

Bernburg  
Dessau  
Köthen



**Hochschule Anhalt**  
Anhalt University of Applied Sciences



Fachbereich  
Elektrotechnik, Maschinenbau  
und Wirtschaftsingenieurwesen

## Bachelorarbeit

zur Erlangung des akademischen Grades  
Bachelor of Engineering (B. Eng.)

**Robert Brocke**

---

Vorname Nachname

Elektrotechnik, 2008, 4049877

---

Studiengang, Matrikel, Matrikelnummer

Thema:

**Untersuchung der IPv6-Fähigkeit  
von VoIP-Lösungen für die  
kleingewerbliche Nutzung**

Prof. Dr. Eduard Siemens

---

1. Prüfer/in

Dr. Dmitry Kachan

---

2. Prüfer/in

07.02.2018

---

Abgabe am

---

## Selbständigkeitserklärung

Hiermit erkläre ich, dass die Arbeit selbständig verfasst, in gleicher oder ähnlicher Fassung noch nicht in einem anderen Studiengang als Prüfungsleistung vorgelegt wurde und keine anderen als die angegebenen Hilfsmittel und Quellen, einschließlich der angegebenen oder beschriebenen Software, verwendet wurden.

Köthen, 05.02.2018

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift/en der/des Studierenden

## Sperrvermerk

Sperrvermerk:

ja

nein

wenn ja:

Der Inhalt der Arbeit darf Dritten ohne Genehmigung der/des (Bezeichnung des Unternehmens) nicht zugänglich gemacht werden. Dieser Sperrvermerk gilt für die Dauer von X Jahren.

Köthen, 05.02.2018

\_\_\_\_\_  
Ort, Datum

\_\_\_\_\_  
Unterschrift/en der/des Studierenden

---

## Angaben zum Unternehmen

Logo des Unternehmens



Name des Unternehmens Cubeoffice GmbH & Co.KG

Abteilung Netzwerk Service / VoIP

Name des Betreuers Dipl.-Ing. Matthias Kunert

### Kontaktdaten

Anschrift des Standortes, an dem die Arbeit verfasst wurde cubeoffice GmbH & Co.KG  
Fichtestrasse 29a, 39112 Magdeburg

E-Mail-Adresse des Betreuers [mk@cubeoffice.de](mailto:mk@cubeoffice.de)

---

Für meine Familie  
Annika, Finn und Laurin

---

## Kurzfassung

Mit dem IP-Protokoll (egal ob IPv4 oder IPv6) können viele Dienste übertragen werden. Mit der Verfügbarkeit höherer Bandbreiten in der Fläche hat sich ein Dienst ganz besonders dazu angeboten, seine klassischen Leitungswege zu verlassen und künftig über neue Leitungswege unter Nutzung des IP-Protokolls zu kommunizieren – **die Telefonie**.

Seit Anfang des 21. Jahrhunderts begannen die Telefongesellschaften damit, die Kommunikation zwischen Vermittlungsstellen auf IP umzustellen. Parallel dazu fand diese **VoIP**-Technologie sehr viel Zuspruch in den Unternehmen, welche IP-basierte Telefonanlagen anschafften und damit innerhalb der Unternehmensnetzwerke zu einer Verbreitung von VoIP beitrugen. Seit ein paar Jahren werden nun auch die Endkundenanschlüsse für Telefonie immer häufiger als VoIP-Produkt ausgeführt. Es ist daher konsequent, dass alle Telefongesellschaften die Abschaffung klassischer Telefonnetze vorantreiben und somit eine IP-basierte Sprachkommunikation ohne Medienübergänge ermöglichen. Nicht zuletzt, weil aktuelle VoIP-Technologien mehr können, als ISDN-Netze oder analoge Anschlüsse.

Die vorliegende Arbeit untersucht heute verfügbare **VoIP-Lösungen** auf Ihre Zukunftsfähigkeit und auf Ihre Unterstützung für das Internet der nächsten Generation – das **IPv6-Internet**. Dabei sollen Lösungen im Fokus stehen, die vor Allem im kleingewerblichen Rahmen, dem Markt für **SOHO-Produkte**, eingesetzt werden.

Mittels eines Versuchsaufbaus werden Diensteanbieter für VoIP-Produkte, Internetanbieter, Router und verschiedene Clients auf ihre Funktionalität in IPv6-Szenarien getestet. Die Arbeit zeigt die Ergebnisse und gibt eine Einschätzung, in welchem Umfang eine Umstellung von Telefonielösungen auf IPv6 zum gegenwärtigen Zeitpunkt bereits sinnvoll ist.

---

# Inhaltsverzeichnis

<b>Abkürzungsverzeichnis.....</b>	<b>VIII</b>
<b>1 Motivation und Zielsetzung.....</b>	<b>1</b>
1.1 Einleitung .....	1
1.2 Zielsetzung der Arbeit .....	4
1.3 Struktur der Arbeit .....	5
<b>2 Stand von Wissenschaft und Technik.....</b>	<b>6</b>
2.1 Begriffsdefinitionen .....	6
2.1.1 SOHO-Netzwerke .....	6
2.1.2 Einteilung in Rollen/Bestandteile .....	7
2.1.3 IP-Telefonie (VoIP) .....	8
2.1.4 Konvergente Netze: NGN, All-IP, „Netz der Zukunft“ .....	9
2.1.5 Breitband-Internetanschlüsse .....	11
2.2 Internet Protokoll (IP) .....	13
2.2.1 IPv4 .....	13
2.2.2 IPv6 .....	13
2.2.3 Vorteile und Umstiegsgründe .....	15
2.2.4 DualStack-Verfahren .....	15
2.2.5 DS-Lite .....	17
2.3 SIP .....	18
2.3.1 TK-System im lokalen LAN, SIP-Trunking zum Carrier .....	19
2.3.2 TK-System beim Carrier .....	20
2.3.3 NGN-Anschlüsse: TK-Anlage beim Carrier, Proxy-Gateway im LAN.....	21
<b>3 Untersuchung im Versuchsnetz.....</b>	<b>23</b>
3.1 Aufbau des Versuchsnetzes .....	23
3.2 Diensteanbieter (ASP) .....	24
3.2.1 Webseiten.....	24
3.2.2 Internettelefonieanbieter (ITSP) .....	28
3.2.3 Das DNS-Problem bei den ITSP .....	30
3.2.4 Bewertung ASP .....	31
3.3 Internet Service Provider (ISP) .....	32
3.3.1 Prüfverfahren .....	32
3.3.2 Anbieter die DS-Lite verwenden.....	35
3.3.3 Anbieter die DualStack implementiert haben .....	36
3.3.4 feste/dynamische Präfixe .....	37
3.3.5 Bewertung ISP .....	38
3.4 Router .....	40
3.4.1 Prüfverfahren .....	41
3.4.2 Getestete Router.....	42
3.4.3 Ergebnisse Routertests.....	49
3.5 Clients.....	51
3.5.1 Prüfverfahren .....	52

---

3.5.2	Softwarebasierte Clients.....	53
3.5.3	Hardwarebasierte Clients.....	60
<b>4</b>	<b>Best Practice .....</b>	<b>68</b>
4.1	Beispielnetzwerk IPv6.....	68
4.2	Sicherheit .....	72
4.3	Selfhosted PBX – die eigene, cloudbasierte IP-PBX.....	74
4.3.1	vServer.....	74
4.3.2	IP-PBX-Software .....	75
4.3.3	Client-Einrichtung .....	78
4.3.4	SIP-Trunk.....	80
<b>5</b>	<b>Zusammenfassung und Ausblick .....</b>	<b>81</b>
	<b>Abbildungsverzeichnis.....</b>	<b>i</b>
	<b>Tabellenverzeichnis .....</b>	<b>iii</b>
	<b>Literaturverzeichnis .....</b>	<b>iv</b>
	<b>Anhang.....</b>	<b>ix</b>
	<b>Danksagung .....</b>	<b>x</b>

## Abkürzungsverzeichnis

ASP	<b>Application Service Provider</b> – Diensteanbieter – stellt Dritten nutzbare Dienste und Applikationen zur Verfügung, die diese mittels Internetanschlüssen nutzen können.
CGN	<b>Carrier Grade NAT</b> – siehe NAT, jedoch steht der NAT-Router nicht beim Endkunden, sondern beim Carrier und das priv. IP-Netz beginnt ebenfalls bereits im Netzbereich des Carriers. [RFC6264] Diese Technologie ist Schlüsseltechnologie für DS-Lite. IP-Adressen werden i.d.R. aus dem Bereich der [RFC6598] „Reserved IPv4 Prefix for Shared Address Space“ zugeteilt.
DNS	<b>Domain Name System</b>
DS-Lite	<b>DualStack-Lite</b> – IPv4/IPv6-Übergangstechnologie für Internetanschlüsse bei der beide Protokolle übertragen werden, jedoch nur eine priv. IPv4-Adresse in Verbindung mit CGN zugeteilt wird. Siehe <i>Abschnitt 2.2.5- DS-Lite</i>
DSP	<b>Digitaler Signal-Prozessor</b> – Hardwarelösungen für das Umrechnen digitalisierter Audiodaten in Echtzeit. In TK-Systemen und VoIP-Gateway-Systemen meist mehrfach vorhanden (entspr. ausgelegter Sprachkanäle)
EDV	<b>Elektronische Datenverarbeitung</b>
FTTx	<b>Fiber to the x</b> - Anschlusstechnologien auf Glasfaserbasis (passive optische Netze (PON)) werden im technischen Sprachgebrauch häufig als FTTx bezeichnet. Das „x“ kann je nach Ausbaustufe jeweils durch die allg. Abkürzung für den Abschlußpunkt der Glasfaser ersetzt werden (z.Bsp.: Home, Curb, Basement, Desk)
IETF	<b>Internet Engineering Task Force</b> – offene, internationale Organisation zur Standardisierung im Internet eingesetzter Kommunikationsprotokolle. Die IETF ist Herausgeber einer Großzahl der RFC (Request for Comment) die sich mit der Standardisierung des Datenverkehrs im Internet beschäftigen.
IP	<b>Internet Protocol</b> – Netzwerkprotokoll, stellt die Grundlage des Internets dar. Erste, vom Übertragungsmedium unabhängige Schicht im <i>OSI-Modell</i> .
IPv4	<b>Internet Protocol Version 4</b> – heute verbreitete Version des IP-Protokolls. Durch das DARPA-Program 1981 definiert [RFC791] hat es sich bis zum heutigen Tage weltweit durchgesetzt. Aufgrund der Verbreitung bestehen Probleme mit der Anzahl verfügbarer IPv4-Adressen (32bit Adressraum). Die Einführung privater (mehrfach nutzbarer) Adressbereiche schaffte Abhilfe, führte aber auch zu weiteren Beschränkungen (z.B. NAT).
IPv6	<b>Internet Protocol Version 6</b> – entwickelt ab 1995, erste Veröffentlichung in [RFC2460], Zusatzdefinitionen in weiteren RFC. Offiz. Nachfolger des IPv4, dessen Einschränkungen sollen durch die Einführung von IPv6 behoben werden. IPv6 bietet einen 128bit Adressraum, bei dem von einer Erschöpfung nicht mehr auszugehen

---

	ist und integriert bereits im Protokoll zusätzliche moderne Funktionen wie bspw. Autokonfiguration, Verschlüsselung, MobileIPv6.
ISDN	<b>Integrated Services Digital Network</b> – digit. Telekommunikationsnetz zur Übermittlung von Sprache, aber auch paketverm. Daten (Datex-P), leitungsverm. Daten (Datex-J), Fernschreiben (Telex). Hoher Verbreitungsgrad in der EU, insb. Deutschland. 1980 durch ITU-T (damals CCITT) definiert, besonders verbreitet ab 1989 im Standard DSS1 der ETSI (eur. Institut für Telekommunikationsnormen). Zuletzt stark rückläufige Nutzungszahlen, da nicht konkurrenzfähig gegenüber neuen Technologien (z.B. VoIP).
ISP	<b>Internet Service Provider</b> – Anbieter von Produkten für die Internetkonnektivität
IT	<b>Informationstechnologie</b>
ITU	<b>International Telecommunication Union</b> – Internationale Fernmeldeunion
ITU-T	<b>Telecommunication Standardization Sector der ITU</b> – Normierungs-Abteilung der Fernmeldeunion. Veröffentlicht Empfehlungen (Recommendation). Schematischer Aufbau des Empfehlungsindex siehe [ITU-Struktur]
KMU	<b>Kleine und mittlere Unternehmen</b> (engl.: SMB – small and medium sized businesses), Sammelbezeichnung für Unternehmen, die eine bestimmte Größe nicht überschreiten [EG03]. (z.B. <250 Mitarbeiter). Die KMU bilden in Deutschland rund 99,6% aller USt.-pflichtigen Unternehmen und beschäftigen 58,5% aller sozialversicherungspflichtig Beschäftigten. [IfM17] Zu den KMU zählen ebenfalls die <b>Kleinstunternehmen/Kleingewerbe</b> mit <9 Beschäftigten, welche in Deutschland mit etwa 3,25 Mio. Unternehmen und rund 89,1% aller Unternehmen die häufigste Unternehmensform darstellen <sup>1</sup> . Diese Kleinstunternehmen sind die Zielgruppe für den Verkauf von SOHO-Produkten.
NAT	<b>Network Address Translation</b> – Routingverfahren, bei dem mehrere nur privat erreichbare IP-Adressen sich eine einzelne öffentliche Adresse teilen. Der NAT-Router übernimmt das Umschreiben der Quell- & Zieladressen (Source-NAT, Masquerading). [RFC1631], [RFC2663]
NGN/All-IP	<b>Next Generation Network</b> – gemeinsam mit Kunstbegriff „All-IP“ eine Bezeichnung für Teilnehmeranschlüsse, bei denen die Medien Telefonie und Internet (DoublePlay) oder ggf. auch weitere Medien wie Fernsehen (TriplePlay) als IP-basierte Datenübertragung auf ein- und derselben Netzwerkinfrastruktur übertragen werden. Vorteil dieser Anschlüsse ist die Konvergenz. NGN-Anschlüsse lösen derzeit großflächig ISDN- sowie analoge Telefonanschlüsse ab.
OSI-Modell	auch: ISO/OSI-7-Schichten-Modell, <b>Open Systems Interconnection – Basic Reference Model</b>

---

<sup>1</sup> Siehe Statistisches Bundesamt: Sonderauswertung des Unternehmensregisters im Auftrag des IfM Bonn, Jahrgang 2017 [IfM17]

seit 1977 entwickeltes, 1983 von der ITU-T & 1984 von der ISO (International Organization for Standardization) als Standard veröffentlichtes Referenzmodell für Netzwerkprotokolle. Besonderheit ist die festgelegte Strukturierung in 7 festgelegte Schichten mit eng definierten Aufgaben. [ISO94]

POTS	<b>Plain Old Telephone Service</b> – nachträgliche Sammelbezeichnung für das klassische analoge Telefonnetz. Vgl. PSTN.
PSTN	<b>Public Switched Telephone Network</b> – Telefonnetz, Fachbegriff für das öffentliche Telefonievermittlungsnetz. Die Begriffsverwendung ist unabhängig von verwendeter Technologie (POTS, ISDN, NGN) oder Architektur. Endliche Verbindungen zum Austausch von Sprache.
RFC	<b>Request for Comment</b> – Bezeichnung für einen Großteil der technischen und organisatorischen Dokumente, die sich mit dem Internet (früher: Arpanet) beschäftigen. RFC's werden auch dann noch als solche bezeichnet, wenn sie sich längst zum <i>Standard</i> entwickelt haben.
SIP	<b>Session Initiation Protokoll</b> – Protokoll zum Aufbau und zur Steuerung audiovisueller Kommunikationsverbindungen auf IP-Basis. Siehe eigener Abschnitt 2.3- SIP
SOHO	<b>Small Office/Home Office</b> – Kleinbüro/Heimbüro, siehe eigener Abschnitt 2.1.1 - SOHO-Netzwerke typische Kundengröße im IT-Bereich, (vgl. KMU) beschreibt Netzwerke mit einzelnen bis einigen wenigen Benutzern.
VoIP	<b>Voice over IP</b> – Sprachübertragung unter Nutzung des Internetprotokolls

## 1 Motivation und Zielsetzung

### 1.1 Einleitung

Seit 2011 ist der durch IANA verwaltete, 32bit große Adressraum mit der Bezeichnung IPv4 vollständig an die regionalen Verwaltungsorganisationen vergeben<sup>2</sup>. Die rund 4 Mrd. möglichen Adressen, die nicht einmal ausreichen würden um jedem Erdenbürger eine eigene Adresse zuteilen zu können, sind allesamt an die verwaltenden Regional Internet Registries (RIR) verteilt.

In Europa merkt man von der entstandenen Adressknappheit noch relativ wenig, da Nordamerika und Europa – verglichen mit dem Rest der Welt – einen enorm hohen Anteil an IPv4-Adressen zugeteilt bekommen haben. Insgesamt 58% des gesamten IP-Adressraums entfallen auf die ARIN und die RIPE NCC, weitere 14% sind reservierte Bereiche wie z.Bsp. für lokale Netzwerke. Der gesamte Rest der Welt muss mit den übriggebliebenen 28% der IPv4-Adressen auskommen<sup>3</sup>. Dadurch ist die Knappheit bei uns weniger offensichtlich. Das heißt aber nicht, dass auch die nordamerikanischen sowie europäischen Adressbestände noch große Spielräume zulassen.

Die amerikanische RIR ARIN<sup>4</sup> vergibt seit 2015 keine IP-Adressen mehr, da ihre Adressräume erschöpft sind. Die europäische RIR RIPE NCC<sup>5</sup>, wie auch die anderen RIR-Organisationen können derzeit nur noch unter verschärften Vergabebedingungen kleine Adressmengen aus ihren letzten zugeteilten /8 -Adressbereichen vergeben. Ein /8 IPv4-Adressbereich entspricht etwa 16,7 Mio. IP-Adressen – dies entspricht dem Standard-Segment mit welchem die IANA Adressen an die zuständigen RIR's verteilt. Diese spalten die Segmente erneut und vergeben dann einzelne Adressbereiche weiter an die Provider und Carrier.

Mit der Verteilung des letzten Segments haben die RIR's keine Möglichkeit mehr, Adressräume neu zu bekommen und müssen nun mit den ihnen zugeteilten Beständen auskommen. Zu wenig für das rasante Wachstum des Internets. Die folgende Grafik zeigt deutlich mit welcher Geschwindigkeit sich die Bestände entwickeln.

---

<sup>2</sup> Siehe IANA.org – „IANA IPv4 Adress Space Exhaust (2011-01-30)“ [IAN17]

<sup>3</sup> Vgl. Auswertung der off. IANA-Angaben „IPv4 Adress Report“ [Hus18; IAN17]

<sup>4</sup> Mitteilung ARIN – „ARIN IPv4 Free Pool Reaches Zero“ [Cur15]

<sup>5</sup> Mitteilung RIPE NCC – Vergabe von Adressen aus dem letzten /8 Adressbereich [NCC12]

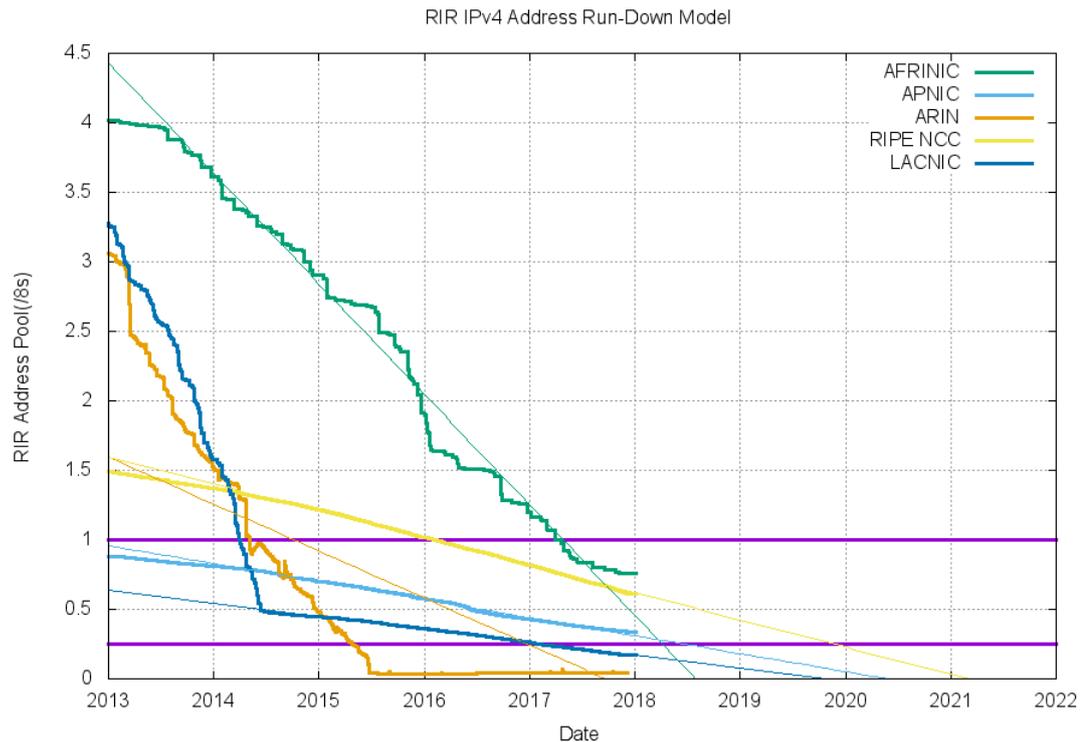


Abbildung 1: Prognosemodell - Reduktion IPv4 freier Adressvorrat der RIR's<sup>6</sup>

Zum aktuellen Zeitpunkt sind die Auswirkungen für die Endverbraucher nur bedingt erkennbar – wer das Internet ausschließlich zum Surfen und Emails versenden benutzt, der muss sich in der Regel mit den IP-Adressen nicht auseinandersetzen und trifft auch keine Auswahl über die zu nutzende Technologie.

Wer hingegen einen Webserver betreibt, erhält nur schwierig IPv4-Adressen. Häufig müssen sich mehrere Server/mehrere Dienste eine einzige öffentliche IPv4-Adresse teilen. Auch Heim- oder Firmennetzwerke (allg. LAN) bekommen i.d.R. nur eine einzige öffentliche IPv4-Adresse. IT-Fachleute stellen dann mit Technologien wie NAT, Port-Forwarding und VPN die geteilte Nutzung einer IP-Adresse durch mehrere Rechner sicher. Das Verfahren **NAT** gemäß der [RFC1631] ist heute hauptsächlich dafür verantwortlich, dass IPv4 überhaupt noch Verwendung finden kann. Diese Technologien sind jedoch häufig aufwändig – teilweise sogar so aufwändig, dass es mit IPv4 für manche technische Idee kein wirtschaftlich tragbares Konzept mehr gibt [Ahl16]. Darüber hinaus verhindern sie das ursprüngliche Ende-zu-Ende-Prinzip des Internets, bei dem jeder Host einen anderen anhand seiner öffentlichen IP-Adresse erreichen kann.

<sup>6</sup> Quelle: vgl. Huston, Geoff: IPv4 Adress Report [Hus18]

Ein Großteil der heute im Internet benutzten Dienste verwenden nach wie vor IPv4. Nicht jeder Diensteanbieter hat sich schon mit IPv6 beschäftigt. Die Nutzung von IPv6 steigt jedoch langsam an. Abbildung 2 zeigt, in welchem Maße sich die Anfragen an die Webseite des Internetportals [www.heise.de](http://www.heise.de) in Bezug auf die Nutzung von IPv6 entwickelt haben.

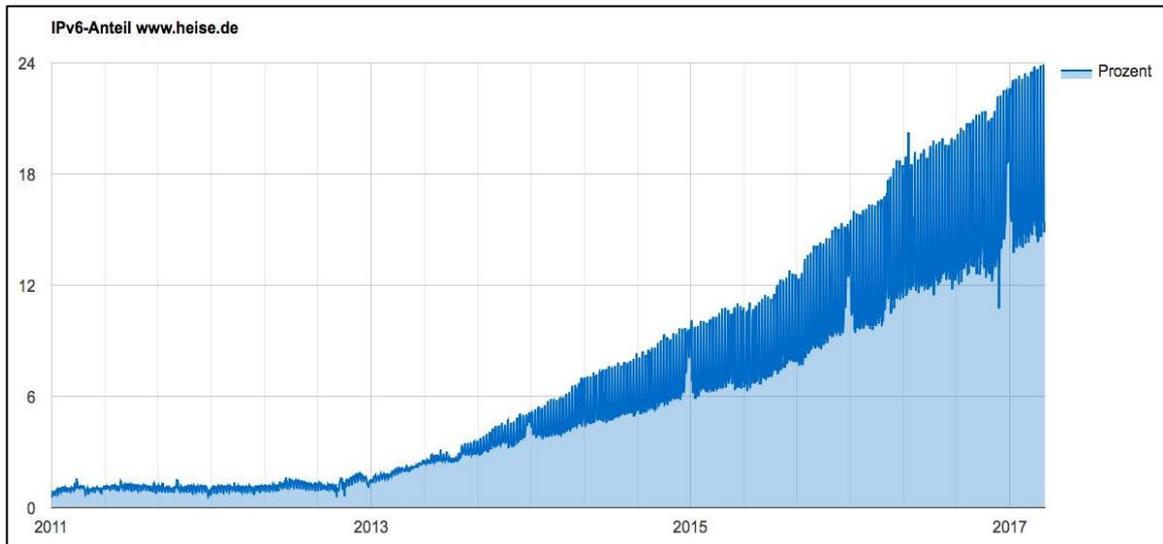


Abbildung 2: IPv6-Anteil auf [www.heise.de](http://www.heise.de)<sup>7</sup>

Hinzu kommt eine weitere Entwicklung, die - ähnlich der Diskussion über das richtige Internet-Protokoll - hohe Auswirkungen auf die verwendeten Technologien hat. Die Rede ist von „All-IP“.

Seit die Telekom die Abschaltung des klassischen ISDN-Netzes angekündigt hat (vgl. [Tel15]), verspricht der Begriff einen Handlungsdruck für alle, die Telefonanschlüsse betreiben oder mieten. Jedes Unternehmen, jeder Privatmensch muss in den nächsten Jahren seine bestehenden Telefonsysteme anpassen und VoIP-fähig gestalten.

Für viele Kunden passiert dieser Prozess relativ unproblematisch, da die Provider fertige Produkte anbieten, die vorkonfiguriert den Kunden erreichen und die wichtigsten Komponenten einer Netzwerkinfrastruktur bereits enthalten (Router, Firewall, VoIP-Telefonanlage, etc).

Für Unternehmen mit mittleren und größeren Telefonsystemen bedeutet die Umstellung jedoch häufig eine signifikante Herausforderung, da die eben genannten Produkte zumeist nur in kleineren Umgebungen skalieren (1-10 User). Kunden dieser Größenordnung können mit VoIP jedoch einen wesentlichen technologischen Vorteil nutzen, der in klassischen

<sup>7</sup> Quelle: vgl. Ahlers, Enst: Das Internet-Upgrade rollt: IPv4 wird abgelöst (2016) [Ahl16]

leitungsvermittelten Netzen nicht möglich war: Die Nutzung einer TK-Anlage, die ein Provider betreibt – in dieser Arbeit als „*Cloud-Telefonie*“ genannt. Richtig eingerichtet kann der Kunde an verschiedenen Standorten und sogar mobil zwischen den einzelnen Netzen telefonieren und das, obwohl er die zugehörige Telefonanlage selbst nie konfiguriert hat, sie nicht einmal selbst betreibt und häufig sogar mit vielen anderen Mandanten teilt. Solche Systeme werden von Providern i.d.R. als Dienst angeboten und mtl. abgerechnet. Abhängig von der Internetanbindung skalieren solche Systeme unproblematisch auch bis >100 Benutzer. Problematisch wird hier das unter IPv4 häufig eingesetzte NAT.

Während für die Umstellung auf VoIP am Markt etliche Lösungen existieren, ist die Transformation auf IPv6 in den meisten Netzwerken noch unzureichend - wenige Unternehmen haben bereits entsprechende Schritte eingeleitet. Dazu kommt, dass aktuell ebenfalls sehr wenige Dienste/Produkte überhaupt eine Unterstützung für IPv6 vorweisen können. So steht der migrationswillige Administrator vor einer Reihe sehr schwieriger Probleme. Das neue Internet-Protokoll, welches die vielen Probleme lösen könnte (z.Bsp. das NAT-Problem für VoIP-Telefonie), ist schlichtweg noch nicht ausreichend von den Herstellern und Dienste-Anbietern adaptiert.

## 1.2 Zielsetzung der Arbeit

Die Arbeit befasst sich mit den Bestandteilen IP-basierter Sprachkommunikationsnetze, wie sie typischerweise in kleingewerblichen Umgebungen genutzt werden. Sie untersucht speziell die Einsatzfähigkeit der beteiligten Komponenten und zeigt damit aktuelle Einsatzmöglichkeiten auf.

- **Darstellung der Vorteile und Umstiegsgründe auf VoIP/IPv6**
- **Ermittlung der Funktionalität aktuell verfügbarer VoIP-Telefonie-Produkte**
- **Ermittlung der Nutzbarkeit in IPv6-Netzwerken (DualStack/IPv6only)**
- **Darstellung typischer Probleme beim Aufbau von IPv6-Netzwerken mit VoIP**
- **BestPractice: Aufbau eines IPv6-Netzwerkes mit eingerichteter VoIP-Kommunikation**

### 1.3 Struktur der Arbeit

Die Arbeit führt in Kapitel 2 zunächst wichtige Begriffe ein, die in dieser Arbeit verwendet werden. Ebenso werden die verschiedenen Bestandteile und deren Rollen innerhalb der untersuchten Kommunikationsnetzwerke abgegrenzt und erklärt. Danach erfolgt die Vermittlung einiger theoretischer Grundlagen der verschiedenen wichtigen beteiligten Technologien und deren Bedeutung.

Im Kapitel 3 werden die verschiedenen Bestandteile eines Kommunikationsnetzwerkes untersucht und bewertet. Es wird erklärt, warum eine entsprechende Auswahl getroffen wurde, wie die Untersuchungen abliefen und zu welchen Ergebnissen die einzelnen Untersuchungen gekommen sind.

In Kapitel 4 werden die Untersuchungsergebnisse praktisch angewandt. Es wird gezeigt, wie ein empfohlenes Szenario für die Nutzung von VoIP-Technologie in einem IPv6-Netzwerk im SOHO-Bereich aussehen könnte. Aufgrund der Unterschiede zwischen IPv6 und IPv4 wird auch das Thema Sicherheit adressiert.

## 2 Stand von Wissenschaft und Technik

### 2.1 Begriffsdefinitionen

#### 2.1.1 SOHO-Netzwerke

**Kleine und mittlere Unternehmen** bilden in Deutschland rund 99,6% aller USt.-pflichtigen Unternehmen und beschäftigen 58,5% aller sozialversicherungspflichtig Beschäftigten [IfM17].

Zu den KMU zählen ebenfalls die **Kleinstunternehmen/Kleingewerbe** mit <9 Angestellten, welche in Deutschland mit etwa 3,25 Mio. Unternehmen und rund 89,1% der gesamten Anzahl aller Unternehmensformen die mit Abstand größte Gruppe darstellen<sup>8</sup>.

Diese Kleinstunternehmen benötigen und betreiben bereits heute EDV-Technik und Kommunikationsnetzwerke - sogenannte SOHO-Netzwerke (SmallOffice/HomeOffice) - verfügen aber i.d.R. nicht über angestellte IT-Fachkräfte oder große Budgets für Infrastruktur, so wie das in großen Unternehmen der Fall wäre. Aufgrund der besonderen Anforderungen (geringere Langlebigkeit, Skalierbarkeit, einfachere Installation, Wartung, usw.) werden spezielle SOHO-Produktlinien von Herstellern angeboten, die sich teilweise deutlich von den Enterprise-Produkten unterscheiden.

Für die Sprachkommunikation werden künftig in KMU ausschließlich VoIP-Lösungen Bedeutung haben, denn KMU sind auf die Anbieter angewiesen, und diese bieten klassische Technologien wie ISDN nur noch übergangsweise an. Mit der Verfügbarkeit von schnellen Breitbandanschlüssen setzen sich auch die NGN- bzw. All-IP-Anschlüsse durch womit die Telefonie bereits heute vielerorts VoIP entspricht.

In SOHO-Netzwerken wird heute noch vorwiegend das **IPv4**-Protokoll genutzt – doch auch die KMU müssen sich mit dem sich langsam verbreitenden **IPv6**-Protokoll beschäftigen. Niemand weiß genau, wie lange IPv4 noch in der Breite unterstützt wird, jedoch ist es sinnvoll, sich vorzubereiten und IPv6 bereits zu nutzen, wo es schon eingesetzt werden kann.

---

<sup>8</sup> Siehe Statistisches Bundesamt: Sonderauswertung des Unternehmensregisters im Auftrag des IfM Bonn, Jahrgang 2017 [IfM17]

## 2.1.2 Einteilung in Rollen/Bestandteile

VoIP-Lösungen bestehen im Groben aus 4 Bestandteilen:

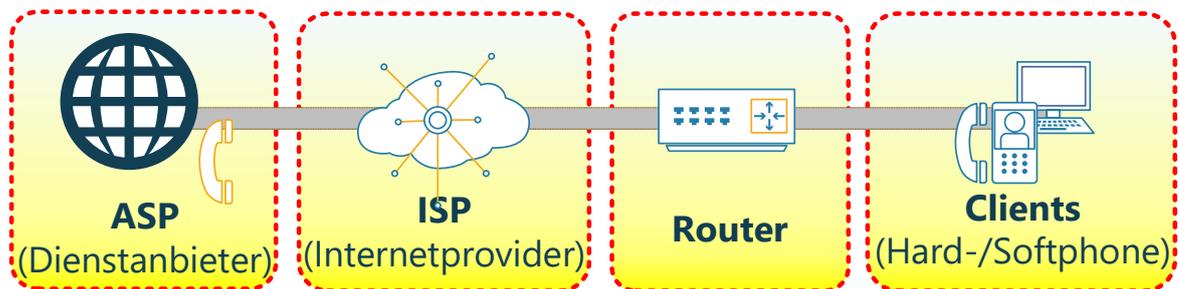


Abbildung 3: Bestandteile einer VoIP-Lösung

- a) **Application Service Provider (ASP)** – Diensteanbieter, der über IP-Protokoll Dienste zur Verfügung stellt, welche von den Clients genutzt werden. Dazu gehören im vorliegenden Fall eben die Internet Telephony Service Provider (**ITSP**). Diese ITSP können weiterhin unterteilt werden in solche, die die Vermittlung IP-basierter Telefonie in die klassischen Telefonnetze (PSTN, POTS) anbieten, und solche, die Telefonanlagendienste (cloudbasiert) anbieten. Bei Letzteren ist häufig die Vermittlung in die klassischen Telefonnetze ebenfalls inkludiert.
- b) **Internet Service Provider (ISP)** – Netzwerkinfrastrukturdienstleister, welche für den Endkunden die Internetkonnektivität herstellen. In manchen Fällen ist der ISP auch gleichzeitig ASP, nämlich immer dann, wenn er Mehrwertdienste wie Webspace, Emailadressen oder eben auch Internettelefonie zusammen mit dem Internetanschluss verkauft.
- c) **Router** – als zentrales Netzwerkgerät an der Schnittstelle zwischen Kundennetzwerk und ISP zuständig für die Internetanbindung (WAN) und Verwaltung des kundeneigenen Netzwerksegments (LAN). Router erfüllen allerdings häufig auch viele weitere Aufgaben. Sie sind oft Firewall, Telefonanlage, NAS-System u.v.m.
- d) **Clients** – Anwendungsprogramme, die auf unterschiedlichsten Betriebssystemen bzw. Hardwareprodukten (PC's, Smartphones, Tischtelefone, Tabletcomputer usw.) ausgeführt werden. Sie verbinden sich über IP mit dem Dienst eines ASP's und ermöglichen somit dessen Nutzung durch den Menschen. Unter Clients werden häufig nicht nur die Anwendungsprogramme selbst, sondern auch die Plattform auf der das Programm betrieben wird verstanden.

