc4285.txt |
| [RFC4291] | IP Version 6 Addressing Architecture, R. Hinden, S. Deering, February 2006, http://www.rfc-editor.org/rfc/rfc4291.txt |
| [RFC4301] | Security Architecture for the Internet Protocol, S. Kent, K. Seo, December 2005, http://www.rfc-editor.org/rfc/rfc4301.txt |

| | |
|---|---|
| [RFC4449] | Securing Mobile IPv6 Route Optimization Using a Static Shared Key, C. Perkins, June 2006, http://www.rfc-editor.org/rfc/rfc4449.txt |
| [RFC4487] | Mobile IPv6 and Firewalls: Problem Statement, F. Le, S. Faccin, B. Patil, H. Tschofenig, May 2006, http://www.rfc-editor.org/rfc/rfc4487.txt |
| [RFC4554] | Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks, T. Chown, June 2006, http://www.rfc-editor.org/rfc/rfc4554.txt |
| [RFC4659] | BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN, J. De Clercq, D. Ooms, M. Carugi, F. Le Faucheur, September 2006, http://www.rfc-editor.org/rfc/rfc4659.txt |
| [RFC4798] | Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE), J. De Clercq, D. Ooms, S. Prevost, F. Le Faucheur, February 2007,http://www.rfc-editor.org/rfc/rfc4798.txt |
| [RFC4852] | IPv6 Enterprise Network Analysis - IP Layer 3 Focus, J. Bound, Y. Pouffary, S. Klynsma, T. Chown, D. Green, April 2007, http://www.rfc-editor.org/rfc/rfc4852.txt |
| [RFC4861] | Neighbor Discovery for IP version 6 (IPv6), T. Narten, E. Nordmark, W. Simpson, H. Soliman, September 2007, http://www.rfc-editor.org/rfc/rfc4861.txt |
| [RFC4864] | Local Network Protection for IPv6, G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, May 2007, http://www.rfc-editor.org/rfc/rfc4864.txt |
| [RFC4877] | Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture, V. Devarapalli, F. Dupont, April 2007, http://www.rfc-editor.org/rfc/rfc4877.txt |
| [RFC4882] | IP Address Location Privacy and Mobile IPv6: Problem Statement, R. Koodli, May 2007, http://www.rfc-editor.org/rfc/rfc4882.txt |
| [RFC4942] | IPv6 Transition/Co-existence Security Considerations, E. Davies, S. Krishnan, P. Savola, September 2007, http://www.rfc-editor.org/rfc/rfc4942.txt |
| [RFC5095] | Deprecation of Type 0 Routing Headers in IPv6, J. Abley, P. Savola, G. Neville-Neil, December 2007, http://www.rfc-editor.org/rfc/rfc5095.txt |
| [RFC5101] | Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information, B. Claise, Ed., January 2008, http://www.rfc-editor.org/rfc/rfc5101.txt |

| | |
|---|---|
| [RFC5158] | 6to4 Reverse DNS Delegation Specification, G. Huston, March 2008, http://www.rfc-editor.org/rfc/rfc5158.txt |
| [RFC5175] | IPv6 Router Advertisement Flags Option, B. Haberman, R. Hinden, March 2008, http://www.rfc-editor.org/rfc/rfc5175.txt |
| [RFC5214] | Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), F. Templin, T. Gleeson, D. Thaler, March 2008, http://www.rfc-editor.org/rfc/rfc5214.txt |
| [RFC5389] | Session Traversal Utilities for NAT (STUN), J. Rosenberg, R. Mahy, P. Matthews, D. Wing, October 2008, http://www.rfc-editor.org/rfc/rfc5389.txt |
| [RFC5445] | Basic Forward Error Correction (FEC) Schemes, M. Watson, March 2009, http://www.rfc-editor.org/rfc/rfc5445.txt |
| [RFC5579] | Transmission of IPv4 Packets over Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), Interfaces F. Templin, February 2010, http://www.rfc-editor.org/rfc/rfc5579.txt |
| [RFC5637] | Authentication, Authorization, and Accounting (AAA) Goals for Mobile IPv6, G. Giaretta, I. Guardini, E. Demaria, J. Bournelle, R. Lopez, September 2009, http://www.rfc-editor.org/rfc/rfc5637.txt |
| [RFC5726] | Mobile IPv6 Location Privacy Solutions, Y. Qiu, F. Zhao, R. Koodli, February 2010, http://www.rfc-editor.org/rfc/rfc5726.txt |
| [RFC5845] | Generic Routing Encapsulation (GRE) Key Option for Proxy Mobile IPv6, A. Muhanna, M. Khalil, S. Gundavelli, K. Leung, June 2010, http://www.rfc-editor.org/rfc/rfc5845.txt |
| [RFC5944] | IP Mobility Support for IPv4, Revised, C. Perkins, November 2010, http://www.rfc-editor.org/rfc/rfc5944.txt |
| [RFC5952] | A Recommendation for IPv6 Address Text Representation, S. Kawamura, M. Kawashima, August 2010, http://www.rfc-editor.org/rfc/rfc5952.txt |
| [RFC5969] | IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification, W. Townsley, O. Troan, August 2010, http://www.rfc-editor.org/rfc/rfc5969.txt |
| [RFC6052] | IPv6 Addressing of IPv4/IPv6 Translators, C. Bao, C. Huitema, M. Bagnulo, M. Boucadair, X. Li, October 2010, http://www.rfc-editor.org/rfc/rfc6052.txt |