### 2.1.3 IP-Telefonie (VoIP)

1973, weit vor der Einführung von NGN-Anschlüssen und der Telekom-Offensive „Netz der Zukunft“ (vgl. Kap. 2.1.4 - Konvergente Netze: NGN, All-IP, „Netz der Zukunft“) wurde erstmals im Arpanet<sup>9</sup> die Übermittlung digitaler Sprache mittels des *Network Voice Protocol* vollführt [Lin81]. Zu diesem Zeitpunkt war das IP-Protokoll noch nicht definiert und viele Erkenntnisse kamen vorrangig den leitungsvermittelten Technologien wie ISDN zugute. Bis zur Verfügbarkeit von Sprachübertragungsprotokollen, die das Internet zur Übertragung nutzen, sollte es noch bis in die 1990er Jahre dauern. Die Technologie hat seit dem jedoch einen Namen – man nennt sie allgemein:

**Voice Over IP** – Die **paketvermittelte Sprachkommunikation auf IP-basierten Leitungswegen** (also dem Internet!).

Zur Unterscheidung:

- klassische Telefonnetze wurden als **leitungsvermittelte, verbindungsorientierte Kommunikationsnetze** aufgebaut. Die klassische Nachrichtenverbindung ist die „für eine bestimmte Zeit oder dauerhaft zur Verfügung stehende Kopplung zweier Kommunikationspartner zum Austausch von Nutzinformationen“ [RSL02, S. 3–5]. Das deutsche Fernsprechnet ermöglicht für analoge Anschlüsse Nachrichtenverbindungen für den Austausch von analogen Signalen zwischen 300Hz und 3400Hz. Digitale ISDN-Anschlüssen stellt es transparente 64-kbit/s-Verbindungen zur Verfügung. Eine solche Verbindung wird als Kanal bezeichnet.
- VoIP-Netze zählen hingegen aufgrund der genutzten Übertragungswege zu den **verbindungslosen, paketvermittelten Kommunikationsnetzen**. In diesen Netzen werden die Daten durch den Transport von Datenpaketen (Daten begrenzter Länge) übertragen. Die Datenpakete enthalten dabei Ursprungs- und Zieladresse der Übertragung. Sie werden im Laufe der Übertragung von den Stationen spontan gesendet, ohne einen vorherigen Verbindungsaufbau zur Zielstation. Auch einen Verbindungsabbau gibt es nicht. Eine Reservierung von Ressourcen speziell für die Verbindung kann aufgrund des fehlenden Verbindungsaufbaus ebenfalls nicht erfolgen. [RSL02, S. 5–7] Das Internet basiert auf diesen Übertragungsprinzipien. Da das Internet (als Kommunikationsnetz) und die Protokolle (IPv4, IPv6) Grundlage für Voice-Over-IP-Technologie sind, gelten für VoIP-Netze die gleichen Eigenschaften.

---

<sup>9</sup> Arpanet – **A**dvanced **R**esearch **P**rojects **A**gency **N**etwork – militärisch/wissenschaftlicher Vorläufer des heutigen Internets

IP-Telefonie (VoIP) ist eine Technologie die es ermöglicht, Telefondienste auf IP-Infrastrukturen zu realisieren, so dass diese herkömmliche Telefontechnologie samt ISDN und allen Komponenten ersetzen kann. Zusätzlich ermöglicht die Technologie ganz neue Arten von Endgeräten und Architekturen. Beispiele:

- gebührenfreie Telefonie
- Softwaretelefonie
- geographisch verteilte Callcenter
- Cloudbasierte Telefonanlagen
- OneNumber-Konzepte, u.v.m.

Sinnvoll konfiguriert bewirkt IP-Telefonie Kostenersparnisse und erhöht die Flexibilität.

Kritiker bemängeln die gegenüber klassischen Telefonnetzen (z.Bsp. ISDN) geringere Zuverlässigkeit. IP-Telefonie kann immer nur so zuverlässig sein wie das genutzte IP-Netz. Allerdings bieten sich auch neue Möglichkeiten zur Schaffung von Redundanzen, welche in klassischen Netzen nicht möglich sind. So können zur Anbindung einer TK-Anlage statt einem auch mehrere Internetanschlüsse verwendet werden. Ist das Routing ordentlich konfiguriert, wäre ein Ausfall einer Internetleitung kompensierbar und nicht mit einer Betriebsunterbrechung der Telefonie verbunden. Die Teilnehmer könnten weiterhin telefonieren. Den Sprachpaketen ist es egal, welchen Weg sie nehmen.

#### **2.1.4 Konvergente Netze: NGN, All-IP, „Netz der Zukunft“**

Das „*Netz der Zukunft*“ ist vor Allem ein Werbebegriff der deutschen Telekom AG, der damit ein sogenanntes All-IP-Netz - oder auch NGN (Next Generation Network) bezeichnet. Es handelt sich dabei um eine einheitliche Infrastruktur, die alle Arten von Informationen übertragen kann – egal ob Webseiten, Emails, Telefonie, Video, Fernsehen etc. – Ein konvergentes Netz für Dienste aller Art!

Das Internetprotokoll (IP), welches zwar speziell für die Übertragung von Daten ausgelegt wurde, jedoch in seiner Nutzung so besonders vielseitig ist, dass Daten, Sprache und Videos gleichzeitig übertragen werden können ist die Grundlage für ein solches konvergentes Netz.

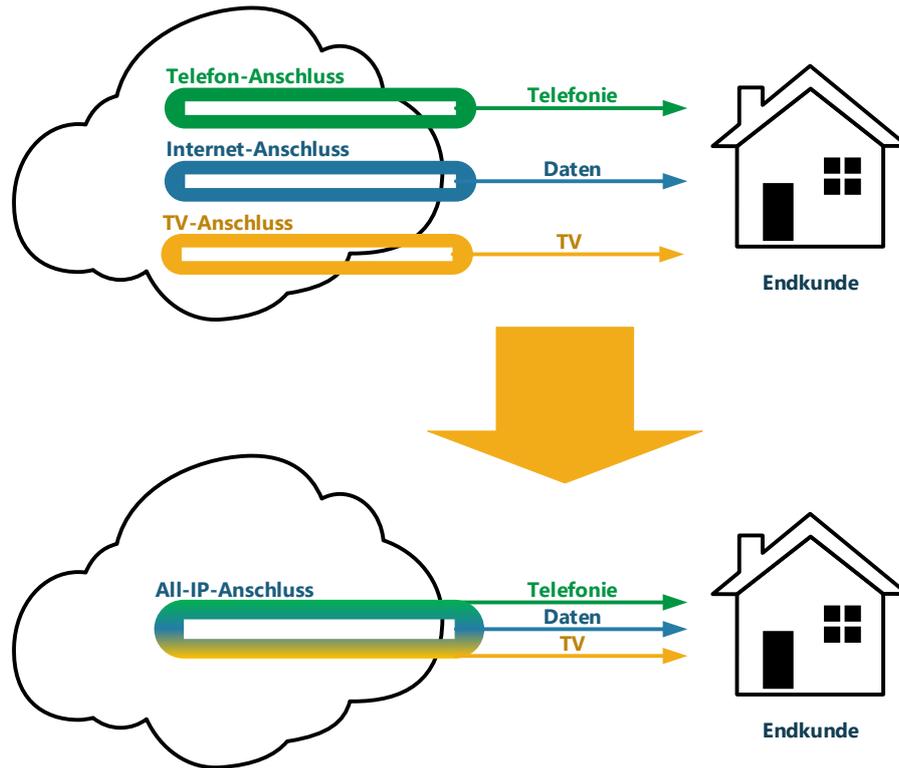


Abbildung 4: konvergenter Anschluss (NGN) - aus vielen Medien wird eins

In der Vergangenheit wurden für unterschiedliche Medien jeweils eigene Netze gepflegt. Carrier arbeiten jedoch weltweit daran, ihre Infrastruktur auf IP-Technologie umzustellen – auch die Telekom. Konnte die Telekom jahrzehntelang ihr (eigentlich ja noch recht modernes) ISDN-Netz für Sprache aber auch Datendienste vermarkten, so steht dessen weiterer Betrieb derzeit dem Fortschritt eher entgegen. Geringe realisierbare Bandbreiten (64kbit/s je Kanal) und der leitungsvermittelte Charakter begrenzen die Technologie aus heutiger Sicht. Konsequenterweise wurde beschlossen, deren Einsatz zu beenden [Tel15] und stattdessen auf All-IP-Anschlüsse (im Telekom-Sprachgebrauch „Netz der Zukunft“) zu migrieren. Für die nunmehr veraltete ISDN-Technik wird es keine Ersatzteile und keinen Service mehr geben. Die folgende Grafik zeigt, wie sich die Sprach- und Datenkommunikation in den vergangenen 20 Jahren entwickelt hat [Tel15]. Kurz vor der Jahrtausendwende, als das Internet zum Massenphänomen wurde, wurde Sprache erstmals häufiger über das Daten- als über das Sprachnetz transportiert.

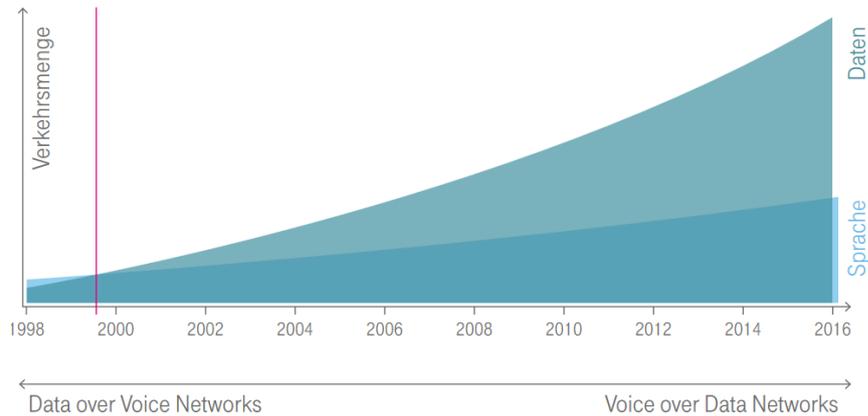


Abbildung 5: Vergleich Sprachverbindungen auf den Telekom-Netzen<sup>10</sup>

Die Realisierung von All-IP-Technologie für Haushalte/Unternehmen erfordert breitbandige Internetanschlüsse (siehe 2.1.5)

### 2.1.5 Breitband-Internetanschlüsse

Der Begriff „Breitband“ ist in der Literatur nicht einheitlich definiert. In der vorliegenden Arbeit werden solche IP-basierten Datenanbindungen als breitbandig verstanden, deren Leitungseigenschaften (v.a. Bandbreite) dem Nutzer die gleichzeitige Nutzung von Medien (Internet, Telefonie,...) ermöglichen und ihn darin nicht limitieren. Geht man von einer einfachen Nutzung (Surfen, Telefonieren, Emails schreiben für 2-3 Personen) aus, so ist ein DSL-Anschluss mit einer Bandbreite von 6Mbit/s ↓ sowie 375kBit/s ↑ durchaus ausreichend, wenn auch nicht besonders komfortabel. Die Bandbreite würde ausreichen, um die gewünschten Dienste abzubilden. Der Anschluss kann trotz möglicherweise anderem Empfindens durch die Nutzer als breitbandig betrachtet werden. Für heute bereits zumeist propagierte „TriplePlay“-Anschlüsse – also Anschlüsse die auch für das Streaming von Video (TV) und viele andere multimediale Dienste geeignet sind, werden jedoch Bandbreiten ab 25Mbit/s benötigt.

Die Bundesregierung treibt politisch den Ausbau des Netzes voran und fördert Kommunen bei der Erschließung von Teilnehmern. Ziel des verantwortlichen Ministeriums (BMVI) ist ein technologieneutraler, flächendeckender Netzausbau für Internetanschlüsse mit mind. 50Mbit/s oder mehr bis zum Jahr 2018 [Bun17; Dob15]. Damit ist aktuell bereits eine hohe Abdeckung des Bundesgebiets mit in unserem Sinne breitbandigen Internetanschlüssen erreicht. Es gibt nur noch vergleichsweise wenige Gebiete in Deutschland, in denen

<sup>10</sup> Quelle: vgl. Telekom: Das Netz der Zukunft – Chancen und Nutzen der IP-Technologie (2015) [Tel15]

weniger als 95% der Internetanschlüsse mit Bandbreiten > 6Mbit realisiert werden können. Gemäß der aktuellen Statistik des BMVI gibt es eine Verfügbarkeit solcher Bandbreiten in 99,0% aller Haushalte, wobei das BMVI bei dieser Bewertung nichtmehr zwischen den verschiedenen Technologien unterscheidet (drahtlos, kabelgebunden).

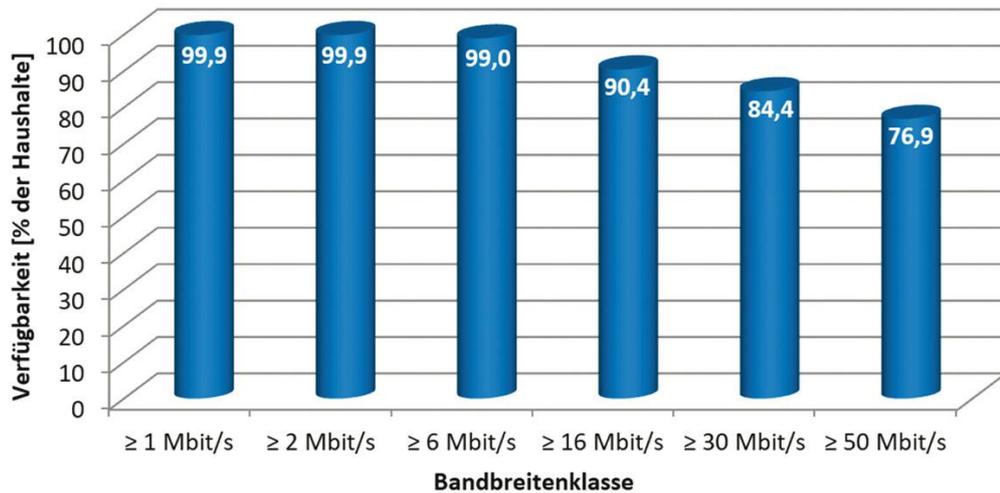


Abbildung 6: Breitbandverfügbarkeit in Deutschland nach Bandbreitenklassen<sup>11</sup>

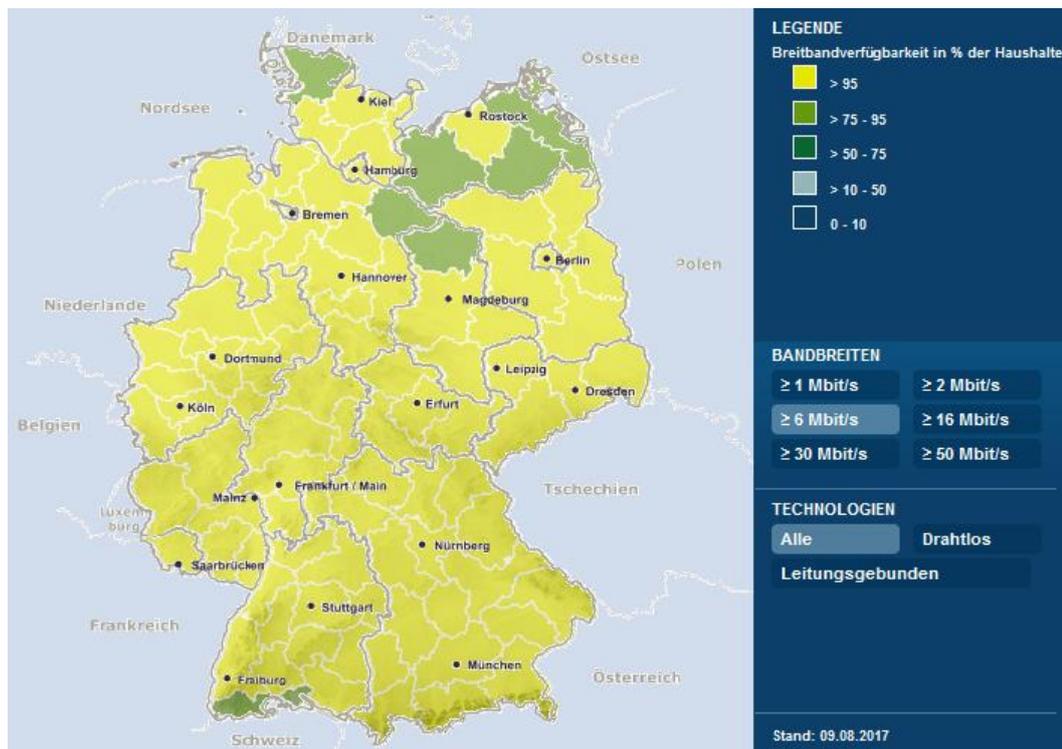


Abbildung 7: Breitbandverfügbarkeit ≥ 6MBit in Deutschland<sup>12</sup>

<sup>11</sup> Quelle: vgl. BMVI: Aktuelle Breitbandverfügbarkeit in Deutschland (Stand Mitte 2017) [Bun17]

<sup>12</sup> Quelle: vgl. BMVI: Aktuelle Breitbandverfügbarkeit in Deutschland (Stand Mitte 2017) [Bun17]

## 2.2 Internet Protokoll (IP)

Das Internet-Protokoll (IP) ist das grundlegende Kommunikationsprotokoll moderner Kommunikationsnetze und legt fest, wie Datenpakete zwischen Kommunikationspartnern ausgetauscht werden. Es bildet heute die Basis des Internets. IP wird dabei häufig als Sammelbegriff verwendet, denn durch die Vielzahl an weiteren Protokollen, die zur Familie der Internetprotokolle gezählt werden, ist heute nahezu jeder gebräuchliche Kommunikationskanal mittels IP-basierter Verbindungen abbildbar.

Um die Kommunikationsprotokolle einzuordnen, existiert das ISO/OSI-Referenzmodell [ITU-X.200]. IP ist dabei das grundlegende Transportprotokoll in der Vermittlungsschicht (Layer 3). Alle anderen, der Protokollfamilie zugehörigen Protokolle, sind den höheren Schichten zuzuordnen und nutzen IP.

### 2.2.1 IPv4

Hauptsächlich verbreitet ist die Kommunikation auf Basis der Version 4 des Internet-Protokolls (**IPv4**), welche 1981 durch die IETF festgelegt wurde [RFC791]. Alle vorigen Versionen werden als experimentell bezeichnet. Ebenfalls experimenteller Natur ist IPv5. Erst das 1998 durch die IETF festgelegte **IPv6**-Protokoll ist ein ernstzunehmender Nachfolger und soll die Probleme von IPv4 (z.B. begrenzter Adressvorrat) lösen und neue Anforderungen integrieren.

IPv4 besitzt einen Adressraum, der insgesamt  $2^{32}$  (~ 4Mrd.) mögliche Adressen umfasst. Dieser Adressraum reicht bereits heute nicht für alle mit dem Internet verbundenen Geräte aus. Das Verfahren Network-Adress-Translation (NAT) kommt deshalb häufig zum Einsatz. Dieses Verfahren verletzt jedoch die ursprüngliche Idee hinter dem Internet-Protokoll, nach der jeder Host einen anderen anhand seiner IP-Adresse erreichen kann.

### 2.2.2 IPv6

IPv6 ist eine Weiterentwicklung von IPv4. Das Protokoll ist in den meisten modernen Betriebssystemen bereits enthalten und funktioniert aufgrund seiner Autokonfigurationsmechanismen häufig ohne zusätzliche Maßnahmen. 1996 wurde mit dem 6Bone das erste IPv6-Netzwerk begründet<sup>13</sup>. 1998 wurde das Protokoll von der IETF verabschiedet [RFC2460]. Seitdem wurden viele zusätzliche Protokolle standardisiert, die zur IPv6-Protokollfamilie gehören. In der Zwischenzeit hat sich IPv6 weltweit

---

<sup>13</sup> Quelle: 6Bone – über 1000 Hosts in über 50 Ländern der Welt, <http://g06.net/ipv6-6bone>

unterschiedlich stark verbreitet. Asien hat das neue Protokoll besonders schnell angenommen, was anhand der Verteilung der Weltbevölkerung im Gegensatz zur Verteilung der IPv4-Adressen konsequent ist.

Die wesentlichen Neuerungen:

- **Erweiterter Adressraum**

Das Adressformat wurde von 32bit auf 128bit erweitert. Dadurch stehen genügend Adressen für jedes Sandkorn zur Verfügung<sup>14</sup>.

- **Autokonfiguration**

Ein neues Feature von IPv6 ermöglicht die Selbst-Zuweisung einer eindeutigen Adresse, ohne dass ein DHCP-Server oder manuelle Konfiguration benötigt werden. Das mit Stateless-Address-Autoconfiguration (SLAAC) bezeichnete Verfahren soll künftig viel Aufwand in der Verwaltung von IP-Adressen ersparen.

- **Flexible Headerstruktur**

Der neu eingeführte Header für IPv6-Pakete ist schlanker, was die Verarbeitung von Paketen beschleunigt. Zusätzlich ist er mit Extension-Headern flexibel erweiterbar, auch solchen, die heute noch nicht definiert sind. Aktuell integriert IPv6 beispielsweise bereits Extension-Header für *Quality-Of-Service*, *Security* (Verschlüsselung und Authentifizierung, statt VPN) und *Mobile IPv6* – Funktionen, die unter IPv4 einen erhöhten Aufwand bedeuteten.

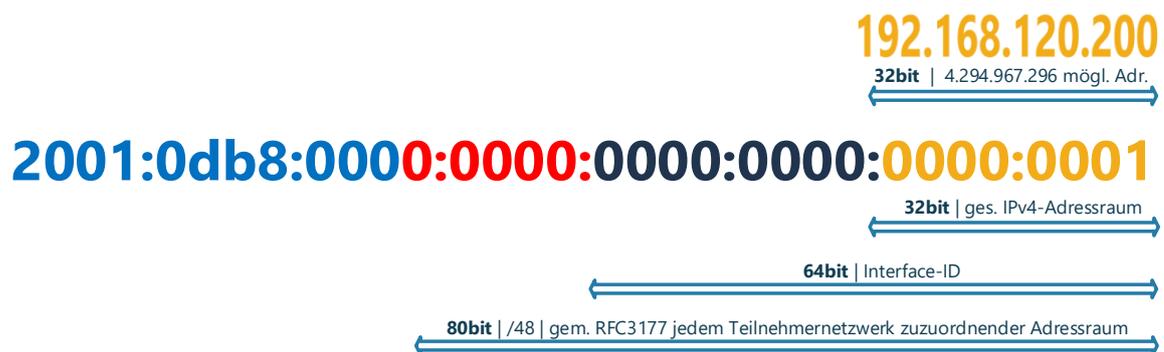


Abbildung 8: Vergleich Adressbereiche IPv4/IPv6

Da IPv6 eine 128bit-Addressierung (vgl. IPv4: 32bit) sowie einen neuen Headeraufbau verwendet, ist es nicht mit IPv4 kompatibel. Eine Koexistenz ist jedoch möglich. Man spricht dann von **DualStack**, da beide IP-Stacks auf demselben Netzzugang zeitgleich vorkommen können.

IPv6 ist bereits voreingestellt in modernen Betriebssystemen implementiert und aktiviert.

<sup>14</sup> Herleitung siehe: [Hag09, S. 5–6]

### 2.2.3 Vorteile und Umstiegsgründe

Das IPv4-Protokoll hat bereits eine seit über 30 Jahren andauernde Erfolgsgeschichte. Aber auch die Entwickler von IPv4 haben die rasante Verbreitung des Internets nicht vorausgesehen. Die zuvor genannten Änderungen (erweiterter Adressraum, Autokonfiguration, flexible Headerstruktur) liefern folgende **Umstiegsgründe**:

- Begrenzter IPv4-Adressraum bereits heute aufgebraucht
- Zusätzlicher Bedarf für IoT-Geräte in IPv4 nicht abdeckbar
- Fehlende Autokonfigurationsmöglichkeiten in IPv4 erzeugen hohen Administrationsaufwand
- Neuer IPv6-Header legt Grundlage für Anpassungen an zukünftige Innovationen  
Viele neue Technologien (z.Bsp. Microsoft Direct Access) unterstützen nur noch IPv6
- Der alte IPv4-Header unterstützt keine Sicherheitsfunktionen. Verschlüsselungen müssen auf höheren Schichten hergestellt werden. Der IPv6-Header unterstützt hingegen einen IPSec-Extension-Header. Damit sind Möglichkeiten zur Verschlüsselung bereits in das Protokoll integriert.
- IPv6 unterstützt neue „TrafficClass“-Header mit denen sich Multimediaanwendungen wie VoIP besser priorisieren lassen.
- NAT verletzt Ende-zu-Ende-Prinzip des Internets.  
Viele Technologien können unter IPv4 nur mit zusätzlichen Einrichtungen funktionieren. VoIP benötigt über Netzwerkgrenzen hinweg beispielsweise STUN-Server und Proxies, obwohl Medienströme am sinnvollsten von Endpunkt zu Endpunkt ausgetauscht würden.

Der wichtigste Grund für die Einführung von IPv6 ist der zu geringe Adressraum von IPv4.

### 2.2.4 DualStack-Verfahren

Das Ziel jeder Migration sollte das reine IPv6-only-Netzwerk sein. Jedoch ist davon auszugehen, dass IPv6 und IPv4 in den meisten Netzwerken wohl sehr lange parallel existieren werden. Die Verbreitung hängt letztlich stark von der Verfügbarkeit der Internetdienste unter dem neuen Protokoll ab, wie sie in Kap. 3 – „Untersuchung im Versuchsnetz“ untersucht werden.

Für den Übergang zu IPv6 kommen spezielle Techniken zum Einsatz:

- **Dual-Stack-Techniken** erlauben die Koexistenz von IPv4 und IPv6 in denselben Geräten und Netzwerken.
- **Translationstechniken** ermöglichen Kommunikation von IPv4-Knoten mit IPv6-Knoten. (Netzwerkadress- und -Protokollübersetzung)
- **Tunneltechniken** ermöglichen den Transport von IPv6-Paketen über IPv4-basierte Infrastruktur bzw. den Transport von IPv4-Paketen über IPv6-basierte Infrastruktur. (Encapsulation)

Solange in einem Kommunikationsnetzwerk beide Formen von IP vorkommen, redet man von einer Dual-Stack-Umgebung. Da während der Übergangszeit sowohl Applikationen existieren, die beide Protokolle unterstützen, als auch Anwendungen die entweder nur IPv4 oder nur IPv6 unterstützen, sichert das Vorhandensein beider Protokolle die Nutzbarkeit der Anwendungen im Netzwerk. Die als „sanfte Migration“ bezeichnete Methode ermöglicht eine angenehmere Umstellungsgeschwindigkeit und ist i.d.R. mit den geringeren Kosten verbunden.

Es muss jedoch beachtet werden, dass der Einsatz von DualStack auch die Konfiguration und Unterhaltung zweier Protokolle auf Hosts, Routern, Firewalls etc. bedeutet.

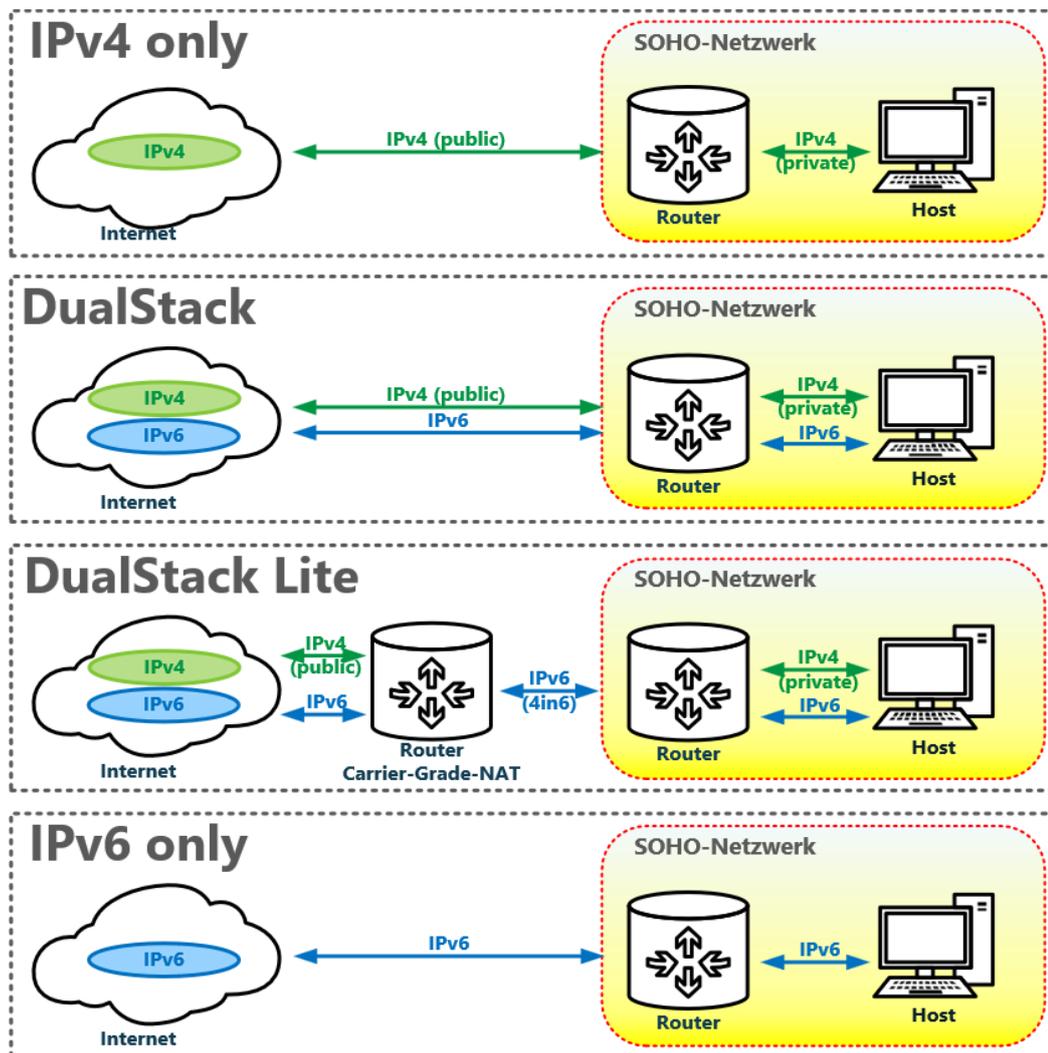


Abbildung 9: Vergleich ausgewählter IP-Stack-Realisierungen

Der DualStack-Ansatz ist allerdings nur einsetzbar, wenn genügend IPv4-Adressen vorhanden sind. Andernfalls müssen andere Technologien wie 6to4, 6rd oder DS-Lite eingesetzt werden. [Hag09, S. 399–402]

### 2.2.5 DS-Lite

Bei DualStack-Lite haben die Knoten ebenfalls beide IP-Versionen vollständig implementiert, jedoch verfügen sie nur über eingeschränkt erreichbare IPv4-Adressen aus den privaten Adressräumen. Damit IPv4-Anwendungen auf den Hosts mit dem IPv4-Internet kommunizieren können, stellen die Provider vielen Kunden gemeinsame NAT-Router zur Verfügung, die aufgrund von Größe, Komplexität und Leistungsfähigkeit Carrier-Grade-NAT genannt werden. Das private „LAN“ dehnt sich damit bis zum Provider aus. Für den Transport der IPv4-Pakete wird entlang der Übertragungsstrecke häufig auf eine zusätzliche Implementierung des IPv4-Protokolls verzichtet. IPv4 wird dann oft als IPv4-in-IPv6 getunnelt.

Viele Provider nutzen diese Technologie. Vor allem dann, wenn sie ungenügend IPv4-Adressen für Ihre Kundenanschlüsse zugeteilt bekommen haben. In Deutschland betrifft dies vor allem die Kabelnetzbetreiber<sup>15</sup>. DS-Lite wurde durch die IETF entwickelt und ist in [RFC6333] festgeschrieben.

DS-Lite-Kunden können jedoch aufgrund der Tatsache, dass sie über keine öffentlich geroutete IPv4-Adresse verfügen, auch keine Portfreigaben für IPv4 nutzen. Damit können hinter einem DS-Lite-Anschluss keine Geräte erreicht werden, die IPv6 nicht unterstützen. Gerade SOHO-Benutzer nutzen jedoch Portfreigaben um auf NAS-Systeme o.Ä. zuzugreifen. Auch der Betrieb einer IPv4-Telefonanlage hinter einem DS-Lite-Anschluss ist unmöglich.

---

<sup>15</sup> Vgl. Abschnitt 3.3.2 - Anbieter die DS-Lite verwenden

## 2.3 SIP

Für die Übertragung von Sprache in Paketen werden Protokolle benötigt, die gemäß ISO-OSI-7-Schichten-Modell ab Schicht 4 an das IP-Protokoll anschließen.

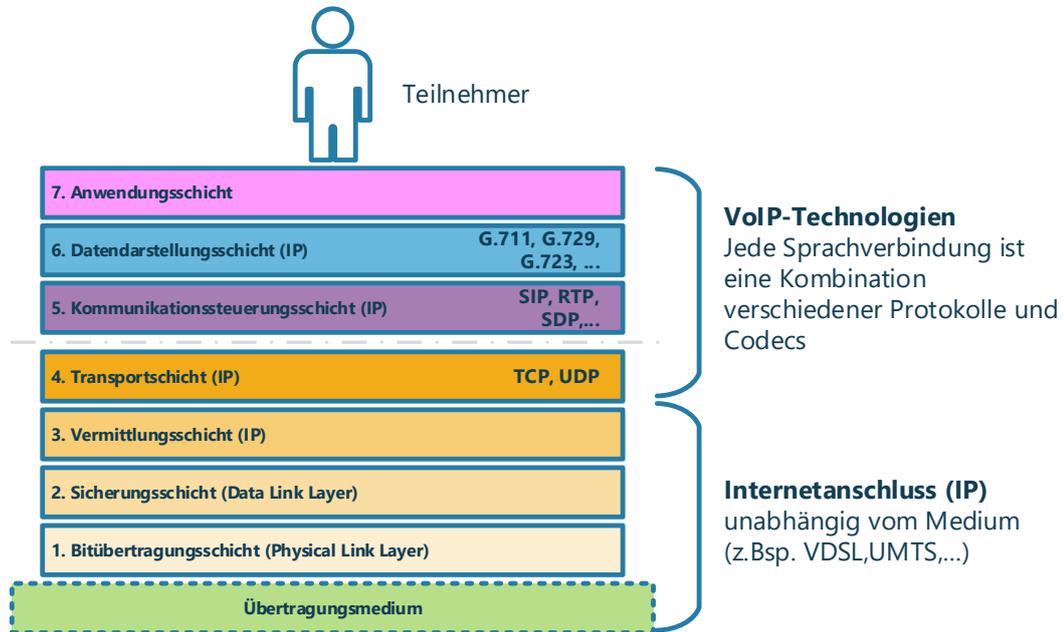


Abbildung 10: Einordnung von VoIP-Protokollen in OSI/ISO-Modell

Bereits ab 1996 verbreitete sich der von der ITU-T spezifizierte **H.323**-Standard, eine ganze Protokollfamilie, welche Regeln zur audio-visuellen Kommunikation auf paketvermittelten Netzwerken enthält [ITU-H.323]. H.323 kann stark vereinfacht als *ISDN over IP* bezeichnet werden und hat viele Grundlagen geschaffen, inzwischen spielt H.323 jedoch nur noch eine untergeordnete Rolle.

Seit 2002 gibt es zusätzlich das **Session-Initiation-Protokoll (SIP)**-Protokoll. Dieses wurde im Gegensatz zu H.323 von der IETF festgelegt und berücksichtigt stärker als H.323 die Stärken und Schwächen von IP-Netzen. Besonders der Einsatz im Zusammenhang mit NAT (welches insb. bei IPv4-Netzwerken häufig nötig ist) ist nur mit SIP sinnvoll möglich. Unter H.323 muss dazu hoher Aufwand betrieben werden. SIP ist allgemeingültiger gehalten und kann Sitzungen beliebiger Art verwalten (nicht nur Telefonie). Seine starke Anlehnung an das http-Protokoll macht SIP besonders beliebt für Internetanwendungen. Der Flexibilitätsgrad ist insgesamt deutlich höher als der von H.323. **SIP** ist heute das wohl wichtigste Protokoll in der IP-basierten, audiovisuellen Kommunikation. Das ist insofern erstaunlich, da SIP selbst nicht einen Ton oder ein Videosignal überträgt. Vielmehr ist SIP das Steuerprotokoll, welches verwendet wird, um IP-basierte Kommunikationssitzungen (z.Bsp. Telefonate, Videokonferenzen, Radiostreams etc.) einzuleiten, zu steuern und wieder abzubauen [RFC3261].

Es verwendet zusätzliche andere Protokolle und Codecs, um einzelne Aufgaben abzubilden. So wird häufig das *Realtime-Transport-Protokoll* RTP verwendet, um die eigentliche Sprache im sog. Medienstrom zu übertragen. Verschlüsselte Verbindungen verwenden hingegen häufig SRTP (die verschlüsselte Variante von RTP). Die Auflösung von Servern passiert mittels DNS-Protokoll. Sprache wird mithilfe von Codecs wie G.711 codiert.

VoIP bzw. SIP kann sehr unterschiedlich realisiert werden. Missverständlich ist für Kunden bereits häufig die Verwendung des Begriffes VoIP, denn der Kauf von VoIP-Produkten (bzw. IP-fähigen Produkten) sagt noch nicht aus, auf welchem Teil eines Kommunikationsnetzes die Technologie auch eingesetzt wird. Die Auswahl der Systemlösung und die Entscheidung über einen Migrationsweg sind oft von vielen Kriterien abhängig. Falls eine vollkommen neue und konvergente Netzwerkstruktur mit VoIP aufgebaut werden soll, sollte ein reines Softswitch-basiertes VoIP-System bevorzugt werden. Die zentralen Telefonanlagen-Vermittlungs-Funktionen werden in diesem Fall durch eine Software übernommen. Vgl. [Bad10, 398-417]

### 2.3.1 TK-System im lokalen LAN, SIP-Trunking zum Carrier

Im Normalfall betreibt der SOHO-Kunde eine Telefonanlage (PBX). Ist diese IP-fähig, dann heißt diese auch kurz **IP-PBX**. Wird nur eine Seite der IP-PBX (extern/SIP-Trunk oder intern/SIP-Clients) IP-basiert genutzt, so spricht man von einem hybriden Szenario.

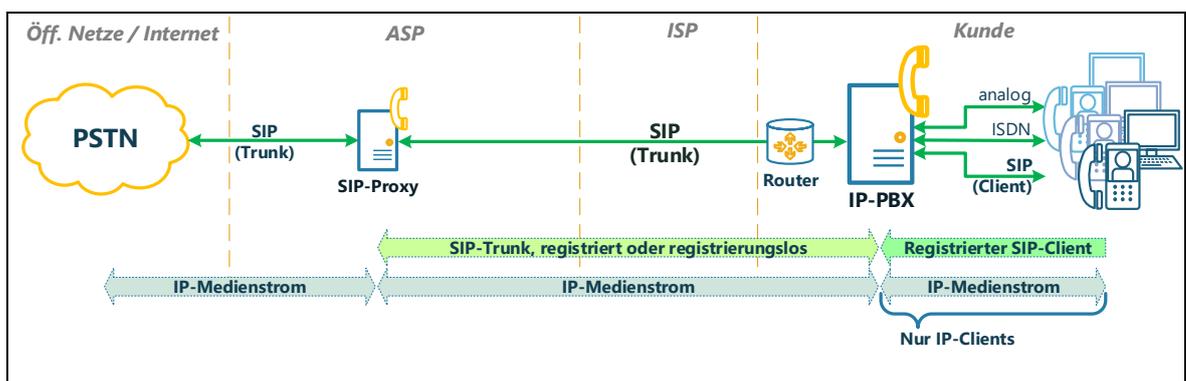


Abbildung 11: IP-basiertes TK-System mit versch. Clients im Kundennetz

Das TK-System (IP-PBX) dient typischerweise den Clients im lokalen Netz als **Registrar** und **Proxy**. Jeder Client muss sich bei ihm registrieren. Damit weiß die IP-PBX jederzeit, welcher Client unter welcher IP zu erreichen ist und kann Telefonate übermitteln. Telefonate werden von ihr sowohl gesteuert (CallControl, SIP), aber auch die Audio-Daten (Medienstrom, RTP) empfängt die IP-PBX, codiert sie ggf. um und sendet sie weiter.

**SIP-Client**-Verbindungen sind vorübergehend bestehende Verbindungen<sup>16</sup> zwischen einer IP-PBX und einem Client. Ihnen ist i.d.R. exakt eine Rufnummer zugeordnet und der Client entspricht exakt einem Teilnehmer. Theoretisch gibt es zwar keine Grenze, aber für einen SIP-Client sind meist nur 1-2 gleichzeitige Gesprächsverbindungen erlaubt.

Zum PSTN nutzt die IP-PBX einen **SIP-Trunk**. Dies ist eine dauerhafte SIP-Verbindung zwischen der IP-PBX und einem ITSP, der die Gespräche des Trunks im öffentlichen Telefonnetz zustellt und auch die Rufnummern des Kunden routet und am SIP-Trunk zuordnet. SIP-Trunks lassen i.d.R. mehrere gleichzeitige Gespräche zu. Ihre theoretische Anzahl ist nur begrenzt durch Leitungskapazitäten und mögl. freie Ports. Die ITSP nutzen jedoch künstliche Limits Abgrenzung unterschiedlicher Produktgrößen. SIP-Trunks können als Nachfolger des klassischen ISDN-Anlagenanschlusses aufgefasst werden.

### 2.3.2 TK-System beim Carrier

Werden im lokalen Netzwerk nur IP-fähige Clients genutzt (darunter zählen auch analoge Geräte hinter einem IP-Analog-Gateway), dann kann die IP-PBX auch außerhalb des lokalen Netzwerkes existieren. Heutige Diensteanbieter wie z.Bsp. Sippgate nutzen diese Eigenschaft und betreiben große IP-PBX-Systeme in ihren eigenen Rechenzentren.

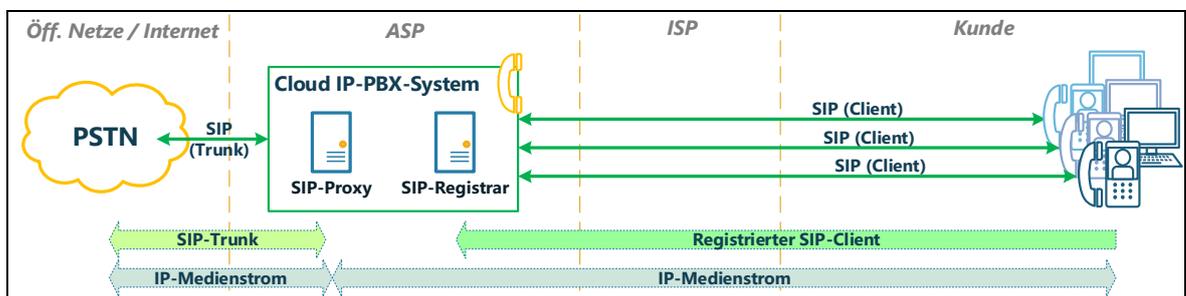


Abbildung 12: IP-basiertes TK-System aus der Cloud

Diese Systeme sind mandantenfähig aufgebaut und erlauben die Bereitstellung von SIP-Client-Profilen für viele unterschiedliche Kunden. Zusätzlich werden oft Systeme unter dem Begriff Centrex<sup>17</sup>-Anlagen vermarktet. Dann handelt es sich i.d.R. nicht um ein gemeinschaftlich genutztes System, sondern um eine Cloud-IP-PBX, die der Kunde allein nutzen und konfigurieren kann. Die ASP trennen bei all diesen cloudbasierten IP-PBX-

<sup>16</sup> Vorübergehend heißt: solange der Client „registriert“ ist. Dies kann auch permanent sein - jedoch ist die Dauerhaftigkeit nicht verpflichtend. Vgl. [Kan05, 93 ff.] „Netzarchitekturen mit SIP“

<sup>17</sup> Centrex – Central Office Exchange. Synonyme: HostedPBX, NetPBX, virtuelle Telefonanlage.

Systemen die einzelnen SIP-Funktionen (Registrar, Proxy, ...) um skalieren zu können und höhere Verfügbarkeiten zu erreichen.

Cloudbasierte TK-Anlagen sind kostengünstig zu betreiben und daher sehr interessant für KMU. Zusätzlich erlauben sie auch zeitgleich die Nutzung des Systems an verschiedenen Standorten.

**Problem NAT:** Bei cloudbasierten IP-PBX baut i.d.R. jeder Client eine eigene Verbindung zum ASP auf. Dies geht jedoch nicht bei der Nutzung von NAT, da jeder Client seine SIP-Datenpakete unter Port 5060 erwartet. Zur Abhilfe müssen für jeden Client separate Ports konfiguriert oder ein gemeinsamer VPN-Tunnel zum ASP etabliert werden, sodass die Clients in der Kommunikation mit dem Registrar jeder über eine eigene (lok.) IP verfügen.

**IPv6** verspricht das Port-Problem zu lösen, da der Port 5060 für jede einzelne globale Unicast-Adresse existiert. Die Tests unter Punkt 3 - *Untersuchung im Versuchsnetz* zeigen, ob dies funktioniert.

### 2.3.3 NGN-Anschlüsse: TK-Anlage beim Carrier, Proxy-Gateway im LAN

Klassischerweise sind Internetanbieter diejenigen Unternehmen, die zuvor auch Telefonanbieter waren. Daher haben diese Provider ein besonderes Interesse, beides aus einer Hand anzubieten. Sehr häufig werden Internet-Service-Provider gleichzeitig zu Internet-Telefonie-Service-Providern und bieten kombinierte Produkte an. Wie bereits unter Abschnitt 2.1.4 - *Konvergente Netze: NGN, All-IP, „Netz der Zukunft“* beschrieben, stellen die Provider auf sog. Next-Generation-Network-Anschlüsse (NGN) um. Dabei handelt es sich um Internetanschlüsse, zu denen zeitgleich eine VoIP-Infrastruktur bereitgestellt wird. Die Besonderheit dabei ist, dass der ISP einen Router mitliefert, der über eingebaute IP-analog- und/oder IP-DECT- bzw. IP-ISDN-Gateway-Technik verfügt. Damit kann der Kundenrouter direkt an das Cloud-IP-PBX-System des ISP angebunden werden und dem Kunden gewohnte Schnittstellen für seine Telefongeräte anbieten. Der Anbieter kann die kostengünstige IP-Infrastruktur nutzen und muss dem Kunden keinen zus. Telefonanschluss mehr bereitstellen.

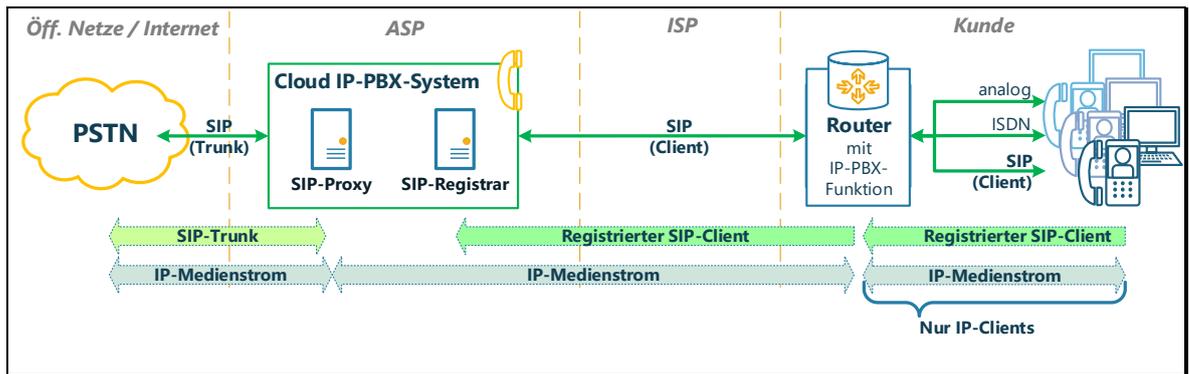


Abbildung 13: NGN-Realisierung, Cloud-TK-System mit lokalem Proxy (im Router)

Die NGN-Variante ist kundenseitig zwar mit zusätzlicher Hardware verbunden, ermöglicht jedoch eine Umgehung des NAT-Problems, da die öffentliche IP-Adresse nur vom Router genutzt wird. Dieser agiert als kombinierter Proxy und Registrar im LAN und ermöglicht damit sogar interne Gespräche bei ausgefallener Internetleitung.

SIP-Client-Konten an NGN-Anschlüssen sind leider häufig auf die normalen Telefoniefunktionen reduziert und bieten wenige Funktionen guter Telefonanlagen (CTI, Präsenzstatus, funktionale Soft-Clients,...). Deshalb können im Einzelfall die anderen Varianten auch für einen SOHO-Kunden sinnvoller sein.

### 3 Untersuchung im Versuchsnetz

#### 3.1 Aufbau des Versuchsnetzes

Zur Untersuchung soll jede Komponente (vgl. Kap. 2.1.2 - Einteilung in Rollen/Bestandteile) einzeln betrachtet und ein kontextbezogener Vergleich angestellt werden. Zur Beurteilung der Fähigkeiten wurden IPv4 und IPv6 selektiv auf den betroffenen Netzwerkinterfaces deaktiviert/aktiviert. Grundlage des Versuchsnetzwerkes ist ein IPv6-fähiger Internetanschluss des ISP 1&1. Der VDSL-Anschluss unterstützt DualStack<sup>18</sup>.

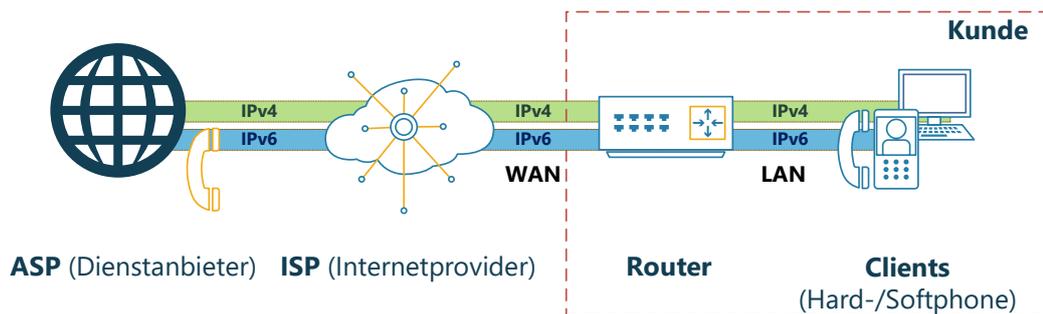


Abbildung 14: Grobeinteilung Komponenten Versuchsnetzwerk

Nach der Einrichtung von IPv6 im eigenen Netzwerk gehen lokale Dienste sehr schnell zu nutzen. Die verbreiteten Betriebssysteme (Linux/Windows/Mac OS X) unterstützen seit vielen Jahren IPv6 und haben das Protokoll bereits im Auslieferungszustand aktiviert. Wer im LAN hauptsächlich mit DNS-Namen arbeitet, merkt unter Umständen nicht einmal, dass er auf die SMB-Freigabe seines Servers neuerdings per IPv6 zugreift. Auf der Konsole kann dies mit den entsprechenden Befehlen jederzeit geprüft werden.

```
Windows-IP-Konfiguration
Ethernet-Adapter Ethernet:

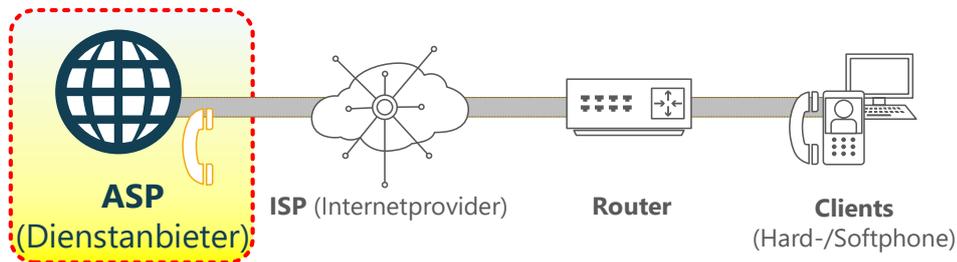
Verbindungsspezifisches DNS-Suffix: fritz.box
IPv6-Adresse . . . . . : 2003:d8:3eb:2900:9443:1eec:b7fe:3990
Temporäre IPv6-Adresse . . . . . : 2003:d8:3eb:2900:21b0:dbc3:b009:a145
Verbindungslokale IPv6-Adresse . . . . . : fe80::9443:1eec:b7fe:3990%2
IPv4-Adresse . . . . . : 192.168.128.154
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : fe80::e228:6dff:fed8:9471%2
                          192.168.128.254
```

Abbildung 15: "ipconfig"- ermittelte IP-Konfiguration eines Windows-PC

Die zugeordneten IP-Adressen waren routerabhängig. Eine manuelle Vergabe von IPv6-Adressen wurde nicht durchgeführt. Mittels eingerichteter Monitoring-Ports auf einem managbaren Switch und den freien Softwareprogrammen pcap und Wireshark konnten Paketmitschnitte des Datenverkehrs aufgezeichnet und ausgewertet werden.

<sup>18</sup> Vgl. Abschnitt 2.2.4 - DualStack-Verfahren

### 3.2 Diensteanbieter (ASP)



Diensteanbieter sind die Dienstleister, die über das IP-Protokoll Dienste zur Verfügung stellen, welche von den Clients genutzt werden können.

Dazu gehören im vorliegenden Fall eben die Internet Telephony Service Provider (**ITSP**). Aber Diensteanbieter können auch die Anbieter von Webseiten, Datenbanksystemen, Email-Provider u.v.m. sein.

Die Unterstützung eines Diensteanbieters für das IPv6-Protokoll liegt nicht in der Verantwortung des Nutzers. Der Anbieter selbst muss die Notwendigkeit von IPv6 einsehen und seine Dienste für IPv6 erreichbar gestalten. Im Folgenden wurden die grundlegendsten aller Dienste (die Webseitenbetreiber) und die im Kontext dieser Arbeit besonders relevanten Telefonieanbieter (ITSP) untersucht.

#### 3.2.1 Webseiten

Als Betreiber eines Webdienstes oder eines Webservers sollte man ein besonderes Interesse daran haben, seine Webseite auch über IPv6 erreichbar zu gestalten. Immerhin erhöht man dadurch die Erreichbarkeit des eigenen Produktes signifikant. Google beispielsweise veröffentlicht regelmäßig eine Statistik zum Aufruf der eigenen Webseiten über das jeweilige Protokoll [Goo18]. Demnach greift bereits weltweit der 5. Teil aller Benutzer auf Google mit dem neuen Protokoll zu. Abbildung 16 zeigt, dass die Tendenz deutlich steigend ausfällt.

Für die Bundesrepublik Deutschland verzeichnet der Suchmaschinenbetreiber sogar Werte von 36,27% (Stand: 04.01.2018) für den Zugriff auf Google-Webseiten per IPv6. Der vergleichsweise gute Wert liegt allerdings wohl kaum daran, dass viele Benutzer aktiv auf IPv6 umsteigen, sondern wohl eher daran, dass IPv6 immer häufiger wissentlich oder auch unwissentlich auf Routern und Clients aktiviert ist und damit parallel zu IPv4 bereits genutzt wird (Dual Stack). Zusätzlich wird, unbemerkt durch die Nutzer, in den moderneren

Mobilfunknetzen (LTE) bereits IPv6 eingesetzt – die meisten Smartphones nutzen also schon IPv6, wenn sie unterwegs die Suchmaschine nutzen.

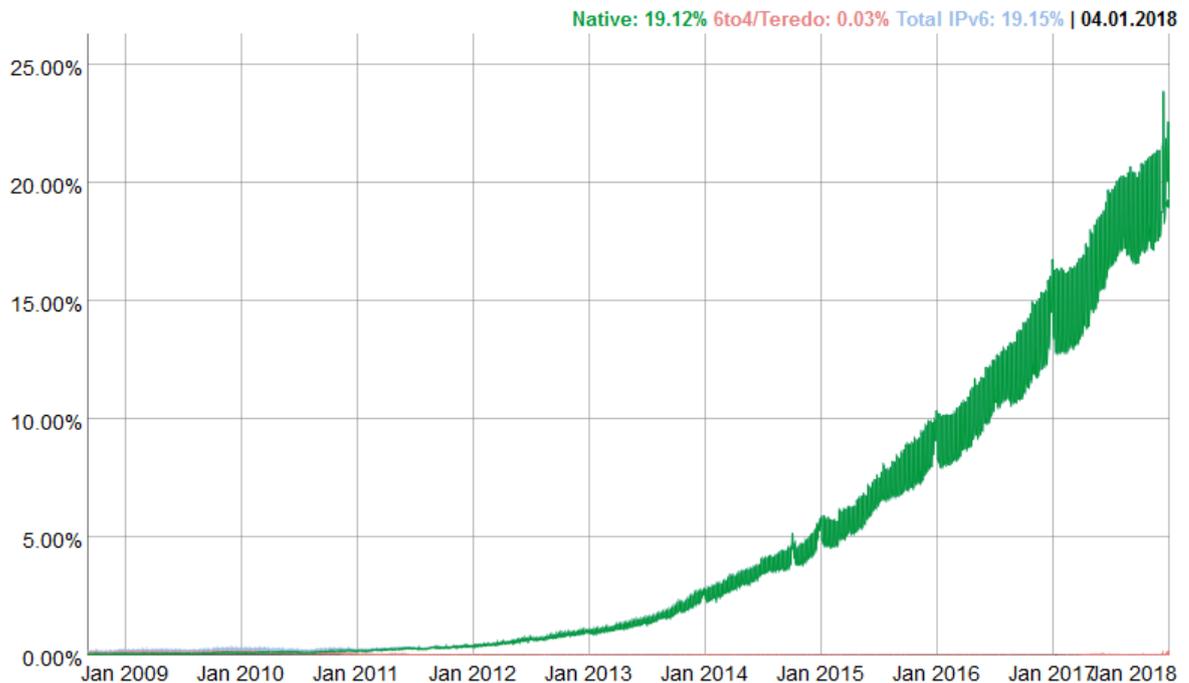


Abbildung 16: Google Inc (IPv6 Adoption) [Goo18]

Google hat also seine Hausaufgaben gemacht und stellt seine Dienste über IPv6 zur Verfügung – aber wie sieht es mit den anderen Anbietern aus? Das Amazon-Tochterunternehmen *Alexa Internet* sammelt Daten über die Aufrufe von Webseiten und veröffentlicht Listen über die am häufigsten aufgerufenen Seiten. [Ale17]

Beschränkt man sich auf eine Überprüfung der 50 in Deutschland am häufigsten besuchten Webseiten auf deren Erreichbarkeit über das IPv6-Protokoll, so stellt man fest, dass derzeit gerade einmal 16 von 50 Webseitenbetreibern reagiert und Ihre Webseiten für IPv6 freigeschaltet haben. Das ist ein ernüchternder Wert, bedeutet es doch, dass zum heutigen Tage eine ausschließliche Nutzung von IPv6 nicht zu empfehlen ist. Ohne die Verwendung von DualStack oder anderer Übergangstechnologien (z.Bsp. DS-Lite, NAT64, 6to4) [Hag11, 49ff] kann ein IPv6-only-Ansatz praktisch als „Selbstbeschneidung um etwa 2/3 des Internets“ bezeichnet werden. Der Ansatz ist aus heutiger Sicht nicht zu empfehlen! Die folgende Tabelle zeigt die Ergebnisse. Nur auf die Anbieter, bei denen im Feld IPv6-Status ein grün hinterlegtes „OK“ steht, konnte man mit IPv6 zugreifen.

Alexa Ranking DE/global	Webseite	IPv6-Status	Aufgelöste IPv6-Adresse
1/22	google.de	Ok!	2a00:1450:4007:816::2003
2/87	amazon.de	Fehler	Kein AAAA-Eintrag
3/116	ebay.de	Fehler	Kein AAAA-Eintrag
4/122	soundcloud.com	Fehler	Kein AAAA-Eintrag
5/287	youtube-mp3.org	Ok!	2400:cb00:2048:1::6814:5e79
6/288	web.de	Fehler	Kein AAAA-Eintrag
7/290	ebay-kleinanzeigen.de	Ok!	2a04:cb41:a516:4::11
8/312	gmx.net	Fehler	Kein AAAA-Eintrag
9/388	researchgate.net	Fehler	Kein AAAA-Eintrag
10/434	spiegel.de	Fehler	Kein AAAA-Eintrag
11/467	t-online.de	Ok!	2a02:cbf7:1:0:62:138:239:100
12/494	pixabay.com	Fehler	Kein AAAA-Eintrag
13/581	chip.de	Ok!	2a02:26f0:d4:187::bf0
14/604	mobile.de	Ok!	2a02:26f0:d4:189::1703
15/615	bild.de	Fehler	Kein AAAA-Eintrag
16/675	jimdo.com	Fehler	Kein AAAA-Eintrag
17/815	clipconverter.cc	Fehler	Kein AAAA-Eintrag
18/927	xing.com	Fehler	Kein AAAA-Eintrag
19/962	blogspot.de	Ok!	2a00:1450:4007:816::2009
20/985	focus.de	Ok!	2a02:26f0:d4:18a::d97
21/1000	welt.de	Ok!	2a02:26f0:d4:188::120a
22/1173	immobilienscout24.de	Fehler	Kein AAAA-Eintrag
23/1205	teamviewer.com	Fehler	Kein AAAA-Eintrag
24/1235	postbank.de	Fehler	Kein AAAA-Eintrag
25/1356	leo.org	Ok!	2400:cb00:2048:1::6814:3bd7
26/1367	telekom.com	Ok!	2a00:da8:ffff:fa01::11
27/1409	otto.de	Fehler	Kein AAAA-Eintrag
28/1435	heise.de	Ok!	2a02:2e0:3fe:1001:7777:772e:2:85
29/1532	gameforge.com	Fehler	Kein AAAA-Eintrag
30/1539	bahn.de	Fehler	Kein AAAA-Eintrag
31/1557	zeit.de	Fehler	Kein AAAA-Eintrag
32/1597	1und1.de	Ok!	2001:8d8:5ff:7::1:3
33/1621	dhl.de	Fehler	Kein AAAA-Eintrag
34/1643	idealo.de	Fehler	Kein AAAA-Eintrag
35/1686	thomann.de	Fehler	Kein AAAA-Eintrag
36/1737	deref-web-02.de	Fehler	Kein AAAA-Eintrag
37/1871	deutsche-bank.de	Fehler	Kein AAAA-Eintrag
38/1915	computerbild.de	Fehler	Kein AAAA-Eintrag
39/1991	dhl.com	Fehler	Kein AAAA-Eintrag
40/2033	linguee.de	Fehler	Kein AAAA-Eintrag
41/2069	avira.com	Ok!	2a01:138:a001:101:1::1
42/2099	autoscout24.de	Fehler	Kein AAAA-Eintrag
43/2189	agar.io	Ok!	2400:cb00:2048:1::6814:197a
44/2200	wetter.com	Fehler	Kein AAAA-Eintrag
45/2222	sueddeutsche.de	Ok!	2001:bc8:32d7:f300::1
46/2230	tagesschau.de	Fehler	Kein AAAA-Eintrag
47/2261	zdf.de	Fehler	Kein AAAA-Eintrag
48/2307	duden.de	Fehler	Kein AAAA-Eintrag
49/2322	kicker.de	Fehler	Kein AAAA-Eintrag
50/2363	commerzbank.de	Fehler	Kein AAAA-Eintrag

Tabelle 1: Ergebnis IPv6-Test Webseiten Top50 Deutschland

Etwas interessanter wird es noch, wenn man die Verfügbarkeit IPv6-fähiger Webseiten in einem zeitlichen Kontext sieht. Abbildung 17 zeigt deutlich, dass sich die Anzahl der IPv6-fähigen Webseiten in Deutschland unter den Alexa-TOP100 von 2012 (ca. 10 Seiten) bis heute (ca. 20 Seiten) gerademal verdoppelt hat. Zu wenig für schnelle Veränderungen.

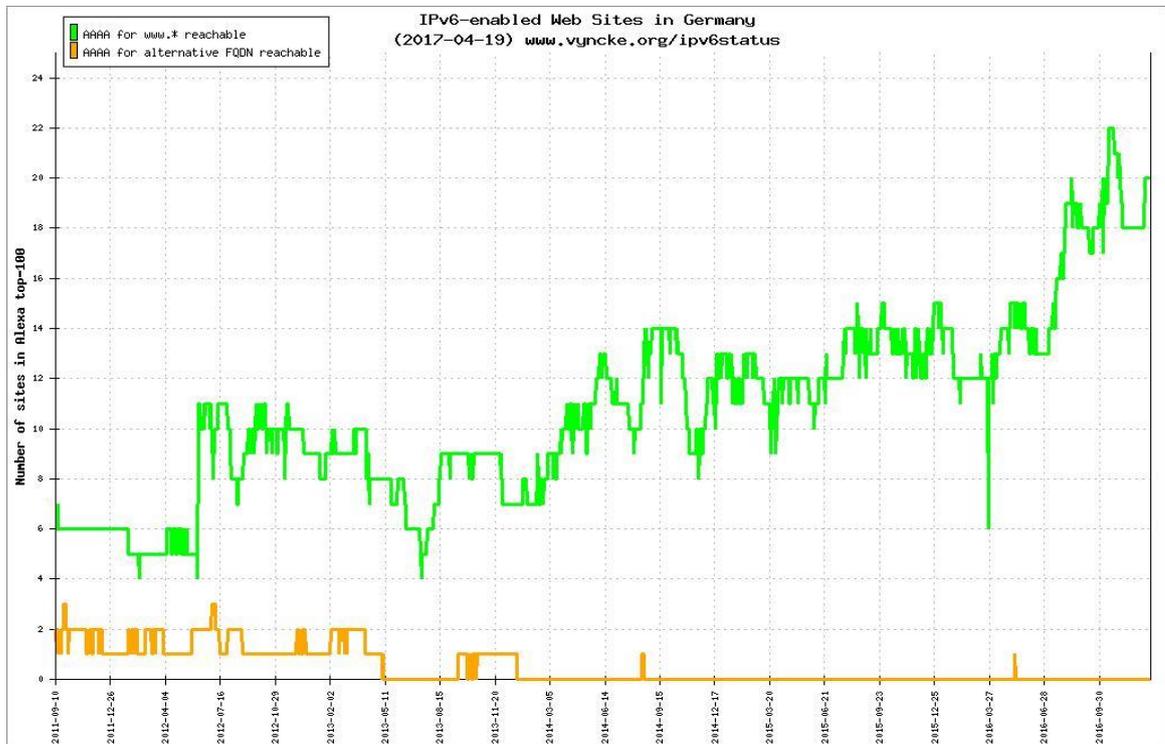


Abbildung 17: Vyncke 2017 - Statistik zu IPv6-fähigen Webseiten in Deutschland [Vyn17]

Die Diensteanbieter hängen den Internetnutzern in der Verwendung von IPv6 deutlich hinterher. Das fehlende Angebot IPv6-fähiger Dienste ist aktuell das größte Hemmnis für eine schnelle Durchsetzung von IPv6. Es wäre wirklich notwendig, dass die Diensteanbieter die IPv6-Unterstützung ebenso selbstverständlich (oder sogar bevorzugt) umsetzen, wie sie es heute mit IPv4 tun.

### 3.2.2 Internettelefonieanbieter (ITSP)

Um zu erkennen, welche Anbieter für Telefoniedienste in Frage kommen, wurde eine Marktrecherche durchgeführt. Das Ergebnis war eine überraschend große Menge an Dienstleistern am deutschen Markt, welche Internettelefoniedienste anbieten. Die hier beschriebenen Anbieter stellen nur eine Auswahl dar und pro Anbieter wurde auch nur das vielversprechendste Produkt überprüft.

Die Unterstützung für IPv6 ist von den Anbietern recht unterschiedlich realisiert – im Gegensatz zu den Betreibern wichtiger Webseiten/Webdienste ist die IPv6-Technologie bei den Telefonieanbietern jedoch schon deutlich stärker verbreitet.

Alle gelisteten Anbieter bieten ein Cloud-Telefonie-Produkt an, bei dem die Telefonanlage selbst sich beim ITSP befindet und der Kunde in seine SIP-fähige Telefonausstattung im Prinzip nur korrekte Zugangsdaten eingeben muss. Dieses Konzept wird häufig mit Bezeichnungen wie *Cloud-Anlage*, *Centrex-Anlage*, *Hosted PBX*, *NetPBX* beschrieben. (Siehe Abschnitt 2.3.2 - TK-System beim Carrier). Der Kunde bucht hier die fertige Nebenstelle.

Da durch die Verwendung des Internet-Protokolls der Standort der eigentlichen Telefonanlage (des Telefonieservers) jedoch variabel ist, gibt es auch andere realisierbare Konzepte. Besonders interessant für KMU könnte der Betrieb einer self-hosted-PBX sein. Näheres dazu im Abschnitt 4.3 - *Selfhosted PBX – die eigene, cloudbasierte IP-PBX*.

Die Tabelle erhebt keinen Anspruch auf Vollständigkeit, soll jedoch einen Eindruck dazu verschaffen, wie aktuell die Anbieter ihre Produkte gestalten.

Interessantes Detail: Internet-Service-Provider, die DS-Lite einsetzen und Ihre Anschluss-Produkte häufig als Kombination mit Telefoniediensten verkaufen, setzen als Telefonie-Server/-Gateway meist ein IPv4-Produkt ein, welches innerhalb des privaten IPv4-Bereichs steht (zwischen Endkunde und CGN-Router). Diese Systeme sind dann nur im Providernetz erreichbar.