| | |
|---|---|
| [RFC6101] | The Secure Sockets Layer (SSL) Protocol Version 3.0, A. Freier, P. Karlton, P. Kocher, August 2011, http://www.rfc-editor.org/rfc/rfc6101.txt |
| [RFC6146] | Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, P. Matthews, I. van Beijnum, April 2011, http://www.rfc-editor.org/rfc/rfc6146.txt |
| [RFC6147] | DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers, M. Bagnulo, A. Sullivan, P. Matthews, I. van Beijnum, April 2011, http://www.rfc-editor.org/rfc/rfc6147.txt |
| [RFC6275] | Mobility Support in IPv6, C. Perkins, D. Johnson, J. Arkko, July 2011, http://www.rfc-editor.org/rfc/rfc6275.txt |
| [RFC6333] | Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion, A. Durand, R. Droms, J. Woodyatt, Y. Lee, August 2011, http://www.rfc-editor.org/rfc/rfc6333.txt |
| [RFC6586] | Experiences from an IPv6-Only Network, J. Arkko, A. Keranen, April 2012, http://www.rfc-editor.org/rfc/rfc6586.txt |
| [RIPE_ADDR] | Preparing an IPv6 Addressing Plan, March 2011, http://www.ripe.net/lir-services/training/material/IPv6-for-LIRs-Training-Course/IPv6_addr_plan4.pdf |
| [Tanger11] | “Herausforderungen für Sicherheitsverantwortliche”, Volker Tanger, iX Magazin, Ausgabe 7/2011, Seite 56 ff. |

## 19. 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.<br><br>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.<br><br>empfohlen / sollte: Die Nutzung der Funktion wird als sinnvoll angesehen. Abhängig von den Gegebenheiten und Anforderungen im Einzelfall kann hiervon auch |

| | |
|---|---|
| | abgewichen werden.<br><br>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) |
| 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<br>(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 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 Klienten 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 | Die technische Ende-zu-Ende-Kommunikation bezieht sich auf eine durchgängige, transparente Kommunikation oberhalb der Netzwerkschicht. Zur Nutzung eines Dienstes oder einer Anwendung wird der gesamte logische Kommunikationspfad zwischen Klient und Server betrachtet, was z. B. Sicherheitskomponenten auf dem Übertragungsweg einschließen kann. Aufgrund des großen Adressumfangs erlaubt IPv6 auch wieder eine Umsetzung der Ende-zu-Ende-Kommunikation ohne einen Eingriff in der Transportschicht. Dies kann in einigen Anwendungsfällen aufgrund von Sicherheitsanforderungen unerwünscht 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 Klienten 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 Routingprotokolle 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 signalisiert. |
| 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<br>(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<br>[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 aktiv Angriffe 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<br>(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 Rechneradressen 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. |
| Klient | Als Klient werden Software und Hardware bezeichnet, die bestimmte Dienste von einem entfernten Server in Anspruch nehmen können. Häufig steht der Begriff Klient für einen Arbeitsplatzrechner (siehe Klientensystem), der in einem Netz auf Daten und Programme eines Servers zugreift. |
| 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 Kommunikations-aspekte. 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 Übersetzungs-komponente 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 Netzinfrastrukturdienste werden in diesem Dokument zusammenfassend Dienste bezeichnet, die für den Betrieb des Netzes selber wichtig oder in der gewählten Konfiguration notwendig sind, normalerweise sind das 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.<br><br>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 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. Sie sind abhängig von ihrer Aufgabe Transitsysteme oder Endsysteme, bzw. auf Endsystemen installiert. |
| Sicherheits-Proxy | (siehe Applikation Level Gateway) |
| Signatur | Zeichenfolge, die über einen 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 (SOHO steht für Small Office, Home Office), 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. Es ist unidirektional, das heißt es 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 des Tunnel-Brokers ist beschrieben in [RFC3053]. |
| Tunneling | Tunneling bezeichnet in einem Netzwerk die Einbettung und Übertragung der PDUs eines Kommunikations-protokolls in einem (insbesondere einem 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 Computernetz-werke, welche nach Internet-Standards aufgebaut sind. Dabei werden Sprache und Steuerinformationen (z. B. für den Verbindungsaufbau) über ein auch für Daten-übertragung 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 | EEin 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 (Computer, Server, Dienst, Person, …), bestimmte, im diesem Zertifikat beschriebene Eigenschaften bestätigt und von einer autorisierten Zertifikats-Stelle ausgegeben und bestätigt worden ist. |

# 20. Abbildungsverzeichnis

## 21. Tabellenverzeichnis