Für die Versuche dieser Arbeit wurden easybell, placetel und sipgate.de als Testkandidaten für weitere Tests (siehe Abschnitt 3.5) ausgewählt, da hier relativ einfach und kostengünstig neue Produkte schaltbar waren. Außerdem war eine Unabhängigkeit des Telefonie-Produktes vom Internetanschluss realisierbar, was beispielsweise bei der Telekom nicht funktioniert.

VoIP-Provider	Produkt	Sip-Server	Ergebnis	Bemerkung
1und1/GMX		sip.gmx.net	negativ	Keine Unterstützung von IPv6
bellsip		proxy.bellsip.com	negativ	Keine Unterstützung von IPv6
blueSIP		bluesip.net	negativ	Keine Unterstützung von IPv6
callavista		sip.callavista.de	positiv	
congstar		tel.congstar.de	negativ	Keine Unterstützung von IPv6
dus.net		proxylv6.dus.net	positiv	
easybell		ipv6.sip.easybell.de	positiv	
ecalling		sip.ecalling.de	negativ	Keine Unterstützung von IPv6
einfachvoip.de		voip6.nexxtmobile.de	positiv	
placetel		sipv6.finotel.com	positiv	
QSC	IPfonie centraflex			IPv6 seit 2013 im Feldtest
sipbase		sip.sipbase.de	negativ	Keine Unterstützung von IPv6
sipgate.de		sipgate.de	positiv	
sipload		sip.sipload.com	negativ	Keine Unterstützung von IPv6
Telekom		tel.t-online.de	negativ	Keine Unterstützung von IPv6
vortel		sip.vortel.de	negativ	Keine Unterstützung von IPv6

Tabelle 2: Unterstützung von IPv6 durch ITSP

### 3.2.3 Das DNS-Problem bei den ITSP

Die getesteten Anbieter (sipgate, placetel, easybell) bieten SIP-Telefonie über das IPv6-Protokoll an. Während der über einen Paketmittelschnitt überwachten Verbindung wurden alle relevanten Pakete über SIP übertragen.

Jedoch war eine Abschaltung des IPv4-Stacks auf den Clients (bis auf 2 Ausnahmen) stets mit einem Verlust der Funktionalität verbunden.

Erklärung: SIP-Clients melden sich durch einen REGISTER bei ihrem zuständigen SIP-Registrar an und halten permanent eine Verbindung zu diesem offen (regelmäßiger REREGISTER). Dadurch weiß der Registrar immer, unter welcher Adresse er den Client erreichen kann. Meldet sich der Client nicht innerhalb eines eingestellten Intervalls wieder an, dann läuft die Registrierung ab und der Client ist für den Registrar abgemeldet.

Um die IP-Adresse (auch IPv6) des zuständigen Registrars zu ermitteln, verwenden die meisten Clients **SRV Resource Records** des **DNS**-Protokolls. Dieses Verfahren ist für SIP-Clients üblich und sogar empfohlen [RFC3263]. Der Client versucht dann nicht die vom Client vorgegebene Domain nach ihrem A- bzw. AAAA-Record aufzulösen und sich auf die entsprechende IP-Adresse zu verbinden, sondern er fragt den DNS-Server nach dem Ergebnis des SRV-Records für die Domain, z.Bsp. `_sip._udp.beispieldomain.tld`.

```
> _sip._udp.sipgate.de
Server: [8.8.8.8]
Address: 8.8.8.8

Nicht autorisierende Antwort:
_sip._udp.sipgate.de SRV service location:
  priority           = 0
  weight             = 0
  port                = 5060
  svr hostname       = sipgate.de
```

Abbildung 18: Abfrage des SRV-Records `_sip._udp.*` für die Domäne `sipgate.de`

Die DNS-Server geben bei allen getesteten Anbietern als Antwort einen CName, der jedoch in allen Fällen von den DNS-Clients nur über das IPv4-Protokoll weiter automatisch abgefragt wurde. War IPv4 aktiviert, dann konnte sogar die IPv6-Adresse des zust. Servers ermittelt werden. War IPv4 deaktiviert, scheiterte die weitere Namensauflösung gänzlich. Dadurch scheiterte demzufolge auch die Registrierung des SIP-Clients bei seinem zuständigen SIP-Registrar.

Fazit: *SIP-Telefonie über reine IPv6-Kommunikation ist zwar grundsätzlich möglich, aber die Anmeldung des Clients am SIP-Registrar erfordert regelmäßig eine IPv4-Verbindung.*

Lediglich der besonders rudimentäre Software-Client *miniSIPPhone* (verwendet SRV-Records überhaupt nicht) und das Hardware-Telefon *Grandstream GXP1450* (Servermethode auswählbar) heben sich von den anderen Sip-Clients ab und erlauben in unseren Versuchen eine IPv6-only-Konfiguration. Alle anderen Client-Tests mussten unter temporärer Zuschaltung des IPv4-Protokolls durchgeführt werden (siehe Abschnitt 3.5 - Clients).

### 3.2.4 Bewertung ASP

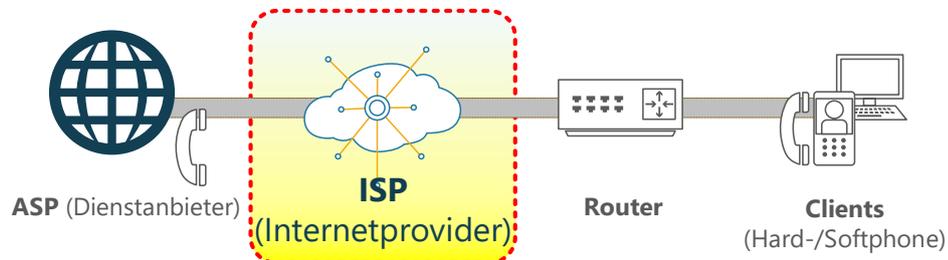
Die Diensteanbieter für Internetbasierte Dienste haben einen sehr hohen Nachholbedarf. Die Anzahl derer, die IPv6 noch nicht implementiert haben ist einfach zu hoch. Offenbar ist die Nachfrage der Konsumenten noch nicht ausreichend, als dass sich die Anbieter hier mit mehr Anstrengung bewegen.

Als Eisbrecher könnten sich moderne Technologien wie VoIP oder die Ausbreitung des Internet of Things erweisen. Diese ziehen klare Vorteile aus einem Internet ohne NAT und Adressmengenbegrenzung und werden somit zum Motor der Umstellung werden. Dies zeigt allein schon der Fakt, dass sich deutlich mehr ITSP mit IPv6 beschäftigt haben und dieses bereits unterstützen, als es die Webseitenbetreiber tun. Wer heute schon auf IPv4 verzichten möchte, kann einen großen Teil des Internets nichtmehr erreichen.

**Die Erfahrungen mit den Diensteanbietern schließen eine ausschließliche Verwendung von IPv6 (ohne IPv4) zur heutigen Zeit aus!**

### 3.3 Internet Service Provider (ISP)

Die Anzahl am Markt befindlicher ISP ist relativ hoch, jedoch gibt es nur wenige Provider, die im Bundesgebiet annähernd flächendeckend breitbandige Anschlüsse anbieten können.



#### 3.3.1 Prüfverfahren

Da es nicht möglich war, für die Vielzahl an Providern und Produkten jeweils eigene Anschlüsse zur Verfügung gestellt zu bekommen, wurden die wichtigsten Anbieter recherchiert und im Rahmen einer Befragung um Angaben zu den Leistungsmerkmalen ihrer Produkte befragt.

Anbieter die aktuell nicht geprüft werden konnten oder kein IPv6 unterstützen, wurden nicht aufgeführt. Die Ergebnisse beschränken sich auf Anbieter, die in irgendeiner Form bereits IPv6 implementiert haben. Sie erheben keinen Anspruch auf Vollständigkeit. Ebenfalls sind die Ergebnisse natürlich nicht dauerhaft. Sie spiegeln den Status zum Zeitpunkt der Niederschrift dieser Arbeit wieder.

Relevanz bei der Befragung/Recherche hatte natürlich die Frage, wie IPv6 implementiert wird. Hierbei unterscheiden sich die Anbieter in steter Regel nach solchen, die DS-Lite verwenden und jenen, die DualStack zur Verfügung stellen. Der wesentliche Unterschied ist die zugeteilte Art von IP-Adresse. Erhält man eine o. mehrere öffentlich geroutete IPv4-Adressen, so hat man einen DualStack-Anschluss und kann beide Protokolle uneingeschränkt nutzen.

Erhält man nur eine private IPv4-Adresse - entweder aus dem klassischen privaten IPv4-Adressbereich gemäß [RFC1918] oder aber aus dem für CGN reservierten Bereich nach [RFC6598] – so stellt der Anbieter DS-Lite zur Verfügung, die IPv4-Kommunikation ist dann nur eingeschränkt nutzbar.

Folgende Anbieter wurden angefragt:

Anbieter	Antwort	IPv6-Implementation?	Bemerkung
1&1	keine, jedoch Ermittlung am eigenen Anschluss	DualStack	/56 Präfix
cablesurf	Antwort per Mail, 15.9.2017, Verweis auf Schnittstellenbeschreibung	DS-Lite und DualStack, abh. Von Tarif	keine Aussagen zu Präfixgrößen
Colt	keine Antwort	unbekannt	
congstar	keine Antwort, Ermittlung an geschaltetem Anschluss, WWW-Angaben	keine (trotz Telekom/QSC als Vorleister)	keine Aussagen zu Planungen
Deutsche Glasfaser	Antwort per Mail, 19.9.2017	DS-Lite	/56 dyn. Präfix andere Produkte ü. Projektgeschäft
DNS-Net	keine Antwort	unbekannt	
easybell	keine Antwort, Ermittlung durch WWW-Recherche	keine	keine Planung
eazy	keine Antwort	unbekannt	
GMX	keine Antwort	unbekannt	
KEVAG-Telecom	keine Antwort, Ermittlung durch WWW-Recherche	keine	im Test, kein Realisierungsdatum
MDCC	Antwort per Mail, 18.9.2017	keine	geplant ab 2018
MDDSL	keine Antwort	unbekannt	
M-net	keine Antwort, Ermittlung durch WWW-Recherche	DS-Lite und DualStack	unterschiedlich für PK und GK
Netcologne	Antwort per Mail, 19.9.2017	DS-Lite und DualStack, abh. Von Tarif	/48 Präfix, fest nur für GK
primacom	Antwort per Mail, 15.09.2017, Verweis auf Schnittstellenbeschreibung	DS-Lite und DualStack, abh. Von Tarif	
QSC	Antwort per Mail, 25.09.2017	DualStack	/48 bis /24 Präfix (stat.) nur nach Beantragung
skyDSL	keine Antwort, Ermittlung durch WWW-Recherche	keine	
telecolumbus	Antwort per Mail, 15.09.2017, Verweis auf Schnittstellenbeschreibung	DS-Lite und DualStack	abh. von Tarif
Telefonica (O²)	keine Antwort, Ermittlung durch WWW-Recherche	keine	keine Planung
Telekom	Antwort per Mail, 15.09.2017	DualStack	/56.../48 Präfix
Unitymedia	keine Antwort, Ermittlung durch WWW-Recherche	DS-Lite	
versatel	keine Antwort, Recherche durch Kundenanfrage	DualStack	nur auf Anfrage, Projektgeschäft
vodafone	keine Antwort, Ermittlung durch WWW-Recherche	DS-Lite, auf Anfrage DualStack	je nach Produkt

Tabelle 3: Ermittlung IPv6-Implementierung div. ISP

Ebenfalls relevant ist die Anzahl der zugeordneten öffentlichen IPv6-Adressen (IPv4 interessiert uns diesbezüglich nicht mehr, die Probleme sind bekannt).

Die IETF empfahl bislang **grundsätzlich** die Zuordnung von **/48-Präfixen** egal wie groß der Kunde ist [RFC3177]. Eine sehr charmante Lösung, da ja genug Adressen vorhanden sind. Dies hätte eine besondere Einfachheit in der Verwaltung zur Folge gehabt, providerunabhängige Grenzen geschaffen und somit auch Vorgänge wie den Providerwechsel erleichtert.

Jedoch wurde diese Empfehlung 2011 (auf Wunsch der Carrier, die dies seit 2005 forderten) mit der [RFC6177] wieder aufgehoben. In der Literatur wird dennoch häufig entsprechend der [RFC3177] ein /48 Präfix für Kunden empfohlen (z.Bsp. [Hag09], [Hag14]) In der Regel erhält ein ISP einen /32-Bereich. Dieser allein entspricht mehr möglichen /64-Kundensubnetzen, als das ganze IPv4-Internet nutzbare Adressen besitzt.

### IPv6-Adresse (128bit):

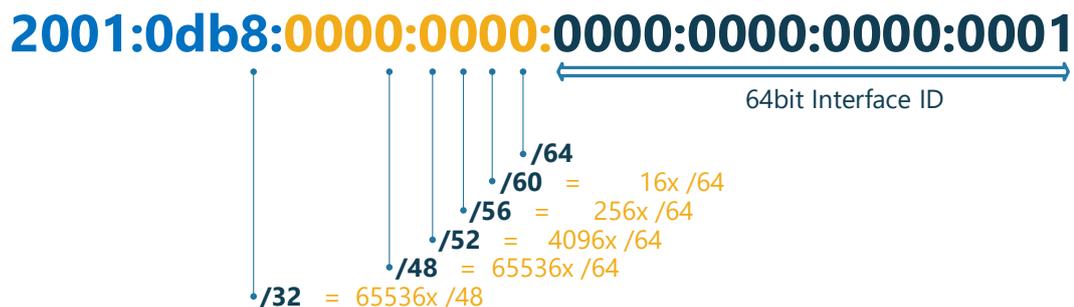


Abbildung 19: Auswirkung der Präfixgröße auf den Adressraum

Die kleingewerblichen Kunden erhalten allerdings i.d.R. keine /48 Präfixe, wie von der RFC empfohlen. Die von den Providern zugeordneten Adressräume variieren zwischen /56 bis /48. Das ist allerdings technisch unproblematisch, denn selbst mit einem /56 Präfix kann man im eigenen Netz noch 256 /64 Subnetze aufbauen oder (vorausgesetzt die HW unterstützt Prefix-Delegation<sup>19</sup>) 256 Router kaskadieren. Wer ein größeres Netz benötigt muss dies bei der Beschaffung seiner Produkte mit dem Provider klären. Alternativ ist auch die Bestellung eines providerunabhängigen Adressraums möglich. Dies ist für KMU und deren SOHO-Netzwerke jedoch kaum interessant.

Die 64bit der InterfaceID sind bei der Adressplanung unveränderbar (SLAAC).

<sup>19</sup> Prefix Delegation - [RFC3769]

### 3.3.2 Anbieter die DS-Lite verwenden

DS-Lite (Kurzform von **DualStack-Lite**) ist für viele Provider (allen voran die UnityMedia-Gruppe) eine wichtige Übergangstechnologie. Sie wurde in der Softwires Arbeitsgruppe der IETF entwickelt [RFC6333] und spielt hauptsächlich in den Breitband-Providernetzen eine signifikante Rolle [Hag09].

Gerade, wenn den Providern keine großen IPv4-Adressräume mehr zur Verfügung stehen, aber dennoch eine große Anzahl an Teilnehmern angebunden werden soll, wird diese Technologie eingesetzt.

Die Provider können die Infrastruktur zum Kunden bereits vollständig als IPv6-Netzwerk betreiben. IPv4-Daten werden jedoch vom Teilnehmer über IPv4-in-IPv6-Tunnel zu einem Carrier-Grade-NAT beim Provider übertragen. Dort teilen sich dann viele Teilnehmer die begrenzten IPv4-Adressen. Für die Provider hat dies zusätzlich den Vorteil, nur ein IPv6-Netzwerk unterhalten zu müssen.

The screenshot shows the 'FRITZ!Box 6490 Cable' web interface. At the top, it displays 'FRITZ!Box 6490 Cable' and 'FRITZ!OS: 06.63'. Below this, there are two main sections: 'Verbindungen' (Connections) and 'Anschlüsse' (Ports). Under 'Verbindungen', it lists 'Internet' (IPv4, FRITZ!Box verwendet einen DS-Lite-Tunnel IPv4 über DS-Lite), 'Internet' (IPv6, verbunden seit 29.10.2016, 15:17 Uhr, IPv6-Adresse: 2a02:908:2e00:2:10f:37e9:d2b6:82fe), and 'Telefonie' (1 Rufnummer aktiv, davon keine registriert). Under 'Anschlüsse', it lists 'Kabel' (verbunden, 135.2 Mbit/s / 6.3 Mbit/s), 'LAN' (verbunden (LAN 1)), 'WLAN' (an, Funknetz 2,4 GHz: FRITZ!Box 6490 Cable), 'WLAN' (an, Funknetz 5 GHz: FRITZ!Box 6490 Cable), 'DECT' (aus), and 'USB' (kein Gerät angeschlossen).

Abbildung 20: Web-Oberfläche eines AVM-Routers an einem Kabelanschluss mit DS-Lite

### Prüfergebnisse

ISP	Produkt	Bemerkung
KabelDeutschland (Vodafone)	Internet & Phone (Kabel), LTE-Zuhause	Standard: DS-Lite, Präfix /62 Produkt kann jedoch auf Anfrage beim ISP auf DualStack umgestellt werden!
KabelBW	Kabel	DS-Lite, Präfix /56
UnityMedia	Kabel	DS-Lite, Präfix /56
M-Net	DSL/VDSL	DS-Lite, Präfix /56
T-Mobile	Mobilfunk (LTE)	DS-Lite (priv. IPv4-Addr. Und öfftl. IPv6-Addr.)

Tabelle 4: ISP mit DS-Lite Implementation

Die Verwendung von DS-Lite bei den Mobilfunkbetreibern ist im Vergleich zu den zu den Kabel- oder DSL-Anbietern kein Rückschritt, da Mobilfunk schon immer private IPv4-Adressen in Verbindung mit einem Carrier-Grade-NAT eingesetzt hat. Jetzt kommen im LTE-Netz öffentliche IPv6-Adressen hinzu. Leider verhindern einige Provider dennoch häufig bestimmten Traffic durch Einsatz großer Firewallsysteme, die bspw. SIP unterdrücken.

### Probleme mit DS-Lite

DS-Lite bringt aber auch einige Probleme für die Anwender. Dies betrifft vor allem IPv4-basierte Dienste, die einen Zugriff von extern benötigen. Da der NAT-Router für IPv4 beim Carrier steht, hat der Nutzer keinerlei Möglichkeiten, Portforwardings einzustellen.

Alle Dienste, die eine öffentliche IP-Adresse benötigen, wie z.Bsp.:

- Fernwartung auf Computer mit VNC oder RDP oder ssh
- Fernkonfiguration von Alarmanlagen
- Lokale NAS mit FTP-, Web-, SMB-, und/oder anderen Diensten
- IP-Videokameras...

...und die (noch) keine Unterstützung für IPv6 bieten, können hier nicht direkt angebunden werden.

Zwar gibt es auch dafür Technologien, diese kosten aber häufig zusätzlich Geld, oder stellen zwischenzeitlich sogar den Dienst ein (wie der Tunnelanbieter SixXS [Ziv17]).

### 3.3.3 Anbieter die DualStack implementiert haben

Die zukunftssicherere und sorgenfreiere Variante für die Kunden ist sicherlich eine providerseitige Implementierung von IPv6 mittels DualStack [RFC4213]. Viele Anbieter haben bereits den Schritt getan und auf diese Weise IPv6 ohne große Aufregung bei den Kunden zur Verfügung gestellt [SB16].[RFC4213]

The screenshot shows the 'Übersicht' (Overview) page of a Fritz!Box 7490. It displays the model name, current energy consumption (26%), and the Fritz!OS version (06.83). The page is divided into two main sections: 'Verbindungen' (Connections) and 'Anschlüsse' (Ports/Connections).

Verbindungen		Anschlüsse	
Internet	IPv4, verbunden seit 06.09.2017, 02:29 Uhr Anbieter: I&I Internet IPv4-Adresse: 84.176.60.238 reale Bandbreite: ↓ 51,4 Mbit/s ↑ 10,0 Mbit/s	DSL	verbunden ↓ 51,4 Mbit/s ↑ 10,0 Mbit/s
Internet	IPv6, verbunden seit 06.09.2017, 02:29 Uhr Anbieter: I&I Internet IPv6-Adresse: 2003:d8:3bf:271:e228:6dff:fed8:9475 reale Bandbreite: ↓ 51,4 Mbit/s ↑ 10,0 Mbit/s	LAN	verbunden (LAN 1, LAN 2, LAN 3)
Telefonie	11 Rufnummern aktiv	WLAN	aus, Funknetz 2,4 GHz: fn6-fb
		WLAN	aus, Funknetz 5 GHz: fn6-5g-fb
		DECT	an, ein Schnurlostelefon angemeldet
		USB	verbunden, 1 Speicher (entfernen)

Abbildung 21: Web-Oberfläche eines AVM-Routers am VDSL-Anschluss mit DualStack

**Prüfergebnisse**

ISP	Produkt	Bemerkung
Telekom DSL (VDSL)	Magenta S/M/L/XL	DualStack, Präfix /56
1und1	DSL/VDSL	DualStack, Präfix /56, bei ADSL können ggf. andere Vorleister ohne IPv6 zum Einsatz kommen
congstar	DSL/VDSL	DualStack, Präfix /56
M-Net	Business DSL/VDSL	DualStack, Präfix /48 nur für Geschäftskunden
Netcologne		DualStack, Präfix /48 nur für Geschäftskunden
Telecolumbus		DualStack, Präfix ?, nur auf Anfrage/Neukunden
Telefonica/O2	Privatprodukte	DualStack, jedoch nur Neukunden
Telefonica/O2	Businessprodukte	DualStack, jedoch nur auf indiv. Projektbasis

Tabelle 5: ISP mit DualStack Implementation

DualStack-Anschlüsse sind, solange IPv4 noch eine signifikante Rolle spielt, die sinnvollste Realisierung für Anschlüsse. Die Technologie ermöglicht weiterhin die uneingeschränkte Nutzung hergebrachter IPv4-Dienste und ermöglicht gleichzeitig die Nutzung moderner IPv6-Dienste.

Viele Provider setzen, analog zur klassischen dynamisch vergebenen IPv4-Adresse, auch weiterhin auf wechselnde Präfixe und fordern User zur Nutzung der Privacy-Option auf<sup>20</sup>.

**3.3.4 feste/dynamische Präfixe**

Wer von seinem Provider ein festes IPv6-Präfix erhält, muss sich um eine Umadressierung seiner Clients keine Gedanken machen. Kunden, die von Ihrem Provider ein dynamisches Präfix erhalten jedoch schon. Auch in der IPv6-Welt werden von den meisten Providern tatsächlich noch dynamische Präfixe verteilt. Einerseits wird dadurch ein Schutz vor zugeordneten, aber ungenutzten Adressleichen aufgebaut, andererseits entspricht das Verfahren dem Wunsch vieler Kunden nach Privatsphäre und Verschleierung.

<sup>20</sup> Die Privacy-Option ist ein Verfahren gem. [RFC4941] bei dem die 64bit Interface-ID der IPv6-Adresse nicht direkt nachvollziehbar aus der MAC-Adresse abgeleitet wird. Durch dieses Verfahren wird ein Host mit unterschiedlichen IPv6-Adressen nichtmehr so leicht identifizierbar für Dritte. Die Interface-ID sieht bei diesem Verfahren für jede erzeugte IPv6-Adresse komplett anders aus.

Bei der Änderung des Präfixes nutzt man die Eigenschaft, dass unter IPv6 ein Host ohnehin zumeist mehrere IP-Adressen besitzt. Somit kann er auch gleichzeitig mehrere globale IPv6-Unicast-Adressen besitzen. Durch ein Router-Advertisement-Paket wird allen Hosts das neue Präfix mitgeteilt<sup>21</sup>. Sie behalten aber bis zum Ablauf der TTL (Angabe im Router-Advertisement) die alte IPv6-Adresse weiterhin bei und sind unter dieser erreichbar.

```
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2003:d8:3ed:d600:9443:1eec:b7fe:3990(Bevorzugt)
Temporäre IPv6-Adresse. . . . . : 2003:d8:3ed:d600:c103:bcd5:adad:d8b5(Bevorzugt)
Verbindungslokale IPv6-Adresse . . : fe80::9443:1eec:b7fe:3990%3(Bevorzugt)
```

Abbildung 22: ipconfig-Ausdruck eines Hosts vor der Umnummerierung

```
Autokonfiguration aktiviert . . . : Ja
IPv6-Adresse. . . . . : 2003:d8:3f4:dd00:9443:1eec:b7fe:3990(Bevorzugt)
IPv6-Adresse. . . . . : 2003:d8:3ed:d600:9443:1eec:b7fe:3990(Verworfen)
Temporäre IPv6-Adresse. . . . . : 2003:d8:3ed:d600:c103:bcd5:adad:d8b5(Verworfen)
Temporäre IPv6-Adresse. . . . . : 2003:d8:3f4:dd00:c103:bcd5:adad:d8b5(Bevorzugt)
IPv6-Adresse. . . . . : fd00::9443:1eec:b7fe:3990(Verworfen)
Temporäre IPv6-Adresse. . . . . : fd00::c103:bcd5:adad:d8b5(Verworfen)
Verbindungslokale IPv6-Adresse . . : fe80::9443:1eec:b7fe:3990%3(Bevorzugt)
```

Abbildung 23: ipconfig-Ausdruck eines Hosts nach der Umnummerierung

Die neue IP wird fortan für alle neuen Verbindungen verwendet (auch für den REGISTER-Vorgang beim SIP-Registrierer). Bestehende Verbindungen können jedoch weiterhin die alte IP-Adresse verwenden. Somit reißt der Audio-Datenstrom eines bestehenden VoIP-Gesprächs durch einen Präfixwechsel nicht ab, die Nutzer können unterbrechungslos zu Ende telefonieren. Ist die Anwendungssoftware ordentlich programmiert, so bemerkt der Nutzer den Präfixwechsel nicht.

Im Rahmen dieser Arbeit wurde die Fortführung eines Gespräches über die Umnummerierung hinweg auf den Systemen getestet, die bereits IPv6-only-Kommunikation unterstützten (miniSIPClient, Grandstream GXP1450). Die Ergebnisse waren, wie erwartet, positiv.

### 3.3.5 Bewertung ISP

Die Internetanbieter haben den Bedarf für IPv6 bereits früh erkannt.

Fast jeder Anbieter stellt mittlerweile auch IPv6 zur Verfügung. Einige verwenden sogar bereits vorrangig IPv6 und setzen IPv4 nur noch mithilfe von CGN an DS-Lite-Anschlüssen um. Nun, sie waren vielleicht auch aufgrund der Adressknappheit zum Handeln gezwungen.

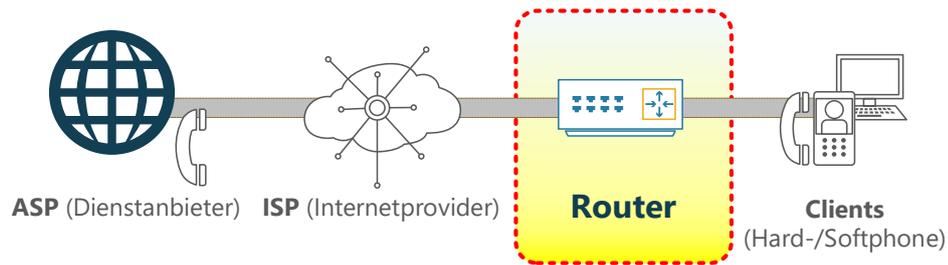
<sup>21</sup> Das Verfahren heißt Router-Renumbering und ist in [RFC2894] festgelegt.

Die Anzahl derer, die IPv6 noch nicht implementiert haben ist überschaubar, und zumindest haben diese Provider bereits die Anforderung erkannt und die Einführung von IPv6 auf ihre Agenden gesetzt.

Ausschließlich IPv6 am Anschluss ist derzeit für keinen Anbieter ein Thema.

**Die Internetanbieter stellen somit keine größere Hürde für die Einführung von IPv6 dar. Wer IPv6 als Kunde nutzen möchte, der findet auch einen ISP der ihm dies zur Verfügung stellt.**

### 3.4 Router



Der Router spielt in einem SOHO-Netzwerk eine besonders zentrale Rolle.

Als zentrales Netzwerkgerät an der Schnittstelle zwischen Kundennetzwerk und ISP ist er zuständig für die Internetanbindung (WAN) und Verwaltung des kundeneigenen Netzwerksegments (LAN). Router erfüllen allerdings auch viele weitere Aufgaben. Sie sind oft Firewall, Telefonanlage, NAS-System u.v.m. – daher gibt es sie auch in unzähligen Varianten und Formen (sogar virtuelle Router sind gang und gäbe).

Für die kleingewerbliche Nutzung bieten sich hardwarebasierte Routersysteme an, die nicht nur den Router enthalten, sondern auch gleichzeitig das LAN verwalten (DNS, DHCP), sowie Modem, WLAN- und Telefoneschnittstellen bereitstellen. Diese All-In-One-Router werden von den meisten Kunden direkt vom Internetanbieter bezogen, der diese auswählt und auch für den Kunden bereits möglichst betriebsfertig konfiguriert ausliefert. (Im Enterprise-Segment werden solche Geräte eher seltener eingesetzt, dort teilt man die Dienste auf.)

Für unsere Untersuchung ist die Unterstützung des IPv6-Protokolls von zentraler Bedeutung. Die am Markt erhältlichen Systeme unterscheiden sich dabei nicht nur von Hersteller zu Hersteller, sondern mittlerweile auch deutlich innerhalb verschiedener Firmwarestände.

Im privaten und im kleingewerblichen Bereich spielt der Hersteller AVM mit seiner Fritz!Box-Modellreihe in Deutschland die größte Rolle. Er stellt deutlich über 50% aller Router in diesem Segment. Die folgende Grafik zeigt zwar die Marktverteilung aus dem Jahre 2010, der Anteil des Herstellers AVM ist seitdem allerdings ähnlich geblieben. Daher setzen auch wir in unserem Testnetzwerk vorrangig eine AVM Fritz!Box ein. Aber wir prüfen auch Alternativen.

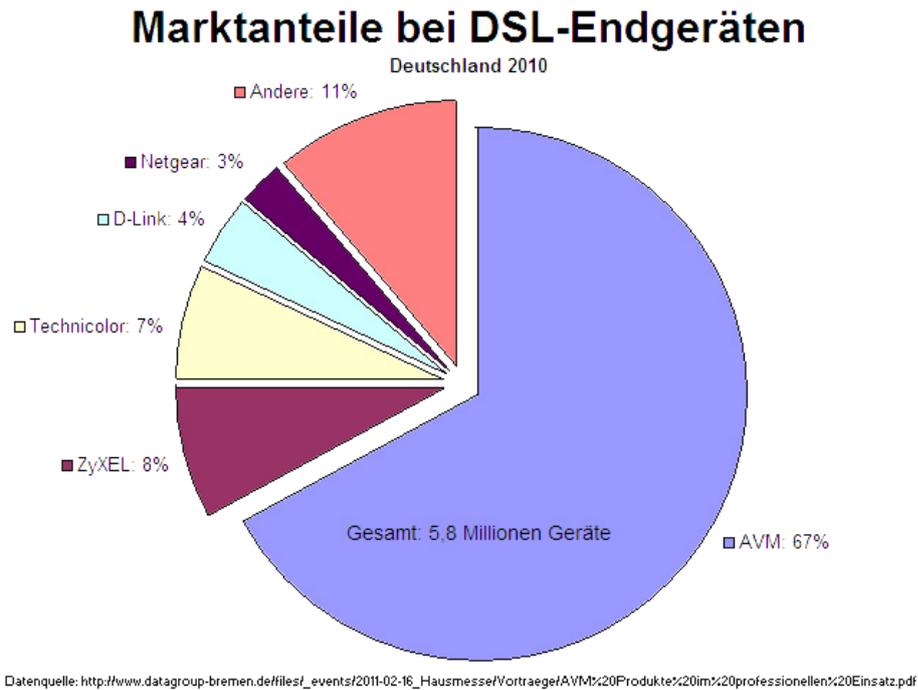


Abbildung 24: Marktanteile Router in Deutschland

### 3.4.1 Prüfverfahren

Die Router müssen nicht nur Standardaufgaben unter IPv4 meistern, der Hauptaugenmerk liegt auf dem Umgang mit dem IPv6-Protokoll und den zur Verfügung gestellten Funktionen.

Getrennt wird dabei nach Funktionen als IPv6-Client (WAN), und Funktionen als IPv6-Server (LAN).

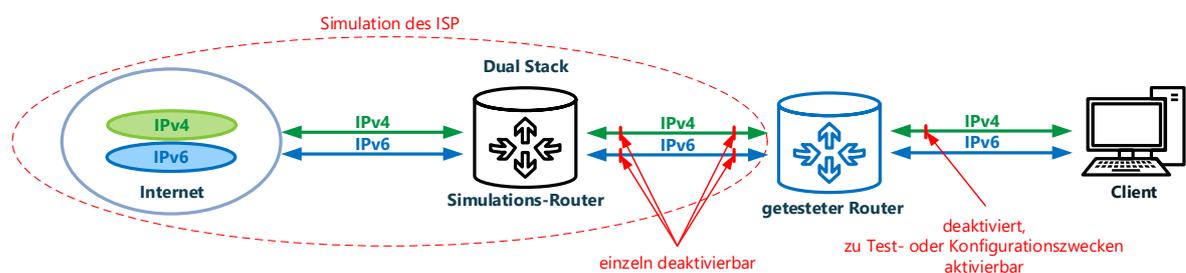


Abbildung 25: schematische Darstellung der Routertests

Interessante Fragen, auf die die Geräte getestet wurden:

- Werksseitige Auslieferung (Ist IPv6 bereits im Auslieferungszustand aktiviert?)
- Konfigurierbarkeit über IPv6 (erreiche ich alle Einstellungen, ohne IPv4 nutzen zu müssen?)
- Erhalt weitergegebener Präfixe (kann ich vom ISP erhaltene Präfixe weiterverteilen und damit ggf. Router kaskadieren?)

- SLAAC/DHCPv6? Wie kommen Netzwerkgeräte zu ihren IPv6-Adressen?
- ULA-Zuweisung (parametrierbar, in Abhängigkeit von Internetkonnektivität?)
- Umgang mit Portweiterleitungen/Firewallregeln
- Funktioniert VoIP-Telefonie unproblematisch?
- Inwiefern funktionieren typ. Router-Funktionen i.V.m. IPv6 (DynDNS, NTP, VPN)

### 3.4.2 Getestete Router

#### ASUS DSL-AC68U

Der taiwanische Hersteller ASUSTek Computer Inc. stellt seit 1989 neben Netzwerkprodukten auch Computer, Mobiltelefone, Bildschirme und viele andere



Abbildung 26: ASUS DSL-AC68U

Elektronikprodukte her. Im Portfolio befinden sich Router, die sich vor allem an Heimanwender richten und mit besonders guten WLAN-Eigenschaften und Verbindungsgeschwindigkeiten werben. Das hier getestete Modell DSL-AC68U ist ein Mittelklasse-VDSL-Router, d.h. er hat ein VDSL-Modem bereits an Bord. Es kann jedoch auch über Ethernet1 oder über einen 3G/4G-Mobilfunkstick mit dem Internet verbunden werden, der Hersteller wirbt sogar mit FallBack-Funktionalität. Für den Test wurde das Gerät auf die neueste Firmware. Version 3.0.0.4.380.7712

vom 11.Aug. 2017 aktualisiert – ASUS bringt vergleichsweise häufig Updates für die Geräteserie heraus.

Bei der ersten Inbetriebnahme jedoch geht der Hersteller davon aus, dass das Gerät an einem DSL/VDSL-Anschluss betrieben wird, der Einrichtungsassistent ist schnell über den DNS-Namen <http://router.asus.com> erreichbar, lässt sich aber nur mit Fehlermeldungen von den möglichen anderen Uplink-Varianten überzeugen.

Nach Beendigung des Einrichtungsassistenten steht zunächst ausschließlich IPv4 zur Verfügung. Sämtliche gewünschten IPv6-Einstellungen (auch die Konfiguration einer IPv6-Adresse auf der WAN-Schnittstelle) sind nicht konfiguriert, der Router wird als reiner IPv4-Router vom Hersteller verstanden. In der Konfigurationsoberfläche existiert genau ein Menü „IPv6“ mit genau einem Schalter, mit dem die Unterstützung zugeschaltet werden kann. Mit diesem Schalter kann man aus einer kleinen Anzahl von IPv6-Szenarien wählen, die der Hersteller definiert hat. Wirklich Einfluss auf die IPv6-Konfiguration hat man damit nicht, aber zumindest sind Standard-Szenarien möglich. Eine Konfiguration ohne IPv4 ist

gänzlich unmöglich – die Konfigurationsoberfläche ist nur mittels IPv4 erreichbar und reagiert auf IPv6-Anfragen nicht. IPv4 lässt sich am Gerät auch nur durch Deaktivierung des DHCPv4-Servers reduzieren. Die Optionen in Verbindung mit der IPv6-Aktivierung sind versteckt, und werden erst angezeigt, wenn man die passenden Optionen des ASUS-Szenarios gewählt hat. Die Benennung von Konfigurationsoptionen ist teilweise irreführend. Man muss erst „automatisch mit DNS-Server verbinden“ deaktivieren, bevor man entsprechende Optionen sieht, mit denen der zu verteilende DNS-Server spezifiziert werden kann. Die Konfiguration erfordert Experimentierfreude. Dann jedoch gehen die Möglichkeiten sogar soweit, dass der Nutzer entscheiden darf, ob ein Präfix übernommen werden soll, oder ob ein eigener, selbstdefinierter ULA-Präfix verwendet wird. Zusätzlich darf noch die Adress-Zuweisungsmethode (stateless/stateful) gewählt werden, bei der sogar die InterfaceID-Nummerierung durch den DHCPv6 erfolgen könnte. Im praktischen Versuch hat diese Methode jedoch weder für Windows-, noch für Linux-PC's funktioniert. Eine IPv6-Firewall ist ebenfalls an Bord. Im Grundzustand wird jeder Traffic nach außen erlaubt, genauso wie daraufhin eingehender Traffic (entsprechend einem NAT-Verhalten). Weitere Freigaben müssen händisch eingetragen werden, wobei der Hersteller die Einrichtung von Freigaben nur für feste IPv6-Adressen erlaubt. Die Übernahme eines dynamischen externen Präfixes für die Anlage von Firewallregeln ist nicht möglich. Eine Zuordnung von MAC-Adressen zu IPv6-Adressen bekannter Hosts macht der Router nicht. Ebenso fehlt leider eine Übersicht erkannter IPv6-Geräte. Für IPv4 existiert diese Übersicht und kann sogar zum Erstellen von Firewallregeln verwendet werden – klarer Nachholbedarf des Herstellers bei der Implementierung des neuen IP-Stacks in der eigenen Firmware.

Zur Einrichtung von VPN-Verbindungen ist ein VPN-Gateway-Dienst aktivierbar. Dem Dienst fehlt jedoch die Unterstützung für das IPv6-Protokoll. Ein aus dem Internet gesendetes IPSec-Proposal-Paket an seine IPv6-Adresse wurde im Gegensatz zu IPv4 nicht beantwortet.

Die Telefonie durch den Router hindurch mittels IPv6-Telefon funktioniert von Anfang an problemlos, die für die Kommunikation benötigten Ports werden von der Firewall selbständig geöffnet. Das Mediastreaming funktioniert problemfrei. Eigene VoIP-Features wie ein lok. SIP-Gateway bietet der Router jedoch nicht an.

Für einen Preis ab 150€ gehört der Router sicherlich nichtmehr der Einstiegsklasse an, aber er verbindet leistungsfähige Hardware mit ausbaufähiger Firmware. Nutzer, die IPv6 in einer Dualstack-Umgebung einsetzen möchten, können dies mit dem Gerät bereits tun.

Die häufige Veröffentlichung neuer Firmware des Herstellers lässt auf Verbesserungen bei den Schwachstellen in der Konfiguration hoffen.

### TP-Link Archer C59 AC1350

Der chinesische Hersteller TP-Link bedient seit 1996 den Markt mit günstigen



Netzwerkkomponenten. Seine Heimrouter-Serie zeichnet sich durch ein abwechslungsreiches Portfolio verschiedenster Modelle mit jeweils ähnlichen Software-Ständen aus. Die Geräte sind im Vergleich sehr günstig, wir testen ein Einstiegsmodell der aktuellen Serie, den Archer C59. Das Gerät ist ein reiner Router, ohne DSL- oder Kabelmodem und ohne

Abbildung 27: TP-Link Archer C59

Telefonieschnittstellen, wie dies tlw. bei den größeren Modellen zu finden ist. Ebenfalls hat der Router nicht

die schnellsten WLAN-Schnittstellen – dafür ist er aber bereits zum Preis von etwa 40€ erhältlich. Der Funktionsumfang in Bezug auf Unterstützung des IPv6-Protokolls ist laut Herstellerangaben derselbe, wie bei den größeren Modellen. Das Gerät wurde mit der Firmware 1.0.2 vom 25.7.2016 getestet, welche die aktuellste verfügbare Version darstellt. Im Auslieferungszustand sind IPv6 sowohl im LAN, als auch im WAN aktiviert. Für die WAN-Schnittstelle muss jedoch der Typ (dyn./stat./DHCP/SLAAC/usw.) noch selbst angepasst werden. Im LAN ist IPv6 als automatische Konfiguration (SLAAC + stateless DHCPv6) aktiviert. Ein angeschlossener Client könnte somit von Anbeginn an mit dem Router per IPv6 kommunizieren. Lediglich die erstmalige Ermittlung der IPv6-Adresse (ULA) des Routers würde eine Schwierigkeit darstellen, denn das Gerät weist als DNS-Server seine eigene IPv4-Adresse zu und der vom Hersteller eingerichtete Kurzname *tplinkwifi.net* – der hinter jedem TP-Link-Router auf den Router selbst verweisen soll, dieser Kurzname liefert keine IPv6-Adresse zurück, sondern nur den IPv4-Wert. Hat man nun (z.Bsp. mittels Wireshark) die Adresse herausgefunden, könnte man theoretisch von Anfang an das Gerät über IPv6 konfigurieren, jedoch: Der Router stellt das Webinterface über IPv6 nicht zur Verfügung. Das ist insofern wirklich schade, weil der TP-Link im Gegensatz zu den meisten anderen Routern im Testfeld sehr gut einstellbar ist!

Der Router verfügt über einen eigenen DHCPv6-Server, der sowohl eigene ULA- aber auch öffentliche Unicast-Adressen anhand delegierter Präfixe zuordnen kann. Ebenfalls ist die Konfiguration verteilter DNS-Server möglich. Wer den DHCPv6 nicht benötigt kann ihn auch abstellen und beispielsweise auf SLAAC vertrauen (und ggf. mit Router-Advertisements

ergänzen). Sogar die Lease-Time ist anpassbar. Der interne DHCPv4-Server kann abgeschaltet werden, die IPv4-Adresse auf der eigenen LAN-Schnittstelle bleibt jedoch erhalten. Da die Konfiguration ausschließlich über IPv4 möglich ist, ist das natürlich auch sinnvoll.

Das Gerät unterstützt DDNS-Dienste, aktualisiert dort jedoch nur eine IPv4-Adresse.

Eine IPv6-Firewall lässt das Gerät leider vermissen. Ein VPN-Gateway-Dienst ist aktivierbar, jedoch fehlt die Unterstützung für IPv6 vollständig. Das Gerät reagierte bereits auf das IPSec-Proposal-Paket an seine IPv6-Adresse nicht.

Die Verbindung des Telefons über IPv6 durch den Router hindurch funktionierte auf Anhieb tadellos (Registrierung sowie eingehende und ausgehende Gespräche, auch bei deaktiviertem IPv4-Stack am Telefon).

Zusammengefasst lässt sich sagen, dass der Router durchaus gut vorbereitet auf Nutzer ist, die in Ihrem Netz IPv6 kontrolliert einsetzen möchten, die kleinen Schwachpunkte der fehlenden konfigurierbaren Firewall sowie des über IPv6 erreichbaren Webinterface sind in Dualstack-Umgebungen tolerierbar. Sehr gutes Preis-Leistungsverhältnis.

#### **Cisco/Linksys E2500**

Der bis 2013 noch zu Cisco, nunmehr zu Belkin gehörende amerikanische Hersteller Linksys stellt seit 1988 Netzwerkkomponenten her. Bekannt und verbreitet wurde er durch den Verkauf von preisgünstigen Routern und Netzwerkkarten, die sich mit der Einführung von Windows 95 und dessen integrierten Netzwerkfunktionen einer erhöhten Nachfrage erfreuen durften.



Abbildung 28: Linksys E2500

Das Modell E2500 wird in der aktuellen Produktlinie als Einstiegsmodell positioniert und ist daher relativ günstig. Mit einem Preis von ca. 50€ ist es der günstigste Router unter den getesteten. Er benötigt ein zusätzliches (Kabel-/VDSL-) Modem, denn er verfügt nur über eine normale Ethernet-WAN-Schnittstelle. Der Router wurde auf Firmwareversion 3.0.02 vom 16.06.2016 aktualisiert, welches die nach

Herstellerangaben neueste Firmware ist. Laut Hersteller wird IPv6 unterstützt.

Im Test zeigt der Router in Bezug auf IPv6 jedoch deutliche Schwächen. Die Unterstützung von IPv6 auf der WAN-Schnittstelle ist nur grundsätzlich aktivier- oder deaktivierbar. Im Auslieferungszustand ist sie sogar aus. Alternativ kann statt der

Freischaltung von IPv6 für die WAN-Schnittstelle auch ein Tunneladapter eingerichtet werden, was in unserem Anwendungsszenario keinen Sinn macht.

Damit hat sich dann aber die Einstellbarkeit schon fast erledigt. Lediglich die IPv6-Firewall kann noch aktiviert/deaktiviert und mit Freigaben parametrisiert werden. Die Freigaben der IPv6-Firewall sind nur durch eine feste Zuordnung von IPv6-Adresse/Portnummern des Zielrechners in der Firewallregel möglich. Eine Nutzbarkeit in Verbindung mit dynamischen Präfixen (wie im SOHO-Bereich zumeist anzutreffen) ist ausgeschlossen. Der DDNS-Dienst registriert nur die IPv4-Adresse beim DDNS-Anbieter.

Schön ist, dass sofort nach Aktivierung von IPv6 auf der WAN-Schnittstelle auch die Administrationsoberfläche des Systems per IPv6 steuerbar ist. Der IPv4-Stack kann grundsätzlich nicht deaktiviert werden. Ein IPv6-only-Szenario ist daher ebenfalls ausgeschlossen. Eine DHCPv6- oder eine DNSv6-Funktion sucht man vergeblich. VoIP-Features, die aus dem Router ein kleines IP-TK-System machen würden, kommen ebenfalls nicht vor, was den Einsatz als VoIP-Gateway im SOHO-Netz ausschließt.

#### **AVM Fritz!Box Fon WLAN 7490**

Auch wenn der deutsche Hersteller AVM, der seit 1986 existiert und sich mit der Herstellung von ISDN-Produkten einen Namen gemacht hat, international eher eine untergeordnete Rolle spielt - in Deutschland gilt seine Routerreihe Fritz!Box derzeit unangefochten als Marktführer. Durch Kooperationen mit den großen ISP steht eine Fritz!Box mittlerweile an jedem 2. deutschen Internetanschluss. Die Modelle zeichnen sich durch



Abbildung 29: AVM Fritz!Box 7490

einfache Bedienbarkeit und eine besondere Funktionsvielfalt aus. Der Hersteller entwickelt regelmäßig neue Hardware, um technisch aktuell zu bleiben. Die grundlegende Firmware ist jedoch auf den Modellen gleich, nur ihre Optionen sind entsprechend der Hardware unterschiedlich. Erst wenn ein Modell aufgrund des Alters aus der Modellpalette fällt, wird die aktuelle Version der Fritz!OS-Software nichtmehr für das Gerät angeboten. Dadurch kommt jeder Fritz!Box-Benutzer in den Genuss des aktuellen Funktionsumfangs (insofern seine Hardware dies unterstützt). Fritz!OS ist im Vergleich zu den anderen getesteten Routerfirmware-Produkten eine regelrechte Spielwiese. Das System bietet die größte Vielfalt an Einstellmöglichkeiten. Darstellung als auch Benutzerunterstützung (erklärende Texte, vorgegebene Beispiele,...) sind beispielhaft.

Im Test wird eine Fritz!Box Fon WLAN 7490 mit der Firmware Fritz!OS 06.83 vom 09.03.2017 eingesetzt. Das Modell verfügt über ein integriertes DSL/VDSL-Modem und IP-Telefoniefunktionen. IPv6 ist in den Fritz!Boxen schon seit längerer Zeit implementiert, nicht zuletzt weil in Deutschland verbreitete Kabel-ISP's speziell die Fritz!Box für Ihre DS-Lite-Anschlüsse anbieten und sie dann mit teilweise sogar eigener, angepasster Firmware ausstatten. Diese angepassten Varianten können in Details von der hier getesteten allgemeinen Firmware abweichen.

Nach dem ersten Start im Auslieferungszustand erreicht man die Konfigurationsoberfläche bereits über das DNS-Kürzel „*fritz.box*“. IPv6 ist weder im WAN, noch im LAN aktiviert und muss dementsprechend erst über die erweiterte Ansicht der Konfigurationsoberfläche zugeschaltet werden. Diese Aktivierung ist die Voraussetzung für die Freischaltung des kompletten IPv6-Potentials der Fritz!Box. Ab diesem Zeitpunkt kann jedoch auf IPv4 verzichtet werden. Die Konfigurationsoberfläche kann per IPv6 bedient werden. Selbst der DNS-Kurzname *fritz.box* löst die eingestellte IPv6-Adresse der Box auf.

Die Registrierung bei einem DDNS-Anbieter erfolgt sowohl für IPv4-, als auch für IPv6-Adressen. Die Zeitsynchronisation über IPv6 mit dem NTP-Protokoll funktioniert ebenfalls, es muss jedoch eine IPv6-fähige URL eingetragen werden (z.B.: *2.de.pool.ntp.org*).

Die IPv6-bezogenen Einstellmöglichkeiten zeigen im Testfeld den mit Abstand größten Umfang. Präfixe können nicht nur delegiert, sondern auch beim übergeordneten Router in einer bestimmten Größe angefordert werden (einziger Router im Testfeld, mit dem sinnvoll Subnetze gebaut werden können). Die gängigen Tunneltechnologien für WAN werden ebenso unterstützt, wie die MTU separat für IPv4/IPv6 angepasst werden kann.

Die vom ISP zugeordneten IPv6-DNS-Server werden ordentlich angezeigt, die Konfiguration eigener Adressen ist möglich.

Für die Adressverwaltung im LAN ist das Verhalten ebenfalls umfangreich anpassbar. So können eigene ULA-Adressen mit manuell festlegbarem Präfix verteilt werden (SLAAC oder DHCPv6), es kann jedoch auch der Globale Präfix genutzt werden. Kombinationen aus beidem (ULA/Global) sind ebenfalls möglich. Die Einstellbarkeit geht sogar so weit, dass die Fritz!Box nur dann für die Verteilung von ULA-Adressen bei den Clients sorgt, wenn kein globaler Präfix vorhanden ist.

Die Priorisierung verschiedener Router/DNS-Server im gleichen LAN mittels Präferenzwerten ist möglich – wodurch interessante Redundanzszenarien mit Fritz!Boxen denkbar werden. So könnte ein Netzwerk über zwei Internetanschlüsse mit jeweils einer Fritz!Box verfügen. Jeder Host würde IP-Adressen beider Internetanschlüsse besitzen und darüber kommunizieren können. Bei Ausfall eines Anschlusses (oder eines Routers) könnte

der komplette Verkehr über den verbliebenen geroutet werden. Durch die Präferenzierung wäre sogar eine Festlegung des Standard-Wegs möglich.

Das Gerät verfügt ebenfalls über eine IPv6-fähige Firewall, die im Gegensatz zu den Konkurrenzprodukten nicht nur statisch anhand von IP-Adressen konfiguriert werden kann. Da die Fritz!Box eine Übersicht über ihre Kommunikationspartner mit zugehörigem Hostnamen, MAC-Adresse, IPv4 sowie IPv6-Adresse speichert, kann die Einrichtung von Regeln eigentlich auf Basis des Gerätes (der MAC-Adresse) unabhängig von aktuellen IP-Adressen erfolgen. Für IPv4 funktioniert das auch bereits, für IPv6 ist (noch) die Festlegung der 64bit langen Interface-ID nötig. Damit ist die Fritz!Box im Test der einzige Router, dessen Firewall IPv6-Freigaben für dynamisch wechselnde Präfixe zulässt! Allerdings ist auch die Fritz!Box nicht in der Lage, dauerhafte Freigaben für IPv6-Adressen mit Privacy-Option einzurichten, wobei die Anforderung eher theoretischer Natur wäre.

Nett ist auch, dass die Einstellungen für IPv6 bereits ordentlich in den Übersichten mit angezeigt werden. Die Informationen müssen nicht, wie bei der Konkurrenz, mühsam in unterschiedlichsten Menüs zusammengesucht werden. Einzige Ausnahme ist die „Heimnetzübersicht\Netzwerkverbindungen“, die derzeit noch keine Spalte „IPv6-Adresse“ aufweist, allerdings rechne ich diesbezüglich mit einer Verbesserung durch AVM in einer der nächsten Firmwareversionen.

Ein Manko ist allerdings doch zu finden: VPN! Die Einwahl zur Fritz!Box mittels eines IP-Sec-Clients unter Verwendung des IPv6-Protokolls ist möglich. Die Konnektivität zu Ressourcen im eigenen LAN hinter dem VPN-Tunnel erfolgt jedoch nur mittels IPv4-Adressen, da IPv6-Netze nicht durch den Tunnel geroutet werden können. Die Routing-Einstellungen erlauben nur IPv4-Netze. Das gilt dementsprechend auch für InterSite-Verbindungen (LAN-LAN-Kopplung). Geht man von Dual-Stack-Implementierungen aus und verzichtet auf den IPv6-Only-Betrieb, ist dieses Manko sicherlich verschmerzbar, erfordert jedoch genaue Planung bei der Bereitstellung von Diensten im LAN.

Die Fritz!Box kann im Gegensatz zu den anderen getesteten Routern aufgrund eingebauter VoIP-Gateway-Funktionalität auch als IP-TK-System genutzt werden. Diese Funktion findet in den Testergebnissen keine Berücksichtigung, da die anderen ausgewählten Router die Funktion nicht unterstützen. Jedoch ist es dadurch möglich, die Fritz!Box selbst als SIP-Client (IPv6-fähig) zu verwenden und daran andere Telefonendgeräte (analog, ISDN oder SIP inkl. IPv6) anzubinden.

Die Fritz!Box ist im kleingewerblichen sowie privaten Umfeld bereits jetzt für die Implementation von IPv6 empfehlenswert, da alle wichtigen Einstellungen getroffen und benutzt werden können.

### 3.4.3 Ergebnisse Routertests

Die folgende Tabelle zeigt die Ergebnisse der Routertests. Klar zu empfehlen ist hier einzig das Modell Fritz!Box, da alle anderen Systeme wichtige Funktionen unter IPv6 noch nicht darstellen können.

	ASUS DSL-AC68U	AVM Fritz!Box 7490	Linksys E2500	TP-Link Archer C59
Firmwarestand	v3.0.0.4.380.7712 11.08.2017	v06.83 09.03.2017	v3.0.02 16.06.2016	v1.0.2 25.07.2016
Unterstützung von IPv6 (Herstellerangabe)	✓	✓	✓	✓
Modem integriert ((V)DSL/DOCSIS/...)	✓	✓	✗	✗
<b>WAN</b>				
Bezug globaler IPv6-Adressen vom ISP	✓	✓	✓	✓
Bezug von IPv6-Präfixen	✓	✓	✓	✓
Unterstützung von DS-Lite	✓	✓	✓	✓
Unterstützung von Tunneltechnologien (6to4, 6in4, 6rd)	✓	✓	✗	✓
<b>LAN</b>				
Auslieferungszustand: IPv6 aktiviert?	✗	✗	✗	✓
Zugriff auf WebGUI per IPv6-Adresse	✗	✓	✓	✗
Konfigurierbarkeit der IPv6 LAN-Optionen	✓	✓✓	✗	✓
Zuweisung von IPv6-Adressen mit <i>eigenem</i> (ULA-) Präfix	✓	✓	✗	✓
Zuweisung von IPv6-Adressen mit <i>übernommenem</i> (globalen) Präfix	✓	✓	✓	✓
Delegation von Präfixen an nachgeordnete Router	✓	✓ <sup>22</sup>	✗	✗
Prefix-Forwarding /Umnummerierung nach Prefix-Wechsel	✓	✓	✓	✓
DHCPv6-Server	✓	✓	✗	✓
DNSv6-Server	✓	✓	✗	✗
<b>Router-Funktionen</b>				
Registrierung der IPv6-Adresse bei DDNS-Anbietern	✗	✓	✗	✗

<sup>22</sup> Präfixlängen konfigurierbar

Zeitsynchronisierung (NTP) über IPv6	x	✓	x	x
Auflösung des herstellerspez. Hilfs-DNS-Namens zu der IPv6-Adresse des Geräts	x	✓	x	x
VPN-Einwahl auf öffentliche IPv6-Adresse	x	✓	x	x
VPN: IPv4-Verkehr durch einen Tunnel	✓	✓	x	✓
VPN: IPv6-Verkehr durch einen Tunnel	x	x	x	x
<b>Firewall</b>				
Firewallregeln für dyn. Präfixe (Hosts unabhängig von ihrer IP identifizierbar)	x	✓	x	x
Firewallregeln für ganze Subnetze	✓	✓	x	x
UPnP-Unterstützung zur Freigabeautomatisierung	✓	✓	x	x
<b>Telefonie<sup>23</sup></b>				
eigene Portkonfiguration für SIP <u>nicht</u> nötig	✓	✓	✓	✓
ausgehende Rufe inkl. Mediastreaming	✓	✓	✓	✓
eingehende Rufe bei angemeldeter SIP-Verbindung (inkl. Mediastreaming)	✓	✓	✓	✓
Konferenzschaltung (mit 2. Teilnehmer im LAN)	✓	✓	✓	✓
Handover (Übergabe an 2. Teilnehmer im LAN)	✓	✓	✓	✓
Telefonat übersteht Präfixwechsel	✓	✓	x <sup>24</sup>	x
Gesamtwertung: <b>Eignung für DualStack</b>	✓✓	✓✓✓	✓	✓
Gesamtwertung: <b>Eignung für IPv6_only</b>	x	(✓) <sup>25</sup>	x	x

Tabelle 6: Ergebnisse Routertests

**Der Router ist für den Umstieg auf IPv6 das wichtigste Bindeglied. Es gibt noch sehr wenige, aber einige Router können heute schon für einen Umstieg auf IPv6 genutzt werden. Ein Betrieb ohne IPv4 scheint aber aktuell bei allen Anbietern noch nicht realisierbar.**

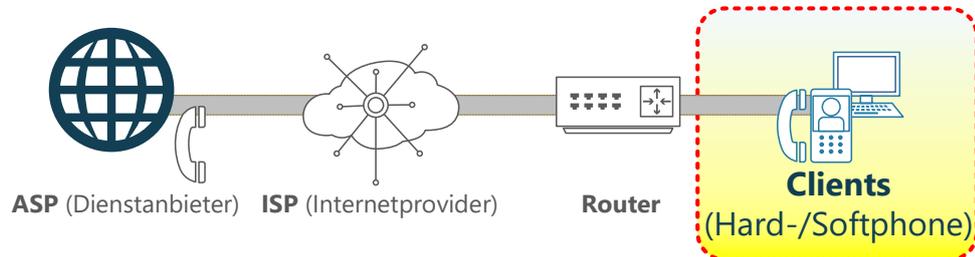
<sup>23</sup> Tests im IPv6-only-Modus durch Deaktivierung von IPv4 am Grandstream-Telefon

<sup>24</sup> Der Präfixwechsel führt scheinbar zu einem Neustart des Netzwerkstacks, der alte Präfix wird trotz TTL sofort vergessen.

<sup>25</sup> Eine Einrichtung ohne IPv4 ist nicht möglich, der spätere Betrieb schon

### 3.5 Clients

Viertes und damit letztes Element in der Kette IP-basierter Sprachkommunikation vor dem Benutzer ist der Client.



Mit der Verbreitung von Internettelefonie entstand auch eine neue Klasse an Endgeräten, die sog. Softwarebasierten Clients. Zuvor waren eigentlich nur klassische Hardware-Telefone verfügbar. Relevant für die Untersuchung sind natürlich beide Gruppen, allerdings aus jeder Gruppe nur diejenigen Clients, welche nativ das SIP-Protokoll unterstützen. Für beide Kategorien gibt es am Markt sehr viele Hersteller, die ihre Produkte verkaufen möchten, meist als proprietäre Systeme in direkter Verbindung mit einer Telefonanlage (IP-PBX). Diese proprietären Clients sind i.d.R. etwas teurer und nicht zwangsläufig für Kunden im kleingewerblichen Bereich gedacht – auch wenn ihre Integrationstiefe in das PBX-System meist stärker ausgeprägt ist. Der Hersteller unify (vormals Siemens Enterprise Communication) stellt beispielsweise Hardwaretelefone her, die jedoch mit einer Firmware ausgeliefert werden, welche das Kommunikationsprotokoll HFA (HiPath Feature Access) bzw. CorNet IP (Corporate Network) verwendet – ein von Siemens selbst entwickeltes Protokoll für die Kommunikation über IP [FS16, S. 178]. Ähnliche Schritte sind auch andere Hersteller gegangen. Erst in jüngerer Zeit verbreitet sich durch die Nachfrage der Kunden und durch die Verfügbarkeit von Alternativen (Snom, Yealink, Grandstream, ...) das SIP-Protokoll auch bei den etablierten Herstellern wie unify oder Ascom. Kunden im SOHO-Bereich waren schon bisher eher ungeeignet für die Vermarktung der proprietären Systeme, da die Einstiegshürde zumeist zu hoch war. Für unsere Untersuchung kommen nur echte SIP-Clients in Frage, jedoch sollen diese auf unterschiedlichen Plattformen getestet werden.

Als Telefonanlage wird auf Cloud-Telefonie gesetzt. Eine lokale IP-PBX würde uns keine abweichenden Ergebnisse liefern und ist aktuell zwar noch häufig anzutreffen, wird aber in den nächsten Jahren (und mit der Verbreitung von IPv6) deutlich Marktanteile an cloudbasierte Systeme verlieren, denn gerade für die kleingewerbliche Nutzung ist die geteilte Nutzung zentralisierter Infrastruktur, welche ein ITSP wie sipgate anbietet, deutlich günstiger als der Betrieb eigener Systeme.

### 3.5.1 Prüfverfahren

Bereits in Abschnitt 3.2.2 - *Internettelefonieanbieter (ITSP)* wurden versch. Produkte und Anbieter getestet. Für die Tests der Clients wurden wie zuvor beschrieben kostengünstige Produkte ausgewählt, die eine Anmeldung als **SIP-Client** erlauben und IPv6 unterstützen. Es wurde vorrangig das Produkt „*sipgate basic*“ benutzt – ein grundgebührenfreier SIP-Anschluss mit einzelner Ortsnetzzufnummer. Lediglich für die Abrechnung von Gesprächsgebühren muss das Prepaid-Produkt mit Guthaben versehen werden. Zur Überprüfung der Ergebnisse wurde ebenfalls ein Anschluss „*sipgate team*“ desselben Anbieters sowie „*call basic*“ des Anbieters *easybell* und „*placetel free*“ des Anbieters *placetel* getestet. Gemäß den Ergebnissen aus *Abschnitt 3.2.2 - Internettelefonieanbieter (ITSP)* und des jeweiligen Preismodells für die Produkte boten sich diese Anbieter für die Versuchsreihe an. In der Beschreibung wird näher auf die Variante „*sipgate basic*“ eingegangen, die Abläufe sind jedoch für die anderen Varianten ähnlich.

#### **Einrichtung der Clients**

Die Anbieter geben sich große Mühe, genaue Anleitungen für verbreitete SIP-Clients bereit zu stellen (Hard- und Soft-Clients). Bei Sipgate kann man sich neben den allg. Anleitungen<sup>26</sup> auf dem Webportal sogar individualisierte Anleitungen zu versch. Geräten mit den jeweils individuellen Login-Daten des Benutzerkontos anzeigen lassen. Auf die IP-Konfiguration wird jedoch in der Regel nicht eingegangen. In der Testumgebung wird zur Ermittlung der Funktionen das IPv4-Protokoll von Seiten des Routers abgeschaltet (Deaktivierung DHCP).

#### **Test der Verbindung**

Nach erfolgreicher Registrierung des Sipgate-Kontos mit dem jeweiligen SIP-Client beim Provider wurde die von Sipgate bereitgestellte Rufnummer 10005 angerufen.

An dieser Rufnummer nimmt ein Automat das Gespräch an, zeichnet den ankommenden Audiostream auf und spielt ihn nach Eingabe der #-Taste durch den Anrufer wieder ab.

Dieser Test eignet sich daher besonders gut für den Nachweis folgender Funktionen:

Rufaufbau outbound, Mediastreaming Tx, Mediastreaming Rx,  
Übertragung von DTMF

---

<sup>26</sup> <https://www.sipgatebasic.de/konfiguration/>

Verschiedene Clients verschiedener Hersteller wurden getestet. Der Rufaufbau für eingehende Anrufe musste jeweils durch einen separaten Anruf aus dem PSTN verifiziert werden.

### **Probleme bei der Nutzung IPv6-basierter Clients**

- Nicht immer ist eine Einrichtung des Gerätes ohne IPv4 möglich
- Autoprovisionierung der Hersteller oft nur mittels IPv4 (FTP)
- Einige Firmwarestände sind im Bereich IPv6 noch fehlerhaft  
Bsp.: bei Grandstream-FW, keine Zeitsynchronisation (NTP) mittels IPv6<sup>27</sup>

### **Problem DNS SRV-Eintrag: keine Registrierung ohne IPv4**

Problematisch kann unter IPv6 bereits die Registrierung des Clients beim Server sein. In nahezu allen Fällen (außer miniSipPhone) konnte die Standardmethode des Telefons die IPv6-Adresse des zuständigen SIP-Registrar-Servers nicht ermitteln. (Siehe Abschnitt 3.2.3-*Das DNS-Problem bei den ITSP*) Dass die ITSP dennoch IPv6 unterstützen kann mithilfe von miniSipPhone oder dem Grandstream GXP1450 nachgewiesen werden, da bei diesen der Registrar-Server auch angegeben werden kann, ohne dass die SRV-Record-Methode angewendet wird. Alle anderen Clients konnten nur im DualStack-Modus getestet werden.

## **3.5.2 Softwarebasierte Clients**

Auf Wikipedia wird eine öffentliche Liste von VoIP-Software gepflegt<sup>28</sup>. Darin befinden sich aktuell 78 Clients, davon sind derzeit 33 Clients für Windows, nicht proprietär und unterstützen SIP. Mit der Forderung nach IPv6-Unterstützung durch den Hersteller wird die Anzahl noch geringer. Die vielversprechendsten Kandidaten sollen hier vorgestellt werden:

### **Zoiper**

Die belgische Firma Securax Ltd. hat unter der Handelsmarke Zoiper einen SoftClient herausgebracht, der mittlerweile in der 5. Version für die Plattformen Windows, MacOS, Linux und für Smartphones bereitgestellt wird. Der Client ist in der Grundversion frei. Für die kommerzielle Nutzung muss eine Lizenz (derzeit 39,95€) gekauft werden. Dafür erhält der



---

<sup>27</sup> NTP-Projekt pool.ntp.org bereits IPv6-fähig [poo17]

<sup>28</sup> [https://de.wikipedia.org/wiki/Liste\\_von\\_VoIP-Software](https://de.wikipedia.org/wiki/Liste_von_VoIP-Software)

Käufer aber auch zusätzl. Funktionen wie Outlook-Addin, Browser-Integration, Vermitteln und Konferenz.

Der Client ist sehr übersichtlich aufgebaut, das sipgate-Konto einfach in den Einstellungen zu konfigurieren, eine Anleitung bei sipgate ist vorhanden.

Leider kann der Client entgegen der Ankündigungen des Herstellers kein IPv6. Liest man deshalb die Angaben des Herstellers genauer<sup>29</sup>, so stellt sich heraus, dass Zoiper bisher nur IPv6-Unterstützung für den iOS-Client implementiert hat. Daher funktioniert Zoiper leider nur im DualStack-Betrieb und auch dann nicht unter Nutzung des IPv6-Protokolls. Daher wird er in den Testergebnissen nicht berücksichtigt.



Abbildung 30: Zoiper-Benutzeroberfläche

### X-Lite (Counterpath)

X-Lite ist die freie, aber eingeschränkte Version des SIP-Clients Bria des Herstellers Counterpath. Der Hersteller kann sich bereits seit längerem hoher Beliebtheit für seine Produkte erfreuen. Zu Bria schreibt er ganz offiziell, dass IPv6 unterstützt wird. Für den X-Lite-Client, der nur professionelle Features vermissen lassen soll, gibt es keine genauere Angabe zu den unterstützten IP-Protokollen. Dass der Client IPv6 unterstützt ist aber zumindest zu vermuten. Die Installation verläuft einfach, die Einrichtung dank Anleitungen von sipgate problemlos.



Leider zeigt sich schnell, dass der Client keinerlei erweiterte Einstellmöglichkeiten besitzt. Er ist im Dual-Stack-Betrieb nicht zur Verwendung von IPv6 zu bewegen. Auch nicht durch Eingabe der konkreten IPv6-Adresse des Servers. Bei deaktiviertem IPv4 verhält er sich, als hätte er gar keine Internetverbindung.

Fazit: Der Client ist für die hier untersuchten Zwecke nicht zu verwenden und wird ebenfalls nicht berücksichtigt.

<sup>29</sup> <https://community.zoiper.com/4361/zoiper-with-ipv6>

## Linphone

Die ursprünglich aus der Linux-Welt stammende Open-Source-Software Linphone<sup>30</sup> ist weit verbreitet und für Linux, Windows und MacOS verfügbar. Der Client versteht die gängigen Sprachcodecs und bietet sogar Videotelefonie und Verschlüsselung an. Linphone verspricht ebenfalls IPv6-Unterstützung. Im Test zeigte sich jedoch, dass die Software ohne IPv4 keine Anmeldung am sipgate-Registrar ermöglicht. Schuld daran ist das bereits beschriebene DNS-Problem<sup>31</sup>. Im DualStack-Betrieb jedoch gelingt die Anmeldung beim Registrar hervorragend und der Client bevorzugt sogar automatisch die Kommunikation über das neue Protokoll. Sipgate bietet eine Konfigurationsanleitung<sup>32</sup> für Linphone an, empfiehlt darin jedoch das Deaktivieren von IPv6. Im Test konnte in einer DualStack-Umgebung kein Grund dafür gefunden werden – bis auf das erste Auffinden des Servers funktioniert der Client mit IPv6 tadellos. Darüber hinaus spart sich der Nutzer das aufgrund des NAT notwendige und möglicherweise aufwändige Konfigurieren unterschiedlicher Ports für jeden einzelnen Client, welches auch sipgate in seiner Anleitung als notwendig beschreibt.

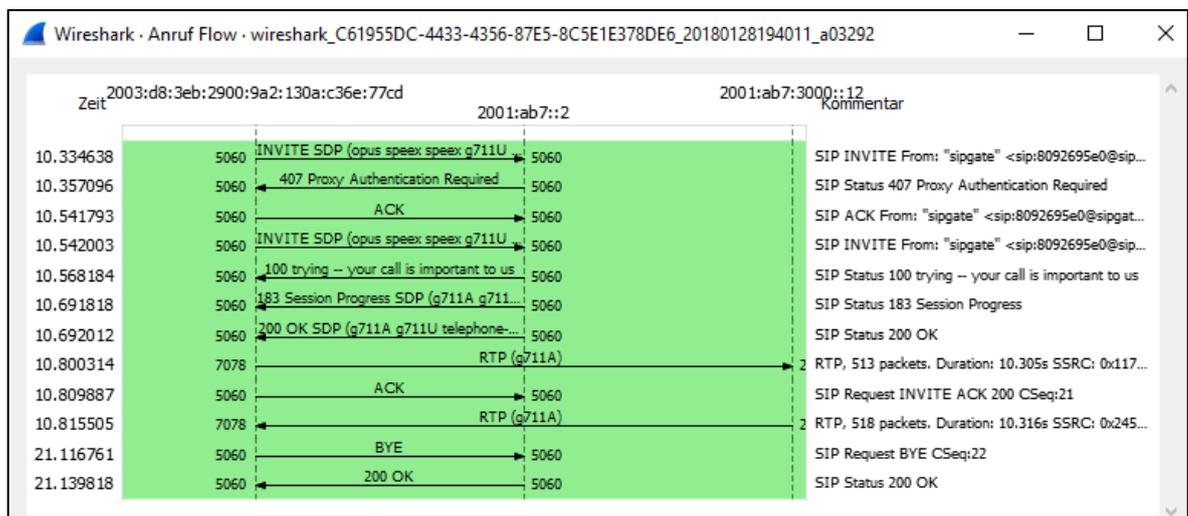


Abbildung 31: SIP-Trace eines Linphone-Anrufes mit IPv6

Testanrufe in- wie auch outbound funktionierten einwandfrei. Konferenzen und Transfers zeigten keine Probleme. Der Client kann daher empfohlen werden.

<sup>30</sup> <http://www.linphone.org/>

<sup>31</sup> Vgl Abschnitt 3.2.3- Das DNS-Problem bei den ITSP

<sup>32</sup> <https://www.sipgatebasic.de/konfiguration/40/windows-softphones-linphone>

## miniSipPhone

Diese Software ist die rudimentärste Realisierung der getesteten SIP-Clients. Die Konfiguration lässt ausschließlich die Eingabe von Registrar-Servername, Port und Benutzername/Kennwort zu. Auch ansonsten besteht die Oberfläche nur aus einem Eingabefeld zum Eingeben von Rufnummern und zwei Schaltflächen zum Abheben und Auflegen. Aufgrund der Einfachheit, wird der Server auch nicht mittels der SRV-Record-Methode aufgelöst. Dadurch hat der Client dann auch keinerlei Probleme unter IPv6. Die Registrierung erfolgt schnell und zuverlässig, binnen kürzester Zeit können Telefonate geführt werden. Die Übermittlung von DTMF, das Weiterverbinden oder Schalten von Umleitungen entfällt. Eben ein sehr puristischer Telefonie-Client. Aber einer, der in IPv6-only-Kommunikationsnetzwerken besonders einfach eingesetzt werden kann.

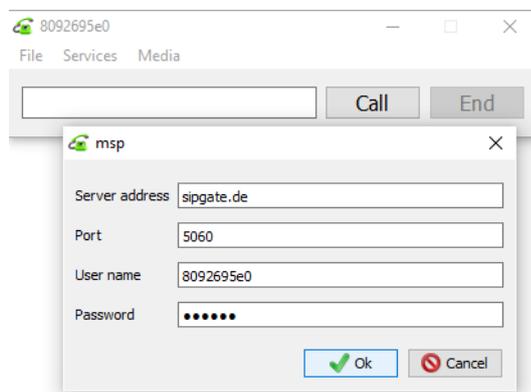


Abbildung 32: miniSipPhone Konfigurationsdialog

Im Dual-Stack-Betrieb bevorzugt er leider IPv4. Der folgende Wireshark-Mittschnitt zeigt den Verlauf eines Testrufes an die Testnummer 10000 von Siptgate bei deaktiviertem IPv4.

No.	Time	Source	Destination	Protocol	Length	Info
919	37.009034	2003:d8:3eb:2900:9a...	2001:ab7::4	SIP	817	Request: REGISTER sip:8092695e0@sipgate.de (1 binding)...
920	37.105503	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP	795	Status: 200 OK (3 bindings)
1171	47.123058	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP	602	Request: BYE sip:8092695e0@192.168.128.198:20000
1172	47.123261	2003:d8:3eb:2900:9a...	2001:ab7::4	SIP	703	Status: 200 OK
1231	51.773463	2003:d8:3eb:2900:9a...	2001:ab7::4	SIP/SDP	865	Request: INVITE sip:10000@sipgate.de
1232	51.804820	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP	557	Status: 407 Proxy Authentication Required
1233	51.844082	2003:d8:3eb:2900:9a...	2001:ab7::4	SIP	675	Request: ACK sip:10000@sipgate.de
1234	51.857150	2003:d8:3eb:2900:9a...	2001:ab7::4	SIP/SDP	1070	Request: INVITE sip:10000@sipgate.de
1235	51.917661	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP	435	Status: 100 trying -- your call is important to us
1236	52.036289	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP/SDP	1042	Status: 183 Session Progress
1237	52.036289	2001:ab7::4	2003:d8:3eb:2900:9a...	SIP/SDP	1028	Status: 200 OK

Abbildung 33: SIP-Trace eines Rufaufbaus unter Verwendung von IPv6

Zur Konfiguration sollte man den Client einmalig mit Administratorrechten starten, sonst kann er die eingestellten Parameter (es sind ja nur 4) nicht speichern und fragt bei jedem neuen Programmstart erneut alles ab.

## Jitsi

Jitsi ist eine multiprotokollfähige Messenger- und IP-Telefonieplattform, die man zum Chatten, Telefonieren und Videotelefonieren verwenden kann. Die Nutzung als SIP-Client ist nur ein Teil des Gesamtumfangs des OpenSource-Programms. Dank Programmierung in Java ist es auf allen Desktop-Plattformen verfügbar (Windows, Linux, MacOS). IPv6 soll bereits vollständig unterstützt werden<sup>33</sup>. Bisher scheint der Client noch nicht besonders verbreitet zu sein, was vielleicht auch an seiner nicht so besonders gefälligen Oberfläche liegt.

Sipgate hat bisher keine Konfigurationsanleitung bereitgestellt, daher gestaltet sich die erste Konfiguration etwas schwieriger. Hinzu kommt, dass der Client nach der Installation zwar Konfigurationsdaten für ein SIP-Konto abfragt, jedoch davon ausgeht, dass dies ein Registrierungsloses SIP-Konto sein soll. Es müssen daher nachträglich noch einzelne Einstellungen des Kontos verändert werden.

Etwas unschön ist auch, dass sich der Client nach manchen Einstellungsänderungen etwas komisch verhält und diese nicht anzeigt oder umsetzt. Dann hilft i.d.R ein Neustart des Clients.

Dafür konnte Jitsi allerdings bei der Unterstützung von IPv6 enorm punkten. Im Dual-Stack wird zwar noch IPv4 bevorzugt (und es gibt auch keine Einstellung, die dies beeinflusst), schaltet man IPv4 jedoch ab, dann wechselt der Client komplett auf Nutzung von IPv6. Sogar das lästige DNS-Problem kann der Client umgehen, denn er besitzt eine Backup-DNS-Resolver-Funktion, bei der er die Auflösung des Registrars an einen Dienst der Jitsi-

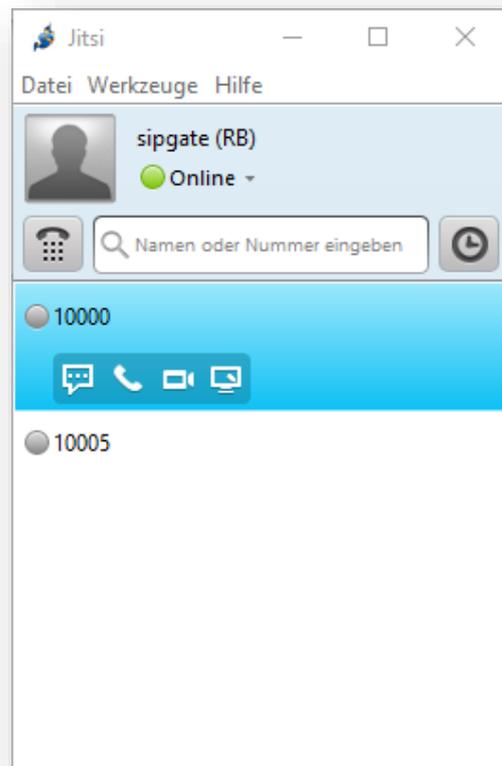


Abbildung 34: Zoiper-Benutzeroberfläche

<sup>33</sup> <https://desktop.jitsi.org/Main/Features>

Plattform ausgelagert. Dies soll im Normalfall den Auflösungsprozess beschleunigen, hat aber unter IPv6 den positiven Nebeneffekt, dass das DNS-Problem nicht auftritt.

### **3CX Phone für Windows**

Der 3CX-Client ist hier nur der Vollständigkeit halber aufgeführt, denn er nutzt zwar SIP, kann jedoch nur zur Anbindung an ein 3CX-Telefonsystem verwendet werden. Abweichende SIP-Einstellungen sind nicht möglich, denn der Client nutzt einen Auto-Provisionierungs-Algorithmus von 3CX, der es leider nicht so leicht ermöglicht, den Client an Standard-SIP-Anlagen zu betreiben. Allerdings stört dies nicht für die unter Abschnitt 4.3 - *Selfhosted PBX – die eigene, cloudbasierte IP-PBX* vorgestellte Alternative. Zu beachten ist, dass der Client mit dem Server proprietär kommuniziert, es findet keine übliche SIP-Registrierung statt, sondern der 3CX-Client baut zum 3CX-Server einen Tunnel auf, durch den die Rufsteuerung und Medienstrompakete gesendet werden. Da dieser Tunnel jedoch auch mit dem IPv6-Protokoll genutzt werden kann, ist diese Realisierung durchaus interessant – allerdings nur, wenn als PBX das Produkt der 3CX eingesetzt wird.



### Ergebnisse softwarebasierte Clients

Die Auswertung zu den Clients untersucht deren Verhalten in IPv6-Netzwerkumgebungen. Aufgrund der fehlenden Unterstützung werden Zoiper und X-Lite nicht in den Ergebnissen berücksichtigt.

	LinPhone (Win)	miniSipPhone	Jitsi	3CX Client
Version	4.1.1 Qt5.9.0	v7	2.10.5550	v15.5.7582.3
Unterstützung von IPv6 (Herstellerangabe)	✓	✓	✓	✓
Unterstützung von Standard-SIP	✓	✓	✓	✗ <sup>34</sup>
<b>Registrierung</b>				
DNS-Auflösung des Registrar-Servers über IPv6	✗	✓	✓	✗
IPv6-Kommunikation durch Angabe der IPv6-Adresse als Server	✓	✓	✗	✓
Registrierung über IPv6-Protokoll	✓	✓	✓	✓
Beständigkeit der Registrierung über Präfixwechsel hinweg	✓	✓	✓	✓
<b>Telefonieren</b>				
Rufaufbau über IPv6-Protokoll	✓	✓	✓	✓
beidseitiges Mediastreaming über IPv6	✓	✓	✓	✓
Fortführung des Gesprächs bei Präfixwechsel	✓	✓	✓	✓
<b>Komfort-Funktionen</b>				
Makeln, Halten,	✓	✗	✓	✓
Verbinden, Konferenzen	✓	✗	✓	✓
Gesamtwertung: <b>Eignung für DualStack</b>	✓	✓	✓	✓
Gesamtwertung: <b>Eignung für IPv6_only</b>	✗	✓	✗	✓

Tabelle 7: Ergebnisse softwarebasierte Clients

**Am Markt befinden sich einige IPv6-fähige Software-Clients für das SIP-Protokoll. Bei Auswahl eines zum System passenden Clients, kann die Nutzung von IPv6 bereits empfohlen werden.**

<sup>34</sup> Nur proprietär an 3CX-Servern verwendbar

### 3.5.3 Hardwarebasierte Clients

Hohe Updatehäufigkeit durch die Hersteller, geringe Lebenszyklen der Produktserien, schnelle Ablösung durch Nachfolgeprodukte, alle diese Eigenschaften sind anzutreffen bei den Hardwareprodukten in der IP-Telefonie. Jeder Hersteller versucht die anderen mit größeren, bunteren Displays und mehr Tasten zu übertrumpfen. Die technischen Eigenschaften und bspw. die Unterstützung für IPv6 spielen in den Vermarktungsstrategien leider keine Rolle. Hinzu kommt, dass viele Hersteller, die für das Enterprise-Segment produzieren, hauptsächlich proprietäre Protokolle einsetzen. Damit verhindern Sie, dass Kunden an ihren Anlagen gemischte Clientumgebungen einsetzen.

- Siemens: OpenStage SIP-Telefone (gehen nicht, kein IPv6-Stack)
- Cisco: Telefone mit proprietärer FW, können nicht an offenen SIP-Servern eingesetzt werden
- Mitel (Aastra): derzeit keine offiz. IPv6-Unterstützung
- Gigaset-DECT-Modelle und Tischtelefone: keine IPv6-Unterstützung

Der Test einer großen Palette ist nicht durchführbar, daher beschränkt sich die Auswertung auf den punktuellen Test häufig eingesetzter Fabrikate. Es gibt am Markt einige Anbieter, die IPv6-Endgeräte anbieten. Dabei handelt es sich um recht junge Unternehmen, die im Gegensatz zu den großen Anbietern nie klassische Telefone gebaut haben. Hier lassen sich Snom, Grandstream und Yealink nennen.

#### **Unify OpenScape Desk Phone CP600, CP400, CP200 und OpenStage 15, 20, 40, 60, 80**

Die Telefonmodelle nutzen alle ähnliche Firmware. Die Geräte sind sowohl mit einer SIP-Firmware, als auch mit der häufiger anzutreffenden HFA-Firmware erhältlich. Letztere stellt eine proprietäre Schnittstelle dar und wird hier nicht untersucht. Die SIP-Variante verfügt über umfangreiche Einstellmöglichkeiten. Leider gibt es zum aktuellen Zeitpunkt keine IPv6-Unterstützung für die gesamte Linie. Der Hersteller arbeitet jedoch nach eigenen Angaben an der Bereitstellung und empfiehlt den eigenen Kunden bereits heute den Einsatz von DualStack-Umgebungen. Laut eigener Angabe soll ab der Firmwareversion V3 R0.1.0 bereits IPv6 unterstützt werden. Die mir vorliegende Firmware V3 R0.33.0 beinhaltet allerdings keine Einstellungen für IPv6.

General information	
MAC address	001ae88bbfe4
Software version	V3 R0.33.0 160126
Last restart	2017-12-09T18:36:08

Abbildung 35: unify OpenStage 15 Firmwarestand

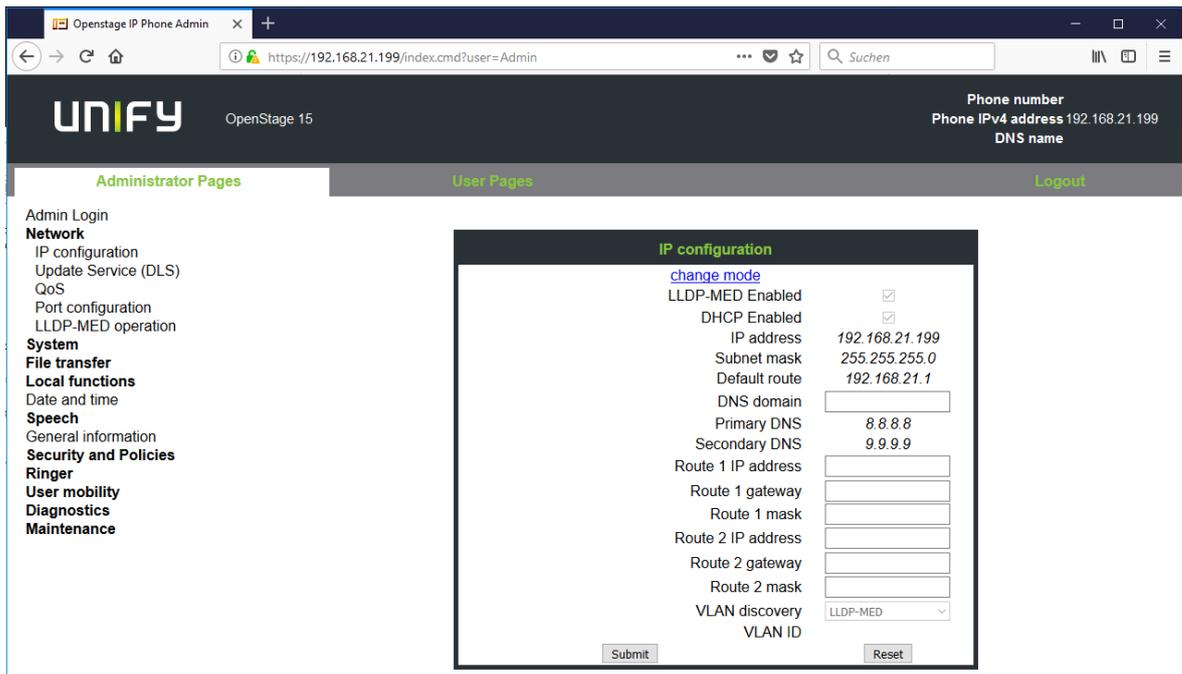


Abbildung 36: Netzwerkeigenschaften unify OpenStage 15

Die Informationen sind daher widersprüchlich. Aufgrund der fehlenden Einstellmöglichkeiten für IPv6 konnte auch kein Gespräch mit dem Gerät unter Nutzung des neuen Protokolls geführt werden.

### snom

Der aus Deutschland stammende Hersteller snom stellt SIP-Telefone her. Er konzentriert sich dabei ausschließlich auf Client-Endgeräte. Ein PBX-System passend dazu hatte snom zwar einige Zeit im Portfolio (eine angepasste Asterisk), das Angebot wird jedoch nichtmehr fortgeführt. Gemäß Herstellerangabe wird IPv6 von allen Geräten der 7xx oder 8xx Serie unterstützt. Die preisgünstige 3xx Serie ist leider nicht IPv6-fähig. Im Test zeigte sich, dass im Lieferzustand des getesteten snom715 das IPv6-



Abbildung 37: snom715

Protokoll noch nicht aktiviert ist. Allerdings ist das Protokoll auf dem Webinterface einfach hinzuschalten. Die Konfigurationsmöglichkeiten sind übersichtlich. Die Einstellung DHCPv6 besitzt 3 verschiedene Optionen, welche das Verhalten für IPv6 regeln – „Auto“ (SLAAC), „An“ (SLAAC oder DHCPv6) oder „Aus“ (IPv6 ganz aus). Der einstellbare NTP-Server wird per IPv6 abgefragt, sodass auch diese Funktion in einem IPv6-Only-Netzwerk funktionierte.

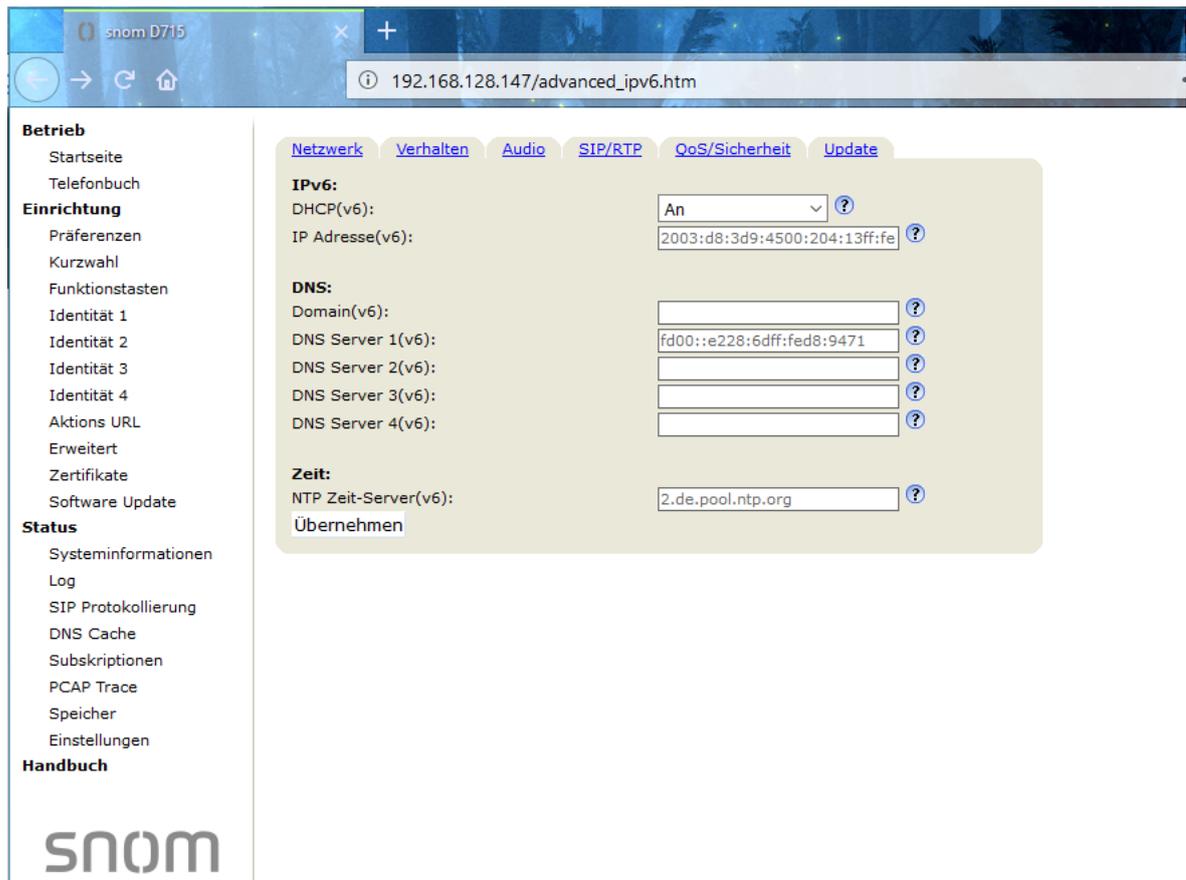


Abbildung 38: IPv6-Einstellungen eines snom715

Beim Booten des Geräts werden die erhaltenen IP-Adressen im Display angezeigt. Allerdings reicht die Anzeige für die Darstellung der IPv6-Adresse nicht aus, und es gibt auch nicht die Möglichkeit, am Gerät zu blättern, sodass eine vollständige Anzeige nicht möglich war.

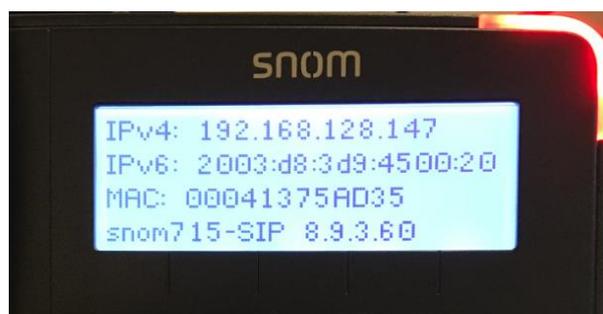


Abbildung 39: Bootscreen snom715

Bei der Konfiguration des SIP-Kontos erwartet das Telefon einen DNS-Alias oder eine IP-Adresse. Die Eingabe des Servers als DNS-Name wird empfohlen. IPv6-Adressen können zwar ebenfalls angegeben werden (unbedingt in eckigen Klammern), jedoch verursacht man dabei neue Probleme, denn die Anbieter wie sipgate wechseln durchaus gelegentlich die IP-Adressen ihrer Services oder nutzen LoadBalancer. Die Eingabe eines DNS-Namens

wäre also obligatorisch – führt aber bei snom zu dem bekannten DNS-Problem (siehe Abschnitt 3.2.3 - Das DNS-Problem bei den ITSP). Deshalb ist das Telefon nur im Dual-Stack-Betrieb uneingeschränkt zu empfehlen. Dann wird die Übertragung mit IPv6 auch bevorzugt (Trotz Auflösung mithilfe IPv4).

Rufaufbau, Mediapstreaming und Rufbeständigkeit über den Präfixwechsel hinweg stellen keine Probleme für das Telefon dar. Zusatzprotokolle wie der Abruf eines Telefonbuchs von einem FTP-Server via IPv6 oder die Synchronisation der Uhrzeit mittels IPv6 funktionierten ebenfalls.

### Grandstream

Das amerikanische Unternehmen stellt seit 2002 SIP-Telefone her und erfreut sich vor allem auf dem amerikanischen Markt einiger Beliebtheit. Zum Testen stand ein etwas älteres Modell zur Verfügung, ein GXP1450, welches laut Herstellerangaben eines der ersten Serien mit IPv6-unterstützung darstellt. Die vorliegende Firmwareversion 1.0.8.9 zeigt auch entsprechende Einträge. Besonders ist, dass bei Grandstream IPv6 grundsätzlich (neben IPv4) aktiviert ist,



Abbildung 40: GXP1450

und der Nutzer es nicht abstellen kann. Man kann ausschließlich eine Präferenz festlegen, welches Protokoll das Telefon bevorzugt nutzen soll. Damit erreicht man das Telefon auch bereits nach der Inbetriebnahme in einem IPv6-only-Netzwerk problemlos.

Allerdings: auch das Grandstream GXP1450 hat (wie das snom715) eine IP-Anzeige am Display die zu kurz und nicht scrollbar ist. Man muss also zwangsläufig mit anderen Methoden die IPv6-Adresse herausfinden.

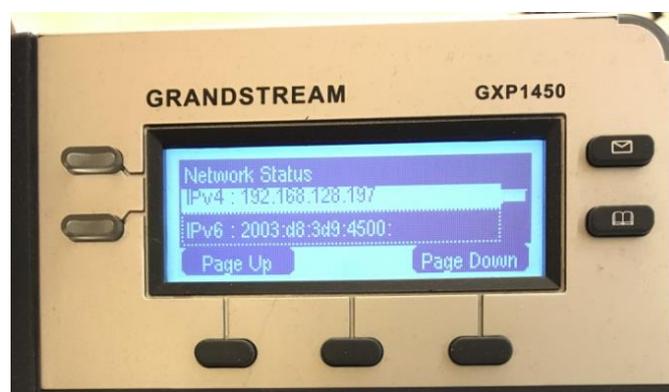


Abbildung 41: IP-Anzeige des Grandstream GXP1450

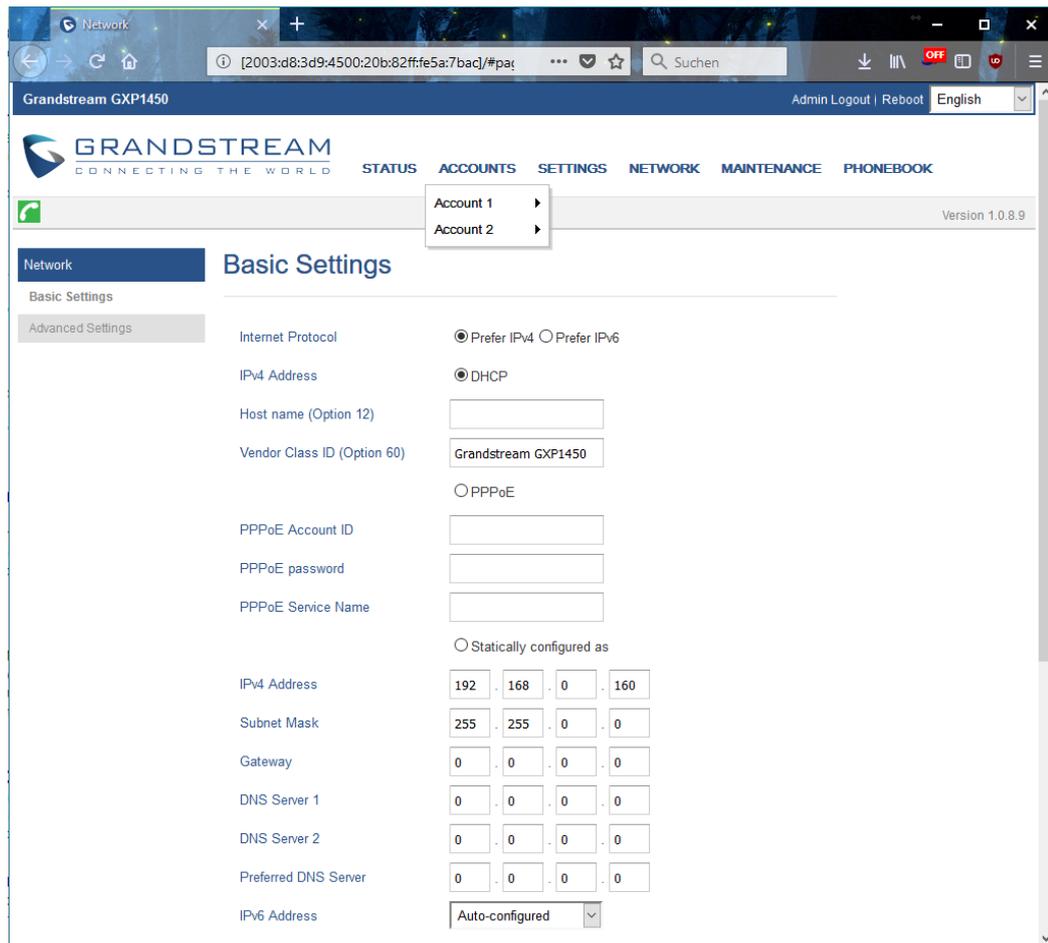


Abbildung 42: Grandstream GXP1450, Netzwerkkonfiguration

Das Webinterface ist grundsätzlich über IPv6 erreichbar. Wer die Adresse über den Router herausfinden kann, der benötigt IPv4 zur Konfiguration des GXP1450 nicht.

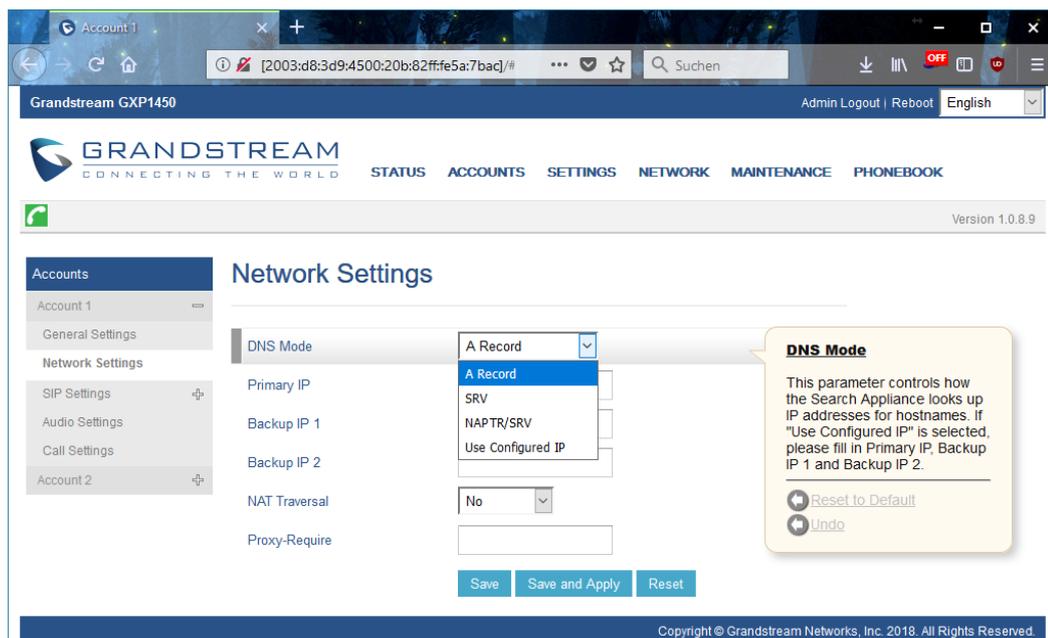


Abbildung 43: Auswahl des DNS-Modus beim GXP1450

Normalerweise gäbe es bei Grandstream ebenfalls das DNS-Problem aus Abschnitt 3.2.3 - *Das DNS-Problem bei den ITSP*. Grandstream nutzt genauso wie die Konkurrenz im Auslieferungszustand die SRV-Methode, für welche kurzzeitig IPv4 benötigt wird. Jedoch gibt es in der SIP-Konten-Konfiguration die Möglichkeit weitere Verfahren auszuwählen. Mit dem DNS-Modus „A-Record“ kann man das Problem sehr gut umgehen, dann löst das Telefon bei bevorzugter IPv6-Nutzung auch AAAA-Records auf und kann sich dort registrieren.

Der Rufaufbau, Mediastreaming und die üblichen Anruffunktionen Makeln bzw. Konferenz funktionieren ohne Probleme. Auch den Präfixwechsel überstehen die Gespräche.

Zusätzliche Funktionen wie ein Update über IPv6 oder der Abruf eines FTP-Telefonbuchs über IPv6 waren möglich. Nur die Synchronisation der Uhrzeit mittels NTP und IPv6 schlug fehl. Dies scheint ein Bug der aktuellen Firmware zu sein.

Das Telefon hat zwar nicht die modernste Optik, überzeugt aber mit der Funktionalität und kann aufgrund des werksseitig aktivierten IPv6-Protokolls und der anpassbaren DNS-Methode als einziges Hardwaretelefon im Test auch für IPv6-Only-Netzwerke eingesetzt werden.

#### **Alternative: DECT-Endgeräte an AVM Fritz!Box**

Die Basisstationen der DECT-Endgeräte des in Deutschland sehr verbreiteten Herstellers *gigaset* unterstützen aktuell IPv6 noch nicht. Nur für die teuren MultiCell-fähigen Profi-Basisstationen hat *gigaset* bisher Ankündigungen getätigt. Angesichts der Preisstruktur (jedes System besteht aus mindestens einer Master- und einer Slave-Zelle, der erste Master kostet bereits über 600€) und aufgrund unserer Anforderungen für den SOHO-Bereich schließen wir die Profi-Serie an dieser Stelle allerdings aus.

Eine ungewöhnlichere, aber für den SOHO-Einsatz durchaus sinnvolle Möglichkeit besteht darin, statt der mitgelieferten DECT-Basisstationen eine AVM Fritz!Box einzusetzen und die Mobilteile daran zu betreiben. AVM pflegt eine Partnerschaft mit *gigaset* und unterstützt deren Mobilteile auf DECT-Basis nahezu vollumfänglich. Ebenfalls unterstützt die Fritz!Box auch IPv6 (wie bereits im Router-Test ermittelt). Um die DECT-Funktionen zu erhalten, muss eine Fritz!Box der Fon-Serie ausgewählt werden. Dann besteht die Möglichkeit, im Menü „eigene Rufnummern“ ein SIP-Konto anzulegen, welches die Fritz!Box anschließend beim angegebenen ITSP registriert und an den lokalen Schnittstellen zur Verfügung stellt. Statt eines DECT-Mobilteils kann aber auch ein analoges Endgerät angeschlossen werden. Dies ist besonders für Faxgeräte nützlich.

Bei der Registrierung über IPv6 nutzt die Fritz!Box das empfohlene Verfahren mit der SRV-Record-Methode. Auch Sie kann die Namensauflösung nur mittels kurzzeitiger Verfügbarkeit von IPv4 lösen. Da aktuell jedoch noch keine IPv6-only-Internetanschlüsse am Markt verbreitet sind scheint dieses Problem erträglich. Alle anderen Anschlussarten mit Dual-Stack, DS-Lite oder auch anderen Tunneltechnologien können natürlich die DNS-Auflösung über IPv4 leisten.

Abbildung 44: SIP-Client-Konfiguration auf einer Fritz!Box 7490

Bei der Einrichtung des SIP-Kontos kann das bevorzugte Kommunikationsprotokoll entsprechend eingestellt werden. Ein Umgehen des DNS-Problems durch Hinterlegung der IPv6-Adresse des Registrars ist ebenfalls möglich, wenn auch nicht unbedingt erwünscht. Telefonate konnten problemfrei aufgebaut, mit entsprechendem Mediastreaming geführt, vermittelt und zu Konferenzen zusammengeführt werden. Probleme beim Präfixwechsel konnten nicht festgestellt werden, die Gespräche überstanden den Vorgang. Die Ermittlung, ob die Fritz!Box auch tatsächlich das IPv6-Protokoll nutzt, konnte durch eine zweite, vorgeschaltete Fritz!Box nachgewiesen werden. Diese Variante bietet sich in SOHO-Netzwerken tatsächlich besonders an, da mit preisgünstigen Mitteln ein gutes Ergebnis erzielt werden kann.

## Ergebnisse hardwarebasierte Clients

	unify Openstage 15	snom715	Grandstream GXP1450	AVM Fritz!-Box Fon 7490
Version	V3R0.3.0	8.9.3.60	1.0.8.9	06.93
Unterstützung von IPv6 (Herstellerangabe)	✓	✓	✓	✓
Unterstützung von Standard-SIP	✓	✓	✓	✓
IPv6 werksseitig aktiviert (damit Konfiguration bereits ohne IPv4 möglich)	✗	✗	✓	✓
<b>Registrierung</b>				
DNS-Auflösung des Registrar-Servers über IPv6	✗	✗	✓	✗
IPv6-Kommunikation durch Angabe der IPv6-Adresse als Server	✗	✓	✓	✓
Registrierung über IPv6-Protokoll	✗	✓	✓	✓
Beständigkeit der Registrierung über Präfixwechsel hinweg	✗	✓	✓	✓
<b>Telefonieren</b>				
Rufaufbau über IPv6-Protokoll	✗	✓	✓	✓
beidseitiges Mediastreaming über IPv6	✗	✓	✓	✓
Fortführung des Gesprächs bei Präfixwechsel	✗	✓	✓	✓
<b>Komfort-Funktionen</b>				
Makeln, Halten,	✗	✗	✓	✓
Verbinden, Konferenzen	✗	✗	✓	✓
FTP-Telefonbuch über IPv6 abrufen	✗	✓	✓	✗
NTP-Synchronisation über IPv6	✗	✓	✗	✓
Firmware-Update über IPv6	✗	✓	✓	✓
Gesamtwertung: <b>Eignung für DualStack</b>	✗	✓	✓	✓
Gesamtwertung: <b>Eignung für IPv6_only</b>	✗	✗	✓✓	✗

Tabelle 8: Ergebnisse hardwarebasierte Clients

**Aufgrund der auswählbaren DNS-Methode kann das Grandstream-Telefon als einziges für den IPv4-losen Betrieb empfohlen werden. Alle anderen Geräte benötigen zumindest übergangsweise noch IPv4. Die Anschaltung einer Fritz!Box als IP-Gateway stellt eine ergänzende sinnvolle Lösung dar – v.A. für Faxgeräte und DECT-Mobilteile.**

## 4 Best Practice

### 4.1 Beispielnetzwerk IPv6

In den verschiedenen Tests stellten sich verschiedene Produkte als besser geeignet heraus, als andere. In diesem Abschnitt wird ein Netzwerk skizziert, welches versucht die besten Produkte miteinander zu kombinieren. Die Betrachtung ist rein theoretisch, da natürlich im praktischen Einsatz unterschiedliche Anforderungen gelten. Aber die skizzierte Umgebung gibt einen Ansatz für eine praktische Umsetzung in einem kleingewerblichen Umfeld und erläutert dessen Umsetzung.

#### **Basisentscheidung zum Migrationsszenario**

Gemäß den Erfahrungen mit den Diensteanbietern (Abschnitt 3.2 - *Diensteanbieter (ASP)*) wird ein DualStack-Netzwerk aufgebaut. Das IPv6-Protokoll soll bereits bevorzugt verwendet werden, um soweit wie möglich auf einen späteren Ausstieg aus IPv4 vorbereitet zu sein.

#### **Internetanschluss**

Der Provider 1&1 stellt einen IPv6-fähigen VDSL-Anschluss zur Verfügung. Der Anschluss bietet DualStack-Technologie und stellt ein etwa alle 48h wechselndes /56er IPv6-Präfix zur Verfügung. Zusätzlich wird eine ebenfalls alle 48h wechselnde dynamische IPv4-Adresse zugeordnet.

#### **Router**

Wir setzen eine Fritz!Box 7490 ein. Der Router ist bereits im Umfang des Internetanschlusses enthalten. Die Basiseinrichtung erfolgt durch Provisionierung des Anbieters am eigenen Netz.

Die Einrichtung von DynDNS-Diensten erfolgt in der Fritz!Box. Dabei ist sie in der Lage sowohl die IPv4- als auch die IPv6-Adresse beim DynDNS-Anbieter zu aktualisieren.

```
C:\Users\Robert>nslookup fn6.dyndns.org
Server:   fritz.box
Address:  fd00::e228:6dff:fed8:9471

Nicht autorisierende Antwort:
Name:     fn6.dyndns.org
Addresses: 2003:d8:3bf:1907:e228:6dff:fed8:9475
          79.197.147.11
```

Abbildung 45: DynDNS-Records einer Fritz!Box an DualStack-Anschluss

Diese Einrichtung ermöglicht später die Nutzung anderer Dienste (z.Bsp. eines NAS im Netzwerk) von außen. Für unser VoIP-Konzept benötigen wir DynDNS nicht.

Die Zeitsynchronisation des Servers wird auf *2.de.pool.ntp.org* umgestellt (sonst klappt sie nach einer möglichen Deaktivierung von IPv4 nichtmehr).

Der DHCPv6-Server der Fritz!Box wird aktiviert. Theoretisch würde die Verteilung des Präfixes und des DNS-Servers als Router-Advertisement [RFC5006] ausreichen, aber durch die Verwendung des DHCPv6 kann die Fritz!Box bessere Übersichten des LANs darstellen und Firewallregeln für einzelne Clients erstellen.

ULA-Adressen soll die Fritz!Box immer verteilen (dann ist das interne Netz unabhängig vom Internetanschluss). Dadurch können intern eigene Adressbereiche aufgebaut werden. Dies ist besonders praktisch, wenn das Netzwerk aus mehreren Standorten bestehen soll. Das ULA-Präfix wird festgelegt auf *fd00::/64* – andere Standorte benötigen abweichende Präfixe.

### Clients

Aktuelle Betriebssysteme haben IPv6 bereits aktiviert. Aufgrund der Einrichtung der Fritz!Box werden Präfixe und DNS-Server über Router-Advertisements oder DHCPv6 korrekt an die Clients übermittelt. Diese erhalten somit automatisch die richtige Konfiguration. Neben der IPv4-Adresse sollte sich beim Prüfen der Netzwerkkarten (z.Bsp. *ipconfig*) mind. eine globale IPv6-Adresse und eine lokale ULA-IPv6-Adresse (*fd00:...*) finden. Das Vorhandensein temporärer IPv6-Adressen lässt sich auf die zusätzliche Lifetime nach einer Umnummerierung zurückführen.

```
Ethernet-Adapter Ethernet:

Verbindungsspezifisches DNS-Suffix: fritz.box
IPv6-Adresse. . . . . : 2003:d8:3d9:600:9443:1eec:b7fe:3990
Temporäre IPv6-Adresse. . . . . : 2003:d8:3d9:600:d051:b2eb:d74f:7560
Verbindungslokale IPv6-Adresse . : fe80::9443:1eec:b7fe:3990%2
IPv4-Adresse . . . . . : 192.168.128.154
Subnetzmaske . . . . . : 255.255.255.0
Standardgateway . . . . . : fe80::e228:6dff:fed8:9471%2
                            192.168.128.254
```

Abbildung 46: *ipconfig* an einem PC im Testnetz

Weitere Clients können im Netzwerk eingebunden werden. Dies können Mobiltelefone (z.Bsp per WLAN) oder auch NAS-Systeme o.Ä. sein. Smartphones mit aktuellen Betriebssystemen (z.Bsp. iOS, Android) haben IPv6 werksseitig aktiviert.

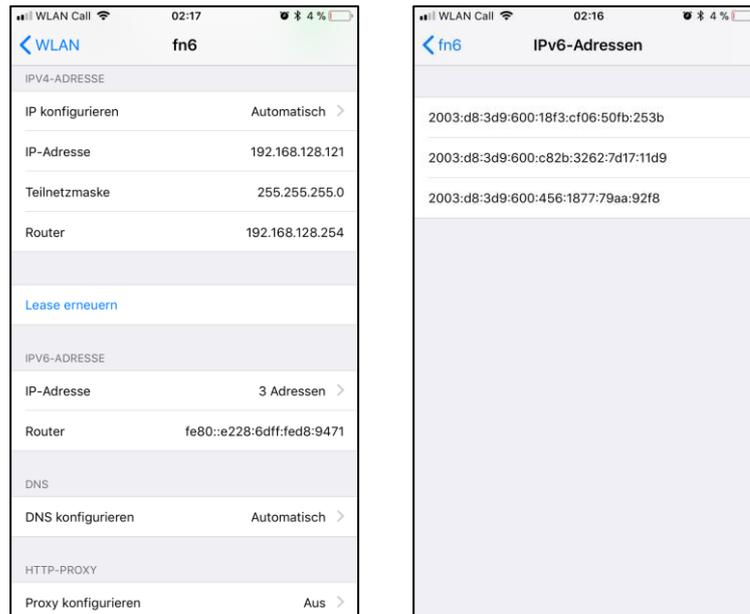


Abbildung 47: IPv6-Adressen auf einem iOS-Client

### Telefonsystem

Als Telefonsystem fällt die Entscheidung auf ein Cloud-PBX-System<sup>35</sup>. Es werden die Angebote des Anbieters sipgate verwendet. Sie haben sich als IPv6-fähig herausgestellt.<sup>36</sup> Je nach Anzahl benötigter Clients und Funktionen kann zwischen den Produkten *sipgate basic* bzw. *sipgate team* gewählt werden. Für die Einrichtung in unserem Netzwerk verhalten sich beide Varianten nahezu identisch, Sie unterscheiden sich nur im von sipgate angebotenen Funktionsumfang bei mehreren Teilnehmern.

Am Router selbst sind keine Einstellungen nötig. Durch die regelmäßigen REREGISTER der Telefone bleiben die nötigen SIP-Verbindungen in der SPI-Firewall der Fritz!Box beständig offen.

Als Softwareclient empfiehlt sipgate das Produkt ZoIPer, welches als nicht IPv6-fähig eingestuft werden musste. Als Alternative wird Linphone genutzt. Aufgrund der DualStack-Konfiguration stellt die problematische DNS-Auflösung keine Hürde dar. Ansonsten funktionierte LinPhone tadellos. Der Softwareclient ist aufgrund seiner Programmierung in Java auf allen Plattformen (Mac, Win, Linux) verfügbar. Auch Smartphone-Apps gibt es.

Als Telefon werden Grandstream GXP1450 eingesetzt. Die Geräte haben IPv6 in der Grundkonfiguration bereits aktiviert.

<sup>35</sup> Im Folgenden wird auch noch eine Alternative dargestellt. Siehe dazu Abschnitt 4.3 - Selfhosted PBX – die eigene, cloudbasierte IP-PBX

<sup>36</sup> Vgl. Tests aus Abschnitt 3.2.2 - Internettelefonieanbieter (ITSP)



## 4.2 Sicherheit

Unter IPv4 wird heute zumeist NAT eingesetzt, was aufgrund seiner Architektur selbst bereits eine Art Firewall-Funktion bietet, da von außen erstmal nichts einfach so in das Netzwerk hineinkommt. Unter IPv6 entfällt diese Sperr-Funktion von NAT.

IPv6-Netze und -Rechner benötigen daher wenigstens eine Firewall, die unerwünschte Gäste fernhält.

### **Firewalls im Router:**

Die einfachste Art, unerwünschten Datenverkehr aus dem Netzwerk zu halten, ist eine wirkungsvolle Firewall bereits im Router. Dass diese auch für IPv6 funktionieren muss ist obligatorisch. Sperrt die Firewall unerwünschten eingehenden Verkehr (Standard: Alles) dann erfüllt sie damit bereits dieselbe Wirkung, die NAT für die Sicherheit des internen Netzes hat. Aktuelle Routermodelle setzen zusätzlich eine Stateful Inspection Firewall (SPI) ein. Diese kontrolliert ein- und ausgehende Datenpakete und weist nicht angeforderte Daten aus dem Internet automatisch ab. Damit sorgt sie dafür, dass nur direkte Antworten auf zuvor angeforderte Anfragen zugelassen werden.

Ein eingehender Anruf wird allerdings immer durch ein zuvor nicht angefordertes Datenpaket eingeleitet. Wäre dem nicht so, müsste der SIP-Client fortwährend den Server anfragen, ob ein neuer Anruf für ihn vorliegt. Dies wäre ein wenig sinnvolles Kommunikationskonzept. Deshalb muss sich unter SIP ein Client regelmäßig beim Server neu registrieren (REREGISTER). Dies hilft nicht nur dem Server zu wissen, dass der Client noch erreichbar ist, sondern es hält auch die Kommunikationskanäle in der SPI-Firewall der Router offen. Damit ist ein SIP-INVITE für ein Gespräch, welches der Server sendet, automatisch eine Antwort innerhalb der bestehenden Kommunikation. Administrativ muss nur sichergestellt werden, dass die wiederholenden Registrierungen des Clients schneller passieren, als der Verbindungstimeout der SPI-Firewall die Verbindungen wieder schließt. Bei Problemen mit Abbrüchen in der Serverkommunikation der SIP-Clients, liegt der Fehler oft an einem zu schnellen Timeout oder zu langsamer Reregistrierung. Dieses Verhalten gilt sowohl unter IPv4 als auch unter IPv6.

Unter IPv4 muss sich die SPI-Firewall der Router nicht nur merken, welche Kommunikationspartner miteinander Verbindungen halten, sondern sie muss eintreffende und ausgehende Pakete auch umadressieren (NAT/Masquerading). Das muss die IPv6-Firewall nicht machen, was ihr einen kleinen Geschwindigkeitsvorteil verschafft.

### Firewalls in den Betriebssystemen:

Unter **Windows** ab Vista, Windows Server ab 2003 sowie Windows XP (SP2) filtert die eingebaute Desktop-Firewall den Netzwerkverkehr für IPv6, was Hersteller Microsoft ausdrücklich wegen möglicher Viren- und Trojaner-Attacken empfiehlt.

Auf Apples **Mac OS X** ab Version 10.5 schützt eine neue von Apple selbst entwickelte Application Firewall<sup>37</sup> das Betriebssystem. Gleichzeitig steht auch der Paketfilter *ipfw*<sup>38</sup> bereit, der ausschließlich per Konsole bedient wird und den das aktuelle Mac OS X kaum nutzt.

**Linux-Systeme** filtern den IPv6-Datenverkehr meist über das Programm *ip6tables*, welches die Funktion *Connection-Tracking* unterstützt. Mit dieser Funktion lässt sich eine IPv6-SPI-Firewall realisieren, die den gleichen Sicherheitslevel bietet wie ein IPv4-NAT-Routing. Linux-Systeme vor Version 2.6.20 beherrschen die Verbindungsüberwachung (Connection-Tracking) in der *ip6tables*-Firewall noch nicht.

Beispiel für die Konfiguration einer IPv6-SPI-Firewall unter Linux (auf einem Host, nicht auf einem Router):

```
ip6tables -P INPUT ACCEPT
ip6tables -P FORWARD ACCEPT
ip6tables -P OUTPUT ACCEPT
ip6tables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
ip6tables -A INPUT -p tcp -dport 22 -j ACCEPT
```

Der Aufruf `ip6tables -A INPUT -p tcp -dport 22 -j ACCEPT` öffnet einen Port, um von aussen auf das System per SSH zugreifen zu können.

Der Aufruf `ip6tables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT` schaltet für eingehende Pakete das Connection-Tracking ein. Dadurch werden die Verbindungen von der Firewall beobachtet, die der Rechner in das Internet aufbaut. Antworten auf diese Anfragen werden von der Firewall durchgelassen, nicht angeforderte Pakete werden verworfen.

---

<sup>37</sup> Vgl. dazu Apple Produktinformation <https://support.apple.com/de-de/HT201642>

<sup>38</sup> Vgl. <https://www.freebsd.org/cgi/man.cgi?query=ipfw&sektion=8>

### 4.3 Selfhosted PBX – die eigene, cloudbasierte IP-PBX

Für findige Technikfreunde werden heute viele Produkte angeboten, die mit dem nötigen KnowHow zu sehr interessanten Diensten konfiguriert werden können. So kann man sich beispielsweise eine eigene, cloudbasierte Telefonanlage mit IPv6-Support zusammenstellen und diese betreiben (lassen). So erhält man mehr Einfluss auf das eigene Telefonie-Produkt, als es die üblichen Cloudtelefonie-Anbieter am Markt zulassen. Eine Erläuterung zum Prinzip sowie eine kurze Anleitung zur Inbetriebnahme ist im Folgenden zu finden.

#### 4.3.1 vServer

WebHosting-Anbieter stellen heute ganze Server inkl. dem Root-Zugriff auf das Betriebssystem des Servers kostengünstig zur Verfügung. Diese Server werden aus Kostengründen meist als virtuelle Server<sup>39</sup> realisiert. Die Produkte tragen dann oft den Titel „vServer“ oder „VPS“ (Virtual Private Server) im Namen.

Eine Softwaretelefonanlage (IP-PBX) benötigt vergleichsweise wenige Ressourcen, dadurch können Angebote mit Einstiegs-Produkten für diese Aufgabe verwendet werden. So kann man bereits für einen Mietpreis von unter 5€ pro Monat einen Server mieten, der durch einen Hosting-Provider bereitgestellt und fertig an das Internet angebunden wurde.

**Wichtig:** bei der Auswahl des vServer-Produktes sollte natürlich darauf geachtet werden, dass der Anbieter zu dem Paket auch eine IPv6-Adresse anbietet. Leider ist das derzeit noch bei den wenigsten Anbietern der Fall.

Der Hosting-Anbieter OVH bietet ein interessantes Angebot<sup>40</sup>. Es handelt sich um ein VPS-System mit 2,4GHz CPU-Takt, 2GB RAM, 10GB SSD-Speicher und sowohl einer IPv4-Adresse, als auch einer IPv6-Adresse. Die Betriebssystemauswahl fällt auf Debian 9 (Anforderung des 3CX-PBX-Systems).

Nach der Bestellung ist das Produkt innerhalb 10-20 Min. durch OVH bereitgestellt. Die IPv6-Adresse ist zwar zugeteilt, jedoch liefert OVH das System ohne eingerichtete IPv6-Adresse. Dies muss nachgeholt werden, bevor der Server per IPv6 erreichbar ist<sup>41</sup>.

---

<sup>39</sup> Virtualisierung: Trennung von Betriebssystem/Applikation und Hardware durch Einführung eines Hypervisors, der die verfügbare Hardware verwaltet und für jedes Gastbetriebssystem simuliert. Dadurch können mehrere Server auf ein- und derselben Hardware betrieben werden.

<sup>40</sup> [https://www.ovh.de/virtual\\_server/vps-ssd.xml](https://www.ovh.de/virtual_server/vps-ssd.xml)

<sup>41</sup> [https://www.ovh.com/world/g2365.configure\\_ipv6\\_on\\_your\\_vps](https://www.ovh.com/world/g2365.configure_ipv6_on_your_vps)

Der Server selbst ist per SSH erreichbar, die Zugangsdaten erhält man im Bestellprozess. Ein „ifconfig“ zeigt die Namen der Netzwerk-Interfaces, in diesem Fall ens3.

Um dem Interface eine feste IPv6-Adresse (die korrekte ist im Kundencenter zu finden) einzurichten, muss die Datei /etc/network/interfaces um folgende Zeilen ergänzt werden, wobei die IPv6-Adressen von VPS selbst und zugehörigem Gateway entsprechend anzupassen sind:

```
iface ens3 inet6 static
address 2001:41d0:401:3100::2ab3
netmask 128
post-up /sbin/ip -6 route add 2001:41d0:401:3100::1 dev ens3
post-up /sbin/ip -6 route add default via 2001:41d0:401:3100::1 dev
ens3
pre-down /sbin/ip -6 route del default via 2001:41d0:401:3100::1 dev
ens3
pre-down /sbin/ip -6 route del 2001:41d0:401:3100::1 dev ens3
```

Nach einem Neustart erreicht man dann die VPS auch mittels IPv6-Protokoll. Hat man sich per SSH auf die Maschine verbunden, dann kann man natürlich auch andere Host mittels IPv6 erreichen, z.Bsp:

```
ping6 ipv6.google.com
```

```
root@vps447624:~# ping6 ipv6.google.com
PING ipv6.google.com(parl0s33-in-x0e.l100.net (2a00:1450:4007:816::200e)) 56 data bytes
64 bytes from parl0s33-in-x0e.l100.net (2a00:1450:4007:816::200e): icmp_seq=1 ttl=52 time=6.49 ms
64 bytes from parl0s33-in-x0e.l100.net (2a00:1450:4007:816::200e): icmp_seq=2 ttl=52 time=6.51 ms
^C
--- ipv6.google.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 6.491/6.503/6.515/0.012 ms
```

Abbildung 49: Ergebnis IPv6-Ping an ipv6.google.com

Nun ist die VPS bereit für die Installation einer IP-PBX-Software.

### 4.3.2 IP-PBX-Software

Zusätzlich zu dem Server wird eine Software-Telefonanlage benötigt. Diese gibt es von vielen Herstellern, mit unterschiedlichsten Funktionen, für unterschiedliche Betriebssysteme und mit unterschiedlichsten Preismodellen. Nennenswert ist hier sicherlich Asterisk – eine freie Software, die ursprünglich von Mitarbeitern der Firma Digium entwickelt wurde und deren Quellcode offen zugänglich ist. Asterisk bietet Unterstützung für Sprachdienste und viele Funktionen einer Telefonanlage. Die Software ist unter der GPL<sup>42</sup> veröffentlicht und wird deshalb in vielen Distributionen angeboten. (digium, FreePBX, usw.). Der Hersteller 3CX bietet ebenfalls eine Software-PBX an, die er

<sup>42</sup> GPL: GNU General Public License - *allgemeine Veröffentlichungserlaubnis* oder *-genehmigung*, verbreitete Softwarelizenz, die die Verbreitung, aber auch die Veränderung (unter Beibehaltung der Lizenz) erlaubt. Softwarehersteller können dadurch Software weiterentwickeln und proprietär anbieten, müssen aber die ursprünglichen Lizenzrechte beibehalten.

kommerziell vertreibt und die einen für KMU sehr interessanten Leistungsumfang bietet. Für kleine Systeme, bei denen nur Basisfunktionen benötigt werden, und für die bis zu 8 gleichzeitige Gespräche ausreichen, stellt der Hersteller sogar eine kostenfreie Version zur Verfügung. Diese ist ideal geeignet, um sie auf einem vServer zu installieren. Eine Unterstützung von IPv6 ist bei allen angebotenen Distributionen offiziell noch nicht vorhanden. Für das Produkt 3CX-FreePBX des gibt es jedoch bereits eine Alpha-Version, für die der Hersteller die Unterstützung von IPv6 bereits erklärt hat<sup>43</sup>.

Die Software kann über den Aptitude-Paketmanager auf Debian bereitgestellt werden.

```
wget -O- http://downloads.3cx.com/downloads/3cxpbx/public.key | apt-
key add -

echo "deb http://downloads.3cx.com/downloads/debian stretch-alpha
main" | tee /etc/apt/sources.list.d/3cxpbx.list

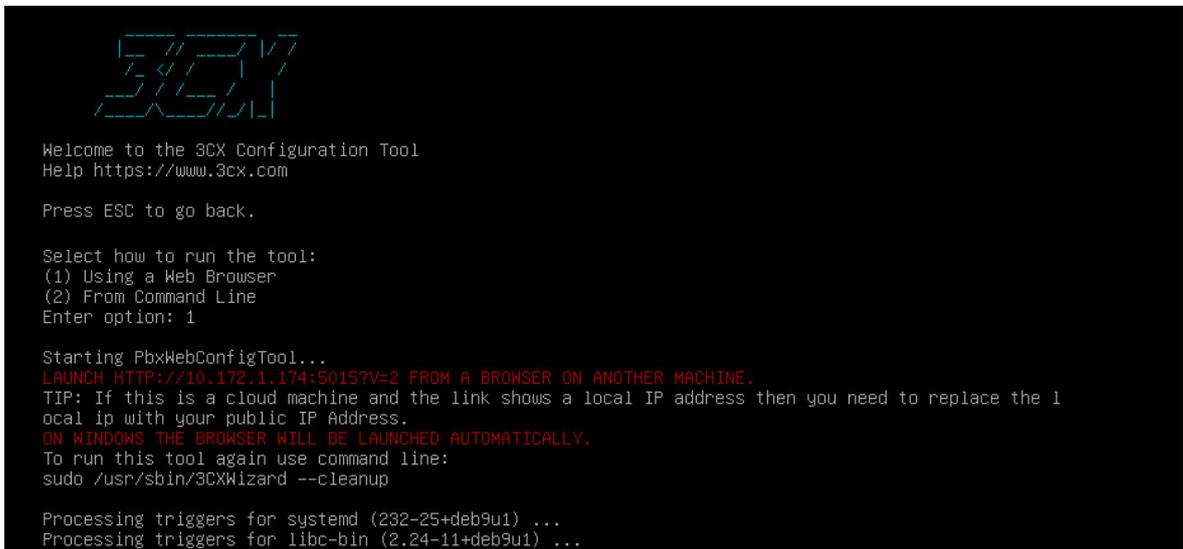
apt-get update

apt-get install libcurl3

apt-get install 3cxpbx

apt-get install net-tools
```

Alle Abhängigkeiten werden durch Aptitude installiert, der gesamte Vorgang verläuft relativ simpel. Nach erfolgter Installation wird darauf hingewiesen, dass die weitere Konfiguration des Systems über dessen Weboberfläche erfolgt<sup>44</sup>.



```

  3CX

Welcome to the 3CX Configuration Tool
Help https://www.3cx.com

Press ESC to go back.

Select how to run the tool:
(1) Using a Web Browser
(2) From Command Line
Enter option: 1

Starting PbxWebConfigTool...
LAUNCH HTTP://10.172.1.174:5015?V=2 FROM A BROWSER ON ANOTHER MACHINE.
TIP: If this is a cloud machine and the link shows a local IP address then you need to replace the l
ocal ip with your public IP Address.
ON WINDOWS THE BROWSER WILL BE LAUNCHED AUTOMATICALLY.
To run this tool again use command line:
sudo /usr/sbin/3CXWizard --cleanup

Processing triggers for systemd (232-25+deb9u1) ...
Processing triggers for libcurl3 (2.24-11+deb9u1) ...

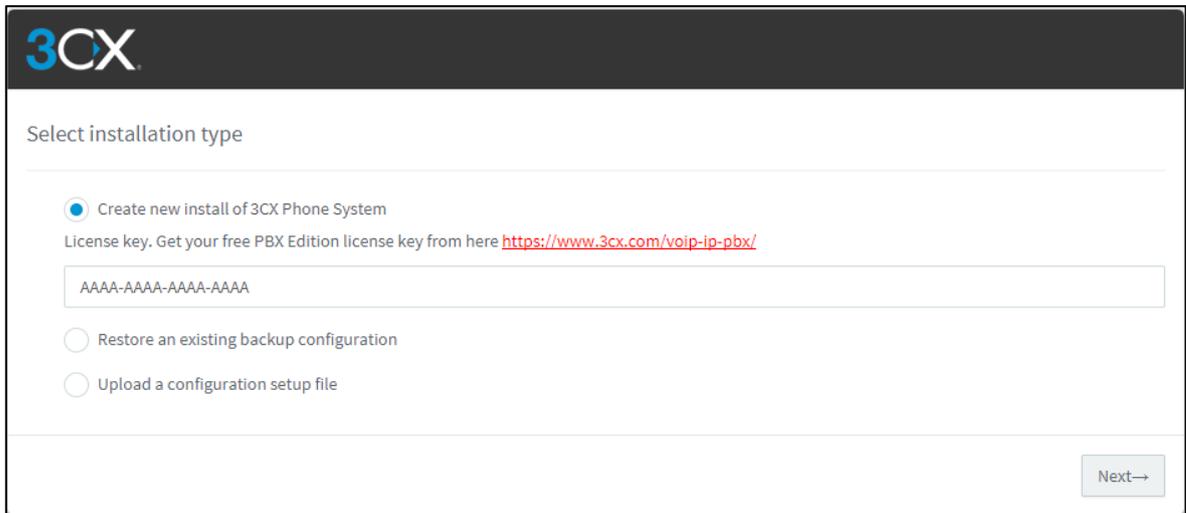
```

Abbildung 50: abgeschlossene 3CX-Grundinstallation

<sup>43</sup> <https://www.3cx.com/blog/releases/ip-pbx-update-alpha/>

<sup>44</sup> Die 3CX-Software installiert einen eigenen nginx-Webserver

Unter der Adresse öffnet sich das Konfigurationsprogramm für das PBX-System, welches zunächst eine Lizenz abfragt. Auch für die freie Version<sup>45</sup> mit bis zu 8 gleichzeitigen Gesprächen muss man sich registrieren und erhält einen eigenen Lizenzkey.



The screenshot shows the '3CX' logo at the top left. Below it, the title 'Select installation type' is displayed. There are three radio button options:
 

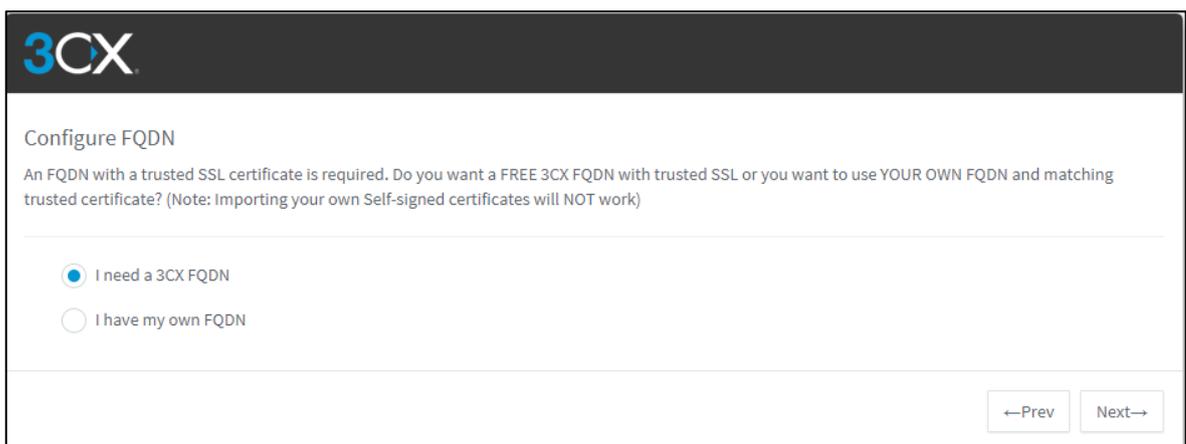
- Create new install of 3CX Phone System
- Restore an existing backup configuration
- Upload a configuration setup file

 Under the first option, there is a text input field containing 'AAAA-AAAA-AAAA-AAAA'. Above this field, the text reads: 'License key. Get your free PBX Edition license key from here <https://www.3cx.com/voip-ip-pbx/>'. A 'Next →' button is located at the bottom right of the form.

Abbildung 51: 3CX-Konfigurationsassistent

Im weiteren Verlauf werden wichtige Parameter wie ext. IP, Art der IP (stat./dyn.), lok. IP, Ports, Email-Konfiguration aber auch Kontaktdaten des Betreibers abgefragt.

Das System benötigt zum Betrieb ein gültiges SSL-Zertifikat und einen auflösbaren DNS-Namen. Als sehr hilfreich erweist sich, dass 3CX einen eigenen Service anbietet, mit dem Benutzern der Software beides bereitgestellt werden kann. Der Anwender erhält im Laufe des Verfahrens einen DNS-Namen der Form *mycompany.3cx.de* und ein gültiges Zertifikat. Bei Veränderungen der Erreichbarkeit (z.Bsp. dyn. IP) meldet die PBX-Software selbständig die neue IP an den FQDN-Service der 3CX und aktualisiert damit DNS-Eintrag und Zertifikat.



The screenshot shows the '3CX' logo at the top left. Below it, the title 'Configure FQDN' is displayed. The text below the title reads: 'An FQDN with a trusted SSL certificate is required. Do you want a FREE 3CX FQDN with trusted SSL or you want to use YOUR OWN FQDN and matching trusted certificate? (Note: Importing your own Self-signed certificates will NOT work)'. There are two radio button options:
 

- I need a 3CX FQDN
- I have my own FQDN

 At the bottom right, there are two buttons: '← Prev' and 'Next →'.

Abbildung 52: 3CX-Konfigurationsassistent (FQDN)

<sup>45</sup> Versionsvergleich: <https://www.3cx.de/ip-telefonanlage/funktionen-comparison/>

Mit der Fertigstellung des Assistenten wechselt man in die normale Administrationsoberfläche des IP-BX-Systems 3CX.

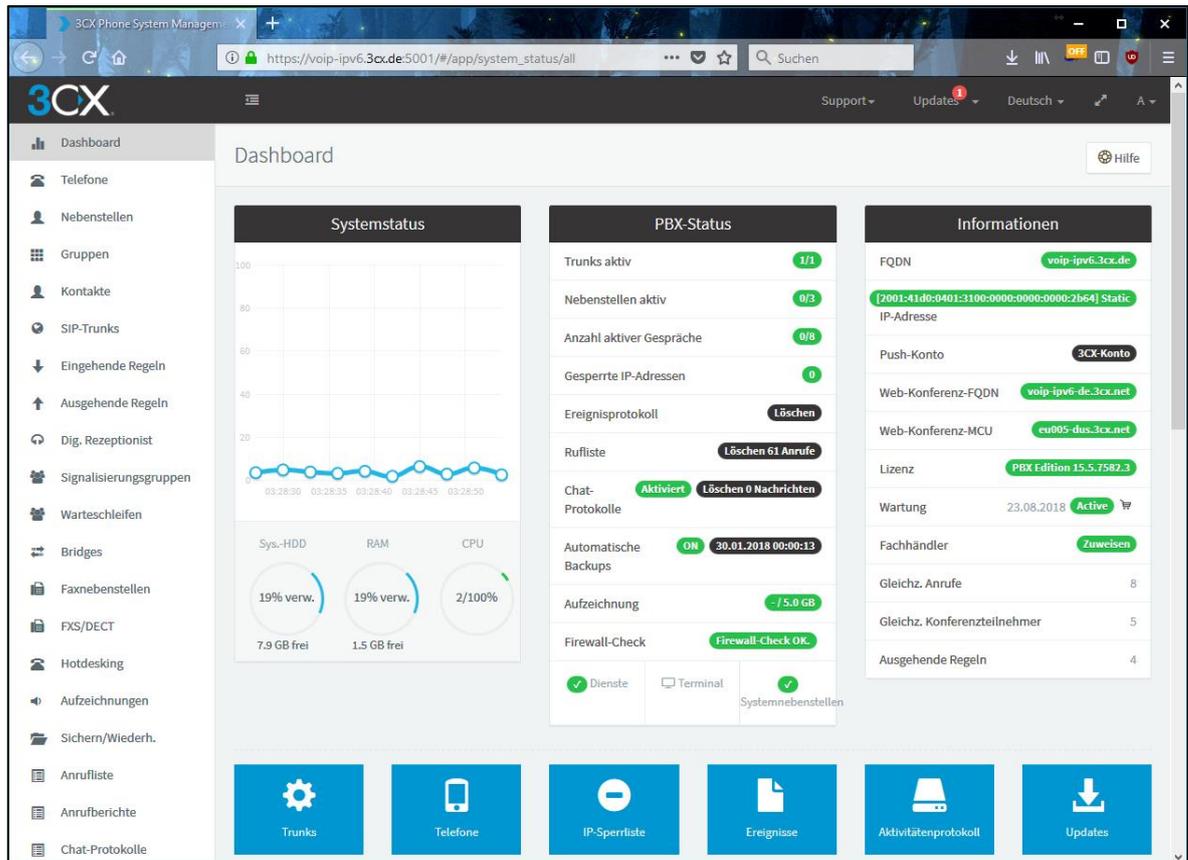


Abbildung 53: 3CX-webbasierter Konfigurationsmanager der selfhosted PBX

Das System ist nun grundsätzlich installiert. Die Oberfläche zeigt, dass von dem gebuchten VPS nur geringe Ressourcen verwendet werden. Weniger als 20% der vorhandenen Ressourcen werden genutzt. Auch im Dauerversuch und mit >10 dauerhaft angemeldeten Endgeräten konnten keine Situationen beobachtet werden, in denen das System ausgelastet war.

Nun kann mit der Einrichtung der Benutzer begonnen werden – die Hilfefunktion ist dabei sehr hilfreich, weshalb der Vorgang hier nicht weiter ausgeführt wird.

### 4.3.3 Client-Einrichtung

Nachdem die Benutzer am System eingerichtet wurden, muss man die Teilnehmer anbinden. Dies geschieht am einfachsten durch Installation der 3CX-Clientsoftware. Für die Konfiguration des Clients lässt sich direkt aus der Administrationsoberfläche eine Email versenden. In deren Anhang befindet sich eine Datei, die (wenn der 3CX-Client bereits installiert ist) beim Ausführen automatisch die richtige Konfiguration einspielt. Es ist aber

auch eine Anbindung der SIP-Telefone möglich. Zur Nutzung von IPv6 muss die IPv6-Serveradresse in eckigen Klammern eingegeben werden. Leider weist keine Fehlermeldung oder anderweitige Syntaxprüfung auf falsche Eingaben hin. Nach erfolgreicher Konfiguration kann man bereits interne Gespräche führen. Ist der Server als IPv6-Server eingetragen, nutzt der Client entsprechend das IPv6-Protokoll.

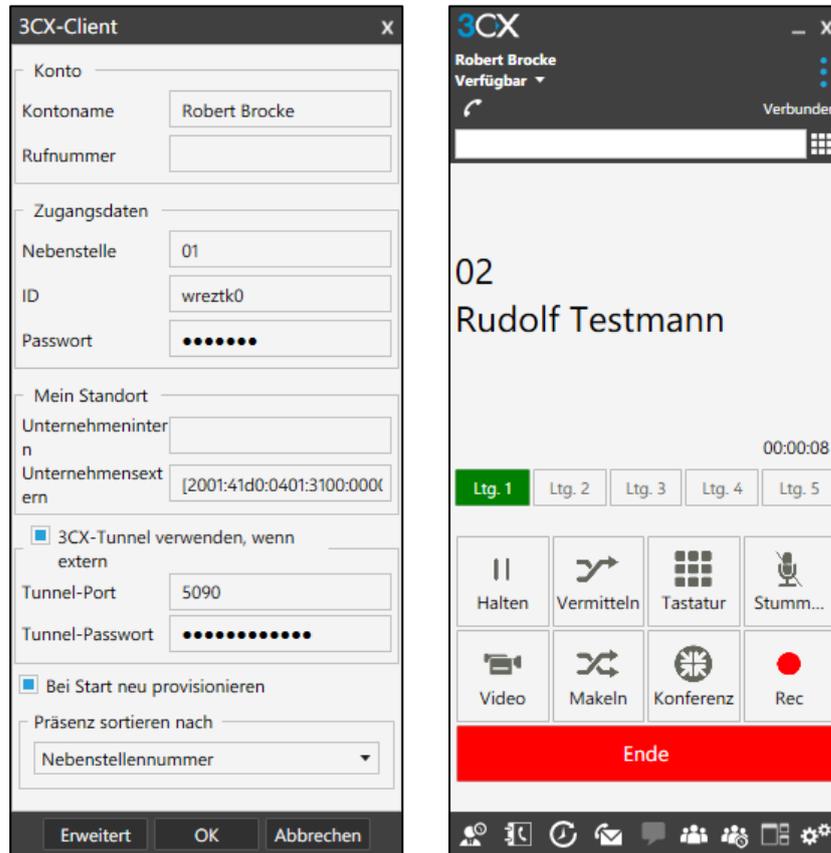


Abbildung 54: 3CX-Client - Kontoeinrichtung und Anruf

Ein Trace zeigt das der Anruf über IPv6 stattfand. Das Mediastreaming war in beiden Richtungen ungestört. Somit konnte VoIP-Telefonie auf ausschließlich IPv6-basierter Basis mithilfe einer eigenen Cloud-TK-Anlage realisiert werden.

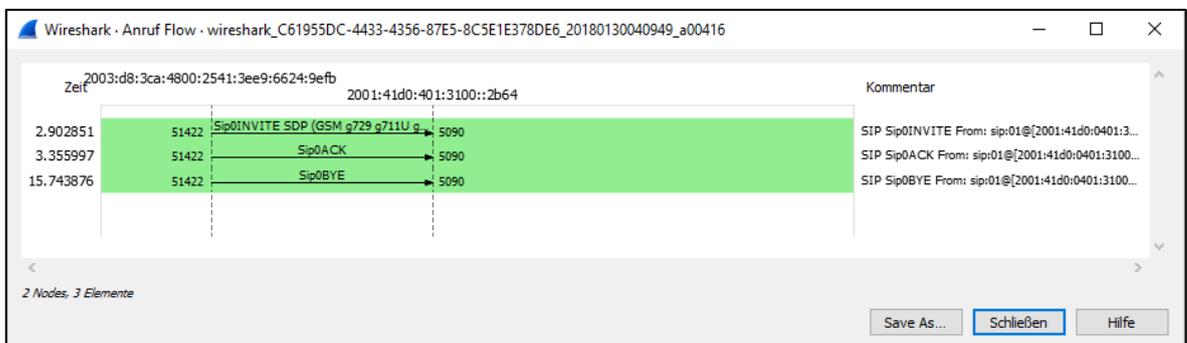
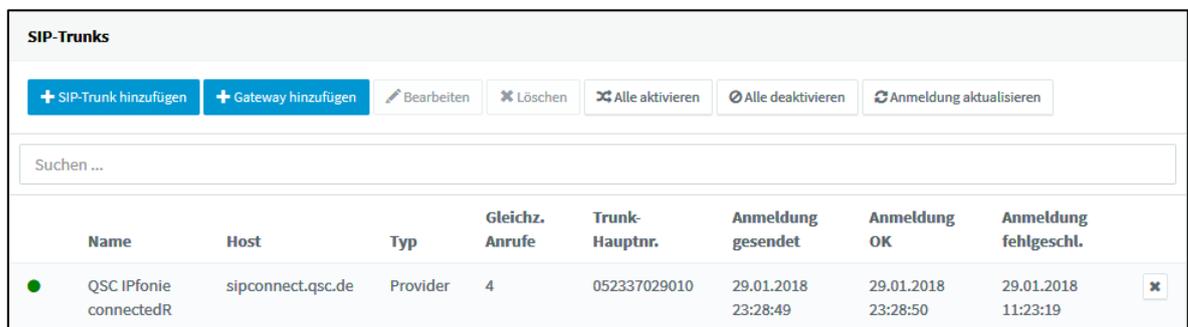


Abbildung 55: 3CX-Client-Trace eines internen Anrufes

### 4.3.4 SIP-Trunk

Ohne eine Anbindung an das öffentliche Telefonnetz kann man zwar intern untereinander an der Anlage telefonieren, jedoch hat man noch keine öffentlichen Telefonnummern. Dies erreicht man durch Beauftragung eines SIP-Trunks, der schließlich auf der selfhosted-PBX eingerichtet werden muss. Damit teilt ein Provider entsprechende Rufnummern aus dem beantragten Ortsnetz zu – diese können dann für die eigenen Nebenstellen verwendet werden. Durch die Nutzung des SIP-Trunks entstehen i.d.R. Gesprächsgebühren.

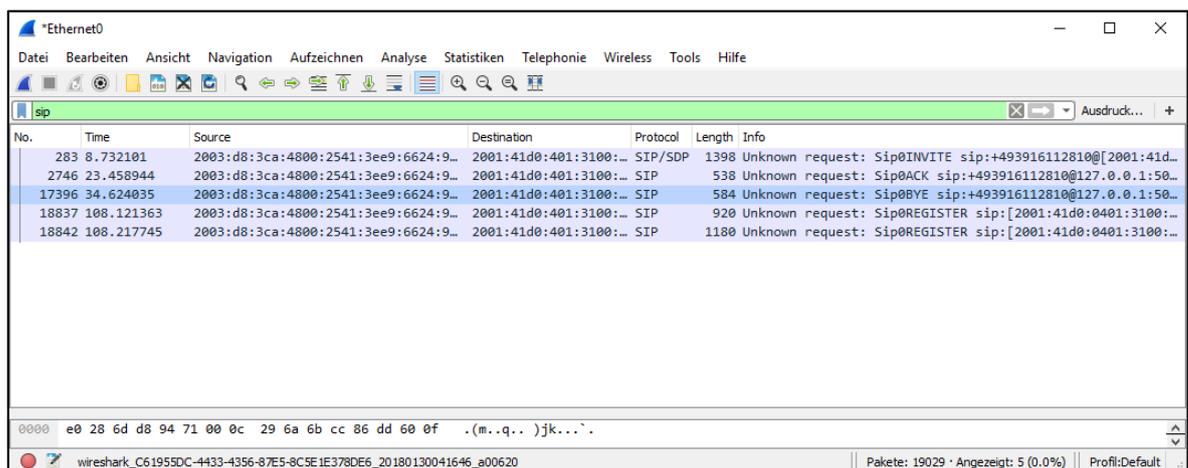
Der von 3CX empfohlene Internettelefonieanbieter **QSC** hat zu Evaluierungszwecken einen 4-Kanal-SIP-Trunk seines Produktes *QSC IPfonie extended connectR* zur Verfügung gestellt. Dieser wurde auf dem System eingerichtet.



Name	Host	Typ	Gleichz. Anrufe	Trunk-Hauptnr.	Anmeldung gesendet	Anmeldung OK	Anmeldung fehlgeschl.
QSC IPfonie connectedR	sipconnect.qsc.de	Provider	4	052337029010	29.01.2018 23:28:49	29.01.2018 23:28:50	29.01.2018 11:23:19

Abbildung 56: 3CX-SIP-Trunk-Einrichtung

Nach Zuordnung der Rufnummern zu einzelnen Benutzern und der Festlegung spezieller Regeln für eingehende und ausgehende Gespräche konnte nun das IP-PBX-System auch am PSTN verwendet werden.



No.	Time	Source	Destination	Protocol	Length	Info
283	8.732101	2003:d8:3ca:4800:2541:3ee9:6624:9...	2001:41d0:401:3100:...	SIP/SDP	1398	Unknown request: Sip0INVITE sip:+493916112810@[2001:41d...
2746	23.458944	2003:d8:3ca:4800:2541:3ee9:6624:9...	2001:41d0:401:3100:...	SIP	538	Unknown request: Sip0ACK sip:+493916112810@127.0.0.1:50...
17396	34.624035	2003:d8:3ca:4800:2541:3ee9:6624:9...	2001:41d0:401:3100:...	SIP	584	Unknown request: Sip0BYE sip:+493916112810@127.0.0.1:50...
18837	108.121363	2003:d8:3ca:4800:2541:3ee9:6624:9...	2001:41d0:401:3100:...	SIP	920	Unknown request: Sip0REGISTER sip:[2001:41d0:0401:3100:...
18842	108.217745	2003:d8:3ca:4800:2541:3ee9:6624:9...	2001:41d0:401:3100:...	SIP	1180	Unknown request: Sip0REGISTER sip:[2001:41d0:0401:3100:...

Abbildung 57: 3CX-Client-Trace bei Anruf an öff. Teilnehmer

Auch hier funktionierte die Nutzung von IPv6 problemfrei. Aufgrund des erhöhten Funktionsumfangs einer solchen Lösung gegenüber den SIP-Client-Produkten der typ. Anbieter wie sipgate, ist der Betrieb einer self-hosted-IP-PBX durchaus zu empfehlen.

## 5 Zusammenfassung und Ausblick

Die vorliegende Arbeit beschäftigte sich mit aktuell verfügbaren VoIP-Lösungen und deren Einsetzbarkeit im IPv6-Internet.

Es zeigte sich im Verlauf der Bearbeitung sehr schnell, dass für eine entsprechende Betrachtung immer die Vielzahl aller beteiligten Kommunikationspartner – vom Telefonieanbieter, über den Internetanschlussbetreiber, über Router und Heimnetzwerk bis hin zu den Clients – eine Rolle spielt. Alle müssen IPv6 unterstützen.

Dabei haben sich unterschiedliche Adaptionsgrade herausgestellt, die den Einsatz von IPv6 unterschiedlich empfehlenswert gestalten.

Schaut man auf die Internetprovider, so ist das IPv6-Internet bereits aktueller Stand der Technik. (Fast) Alle Provider bieten Lösungen für IPv6 an. Einige könnten sogar ohne das neue Protokoll keine Produkte anbieten. Die Mobilfunknetze der neueren Generationen wären ebenfalls undenkbar.

Die in dieser Arbeit im Fokus stehenden VoIP-Lösungen zeigen zwar, dass bei vielen Herstellern von Produkten und Anbietern von Diensten noch Nachholbedarf besteht, jedoch gibt es bereits marktreife Systeme im SOHO-Bereich, mit denen man IPv6 und VoIP gemeinsam realisieren kann. Eine hohe Dynamik bei der Adaption durch die Hersteller und Anbieter ist erkennbar. Tagtäglich kommen neue Versionen Firmware, Software oder Diensten heraus, die Verbesserungen in der IPv6-Integration versprechen.

Dagegen stehen allerdings am anderen Ende die Betreiber von Webseiten und Internetangeboten. Diese haben deutlichen Nachholbedarf bei der Bereitstellung ihrer Angebote im IPv6-Internet. Nicht einmal so große Anbieter wie ebay, web.de oder amazon sind bereit für IPv6. Man kann nur hoffen, dass sich dies auf Druck der Kunden und deren Wunsch nach Lösungen auf Dauer ändern wird. VoIP könnte ein Motor für den Ausbau von IPv6 sein. Leider bedeutet dieser aktuelle Zustand bei den ASP, dass ein IPv6-only-Netzwerk aktuell nicht sinnvoll ist, die Einschränkungen für die Nutzer würden in keinem Verhältnis zum Nutzen der neuen Technologie stehen. Daher kann eine Empfehlung nur für die Realisierung von Netzwerken mit beiden IP-Stacks abgegeben werden – auch wenn der Verfasser dieser Arbeit gern ein anderes Ergebnis erzielt hätte.

In dieser Arbeit wurden verschiedene Produkte, die für die VoIP-Kommunikation relevant sind, auf ihre Eigenschaften unter IPv6 getestet und die Ergebnisse entsprechend aufgeführt. Dadurch ließ sich auch ein Beispielszenario entwerfen, an dem man sich orientieren kann, wenn man selbst IPv6 nutzen möchte. Alle Komponenten um dies zu

realisieren sind heute schon verfügbar. Wie ein solches Netzwerk zu realisieren ist wurde gezeigt. Die Einschränkungen und Hindernisse die dabei auftreten können wurden beschrieben, z.Bsp:

- DNS-Probleme bei der Auflösung von SIP-Servern an Clients
- Fehlende Konfigurationsmöglichkeiten von Hardware, wenn IPv4 nicht benutzt werden soll
- NTP-Synchronisationen erfordern abweichende Serveradressen
- Fehlende Sicherheitseinstellungen wie Optionen zu Aktivierung der PrivacyOption

Es wurde gezeigt, wie sogar der Dienst eines Telefonieanbieters für ein IPv6-fähiges Cloud-IP-PBX-System selbst realisiert werden kann und welcher Hilfsmittel es dafür bedarf. Die vorgestellte Lösung befindet sich mittlerweile in produktiver, täglicher Nutzung durch mehr als 10 Teilnehmer und sorgt durch die Stabilität und Vielseitigkeit für die Zufriedenheit der Anwender. Die Langzeiterfahrung zeigt, dass IPv6 und VoIP bereits heute miteinander funktionieren.

IPv6 verspricht für VoIP-Produkte eine Vielzahl neuer Funktionen, wobei die Hersteller sich aktuell noch darauf konzentrieren dieselben Funktionsumfänge wie unter IPv4 zu realisieren. Das neue Protokoll ermöglicht jedoch noch Vieles mehr. Ideen wären beispielsweise:

- Eingebaute VPN-Tunnel zwischen SIP-Client und SIP-Server unter Nutzung des IPSec-Headers von IPv6
- Nutzung von IPv6 Mobile Option und Roaming der Clients zwischen unterschiedlichen Internetanschlüssen (Beispiel: Fortwährendes Gespräch mit einer Smartphone-App beim Wechsel vom heimischen WLAN in das LTE-Netz unterwegs und dann erneut beim Wechsel ins Firmen-WLAN)
- Unterstützung von mehreren IP-Adressen (es fehlen Einstellmöglichkeiten, da aktuelle Clients noch davon auszugehen scheinen, dass ein Gerät nur eine IP-Adresse (wie bei IPv4) besitzt. Damit könnten Sicherheitsszenarios gebaut werden, die bei Ausfall einen Funktionserhalt ermöglichen (z.Bsp.: wenn der öffentliche Server X über die UID A nichtmehr erreichbar ist, dann registriere dich über die ULA B bei Server Y)

Die Entwicklung zeigt, dass IPv6 für die VoIP-Lösungen der Zukunft eine zentrale Rolle spielen wird und IPv4 perspektivisch ablöst. Ob IPv4 ganz verschwinden kann, bleibt abzuwarten – veraltete Technologien erweisen sich häufig einer besonderen Hartnäckigkeit. Bestes Beispiel dafür ist das Fax.

Die nächsten Jahre werden jedoch mit großer Sicherheit deutliche Fortschritte in Richtung der hier gezeigten Szenarien bringen, davon kann man ruhigen Gewissens ausgehen.

## Abbildungsverzeichnis

Abbildung 1: Prognosemodell - Reduktion IPv4 freier Adressvorrat der RIR's .....	2
Abbildung 2: IPv6-Anteil auf www.heise.de .....	3
Abbildung 3: Bestandteile einer VoIP-Lösung .....	7
Abbildung 4: konvergenter Anschluss (NGN) - aus vielen Medien wird eins .....	10
Abbildung 5: Vergleich Sprachverbindungen auf den Telekom-Netzen .....	11
Abbildung 6: Breitbandverfügbarkeit in Deutschland nach Bandbreitenklassen .....	12
Abbildung 7: Breitbandverfügbarkeit $\geq$ 6MBit in Deutschland.....	12
Abbildung 8: Vergleich Adressbereiche IPv4/IPv6 .....	14
Abbildung 9: Vergleich ausgewählter IP-Stack-Realisierungen.....	16
Abbildung 10: Einordnung von VoIP-Protokollen in OSI/ISO-Modell.....	18
Abbildung 11: IP-basiertes TK-System mit versch. Clients im Kundennetz .....	19
Abbildung 12: IP-basiertes TK-System aus der Cloud .....	20
Abbildung 13: NGN-Realisierung, Cloud-TK-System mit lokalem Proxy (im Router) .....	22
Abbildung 14: Grobeinteilung Komponenten Versuchsnetzwerk .....	23
Abbildung 15: "ipconfig"- ermittelte IP-Konfiguration eines Windows-PC .....	23
Abbildung 16: Google Inc (IPv6 Adoption) [Goo18] .....	25
Abbildung 17: Vyncke 2017 - Statistik zu IPv6-fähigen Webseiten in Deutschland [Vyn17] .....	27
Abbildung 18: Abfrage des SRV-Records _sip._udp.* für die Domäne sipgate.de .....	30
Abbildung 19: Auswirkung der Präfixgröße auf den Adressraum.....	34
Abbildung 20: Web-Oberfläche eines AVM-Routers an einem Kabelanschluss mit DS- Lite .....	35
Abbildung 21: Web-Oberfläche eines AVM-Routers am VDSL-Anschluss mit DualStack .....	36
Abbildung 22: ipconfig-Ausdruck eines Hosts vor der Umnummerierung.....	38
Abbildung 23: ipconfig-Ausdruck eines Hosts nach der Umnummerierung .....	38
Abbildung 24: Marktanteile Router in Deutschland.....	41
Abbildung 25: schematische Darstellung der Routertests .....	41
Abbildung 26: ASUS DSL-AC68U .....	42
Abbildung 27: TP-Link Archer C59 .....	44
Abbildung 28: Linksys E2500 .....	45
Abbildung 29: AVM Fritz!Box 7490 .....	46

---

Abbildung 30: Zoiper-Benutzeroberfläche .....	54
Abbildung 31: SIP-Trace eines Linphone-Anrufes mit IPv6 .....	55
Abbildung 32: miniSipPhone Konfigurationsdialog .....	56
Abbildung 33: SIP-Trace eines Rufaufbaus unter Verwendung von IPv6 .....	56
Abbildung 34: Zoiper-Benutzeroberfläche .....	57
Abbildung 35: unify OpenStage 15 Firmwarestand.....	60
Abbildung 36: Netzwerkeigenschaften unify OpenStage 15.....	61
Abbildung 37: snom715 .....	61
Abbildung 38: IPv6-Einstellungen eines snom715 .....	62
Abbildung 39: Bootscreen snom715 .....	62
Abbildung 40: GXP1450 .....	63
Abbildung 41: IP-Anzeige des Grandstream GXP1450 .....	63
Abbildung 42: Grandstream GXP1450, Netzwerkkonfiguration.....	64
Abbildung 43: Auswahl des DNS-Modus beim GXP1450 .....	64
Abbildung 44: SIP-Client-Konfiguration auf einer Fritz!Box 7490.....	66
Abbildung 45: DynDNS-Records einer Fritz!Box an DualStack-Anschluss .....	68
Abbildung 46: ipconfig an einem PC im Testnetz .....	69
Abbildung 47: IPv6-Adressen auf einem iOS-Client .....	70
Abbildung 48: Schematische Darstellung des DualStack-Netzwerks .....	71
Abbildung 49: Ergebnis IPv6-Ping an ipv6.google.com .....	75
Abbildung 50: abgeschlossene 3CX-Grundinstallation .....	76
Abbildung 51: 3CX-Konfigurationsassistent .....	77
Abbildung 52: 3CX-Konfigurationsassistent (FQDN) .....	77
Abbildung 53: 3CX-webbasierter Konfigurationsmanager der selfhosted PBX.....	78
Abbildung 54: 3CX-Client - Kontoeinrichtung und Anruf.....	79
Abbildung 55: 3CX-Client-Trace eines internen Anrufes .....	79
Abbildung 56: 3CX-SIP-Trunk-Einrichtung .....	80
Abbildung 57: 3CX-Client-Trace bei Anruf an öff. Teilnehmer .....	80
Abbildung 58: Fragebogen zur Ermittlung der IPv6-Fähigkeiten aktueller ISP- Anschlüsse .....	ix

---

## Tabellenverzeichnis

Tabelle 1: Ergebnis IPv6-Test Webseiten Top50 Deutschland.....	26
Tabelle 2: Unterstützung von IPv6 durch ITSP.....	29
Tabelle 3: Ermittlung IPv6-Implementierung div. ISP .....	33
Tabelle 4: ISP mit DS-Lite Implementation .....	35
Tabelle 5: ISP mit DualStack Implementation .....	37
Tabelle 6: Ergebnisse Routertests.....	50
Tabelle 7: Ergebnisse softwarebasierte Clients .....	59
Tabelle 8: Ergebnisse hardwarebasierte Clients .....	67

---

## Literaturverzeichnis

- [Ahl16] AHLERS, Ernst  
**Das Internet-Upgrade rollt: IPv4 wird abgelöst**  
c't - magazin für computer, technik, 2016  
online: <https://www.heise.de/ct/ausgabe/2016-10-Das-Internet-Upgrade-rollt-IPv4-wird-abgeloest-3183991.html>
- [Ale17] ALEXA INTERNET  
**Top Sites in Germany - Alexa**  
Alexa Internet, 2017  
online: <https://www.alexa.com/topsites/countries/DE>
- [Bad10] BADACH, Anatol  
**Voice over IP - Die Technik ; Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit**  
4., überarb. und erw. Aufl. München : Hanser, 2010
- [Bun17] BUNDESMINISTERIUM FÜR VERKEHR UND DIGITALE INFRASTRUKTUR  
**Aktuelle Breitbandverfügbarkeit in Deutschland (Stand Mitte 2017) - Erhebung des TÜV Rheinland im Auftrag des BMVI**  
BMVI. Berlin, 2017
- [Cur15] CURRAN, JOHN (PRESIDENT AND CEO AMERICAN REGISTRY FOR INTERNET NUMBERS)  
**ARIN IPv4 Free Pool Reaches Zero**  
American Registry for Internet Numbers (ARIN), 2015
- [Dob15] DOBRINDT, Alexander  
**Richtlinie „Förderung zur Unterstützung des Breitbandausbaus in der Bundesrepublik Deutschland“ - Bekanntmachung des Bundesministeriums für Verkehr und digitale Infrastruktur**  
BMVI, 2015. Rev. 3 (02.05.2017)  
online: [http://www.bmvi.de/SharedDocs/DE/Anlage/Digitales/foerderrichtlinie-breitband-mai2.pdf?\\_\\_blob=publicationFile](http://www.bmvi.de/SharedDocs/DE/Anlage/Digitales/foerderrichtlinie-breitband-mai2.pdf?__blob=publicationFile)
- [EG03] KOMMISSION DER EUROPÄISCHEN GEMEINSCHAFTEN  
**Empfehlung 2003/361/EG - Empfehlung der Kommission betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen.** Aktenzeichen K(2003) 1422  
In: *Amtsblatt der Europäischen Union* 2003 (2003-05-20)
- [FS16] FISCHER, Jörg ; SAILER, Christian  
**VoIP Praxisleitfaden - IP-Kommunikation aus der Cloud, im WEB und mobil planen, implementieren und betreiben**  
2., überarbeitete und erweiterte Auflage. München : Hanser, 2016
- [Goo18] GOOGLE INC.  
**IPv6-Statistics - We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.**  
Google Inc., 2018  
online: <http://www.google.com/intl/en/ipv6/statistics.html>

- 
- [Hag09] HAGEN, Silvia  
**IPv6 - Grundlagen - Funktionalität - Integration**  
2. Aufl. : Sunny Edition, 2009
- [Hag11] HAGEN, Silvia  
**Planning for IPv6**  
1. Aufl. Farnham : O'Reilly, 2011 (Safari Tech Books Online)
- [Hag14] HAGEN, Silvia  
**IPv6 essentials**  
3rd ed. Sebastopol, CA : O'Reilly, 2014
- [Hus18] HUSTON, Geoff  
**IPv4 Address Report**  
HUSTON, Geoff, 2018  
online: <https://ipv4.potaroo.net/>
- [IAN17] IANA  
**IANA IPv4 Address Space Registry - allocation of Internet Protocol version 4 (IPv4) address space to various registries**  
IANA, 2017  
online: <https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml>
- [IfM17] INSTITUT FÜR MITTELSTANDSFORSCHUNG (IfM) BONN  
**Informationen zum Mittelstand (Stand 2017) - aus erster Hand, wissenschaftlich fundiert, praxisnah** (2017)  
online: [http://www.ifm-bonn.org/fileadmin/data/redaktion/ueber\\_uns/ifm-flyer/IfM-Flyer-2017.pdf](http://www.ifm-bonn.org/fileadmin/data/redaktion/ueber_uns/ifm-flyer/IfM-Flyer-2017.pdf) – Überprüfungsdatum 2017-09-14
- [ISO94] ISO/IEC  
**ISO/IEC 7498-1 - Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.** International Standard  
International Organization for Standardization. Genf, 1994. Rev. 4  
online:  
[http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269\\_ISO\\_IEC\\_7498-1\\_1994\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip)
- [ITU-H.323] ITU-T  
**Recommendation H.323 - Packet-based multimedia communications systems**  
International Telecommunication Union, 1996. Rev. 7.0 (14.12.2009)  
online: <http://www.itu.int/rec/T-REC-H.323-200912-I/en>
- [ITU-Struktur] ITU-T  
**ITU-T Recommendation Structure**  
ITU-T, 2018  
online: <https://www.itu.int/en/ITU-T/publications/Pages/structure.aspx>
- [ITU-X.200] ITU-T  
**Recommendation X.200 - Information technology - Open Systems Interconnection - Basic reference model: The basic model**  
ITU-T, 1994  
online: <http://www.itu.int/rec/T-REC-X.200-199407-I>
- [Kan05] KANBACH, Andreas  
**SIP - Die Technik - Grundlagen und Realisierung der Internet-Technik - Für**

- VoIP, Videotelefonie, Instant Messaging und Presence Service*  
1. Aufl. Wiesbaden : Vieweg, 2005 (IT erfolgreich gestalten)
- [Lin81] LINCOLN LABORATORY  
**ISI / RR-81-90 - A Network Voice Protocol NVP-II**  
USC/ISI, 1981  
COHEN, Danny ; CASNER, Stephen ; FORGIE, James W.  
online: <ftp://128.9.176.20/isi-pubs/rr-81-90.pdf>
- [NCC12] NCC, RIPE  
**Memo zur Vergabe von Adressen aus dem letzten /8-Adressbereich**  
RIPE NCC, 2012  
online: <https://www.ripe.net/publications/ipv6-info-centre/about-ipv6/ipv4-exhaustion/last-8-phases>
- [poo17] POOL.NTP.ORG PROJEKT  
**Continuing IPv6 deployment | NTP Pool News**  
pool.ntp.org Projekt, 2017  
online: <https://news.ntppool.org/2011/06/continuing-ipv6-deployment/>
- [RFC1631] IETF  
**RFC 1631 - The IP Network Address Translator NAT**  
Internet Engineering Task Force (IETF), 1994  
EGEVANG, Kjeld Borch ; FRANCIS, Paul  
online: <https://tools.ietf.org/html/rfc1631>
- [RFC1918] IETF  
**RFC 1918 - Address Allocation for Private Internets**  
Internet Engineering Task Force (IETF), 1996  
REKHTER, Yakov ; MOSKOWITZ, Robert G. ; KARREBERG, Daniel ; GROOT, Geert Jan de ; LEAR, Eliot  
online: <https://tools.ietf.org/html/rfc1918>
- [RFC2460] IETF  
**RFC 2460 - Internet Protocol, Version 6. IPv6, Specification**  
Internet Engineering Task Force (IETF), 1998  
DEERIN, S. ; HINDEN, R.  
online: <https://tools.ietf.org/html/rfc2460>
- [RFC2663] IETF  
**RFC 2663 - IP Network Address Translator NAT - Terminology and Considerations**  
Internet Engineering Task Force (IETF), 1999  
SRISURESH, Pyda ; HOLDREDGE, Matt  
online: <https://tools.ietf.org/html/rfc2663>
- [RFC2894] IETF  
**RFC 2894 - Router Renumbering for IPv6**  
Internet Engineering Task Force (IETF), 2000  
CRAWFORD, Matt  
online: <https://tools.ietf.org/html/rfc2894>
- [RFC3177] IETF  
**RFC 3177 - IAB/IESG Recommendations on IPv6 Address Allocations to Sites**  
Internet Engineering Task Force (IETF), 2001  
INTERNET ENGINEERING STEERING GROUP ; INTERNET ARCHITECTURE BOARD  
online: <https://tools.ietf.org/html/rfc3177>

- [RFC3261] IETF  
**RFC 3261** - *SIP: Session Initiation Protocol*  
Internet Engineering Task Force (IETF), 2002  
SCHOOLER, Eve ; CAMARILLO, Gonzalo ; HANDLEY, Mark ; PETERSON, Jon ;  
ROSENBERG, Jonathan ; JOHNSTON, Alan ; SCHULZRINNE, Henning ; SPARKS,  
Robert  
online: <https://tools.ietf.org/html/rfc3261>
- [RFC3263] IETF  
**RFC 3263** - *Session Initiation Protocol (SIP): Locating SIP Servers*  
Internet Engineering Task Force (IETF), 2002  
ROSENBERG, Jonathan ; SCHULZRINNE, Henning  
online: <https://www.ietf.org/rfc/rfc3263.txt>
- [RFC3769] IETF  
**RFC 3769** - *Requirements for IPv6 Prefix Delegation*  
Internet Engineering Task Force (IETF), 2004  
MIYAKAWA, Shin ; DROMS, Ralph  
online: <https://tools.ietf.org/html/rfc3769>
- [RFC4213] IETF  
**RFC 4213** - *Basic Transition Mechanisms for IPv6 Hosts and Routers*  
Internet Engineering Task Force (IETF), 2005  
NORDMARK, Erik ; GILLIGAN, Robert E.  
online: <https://tools.ietf.org/html/rfc4213>
- [RFC4941] IETF  
**RFC 4941** - *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*  
Internet Engineering Task Force (IETF), 2007  
NARTEN, Thomas ; DRAVES, Richard ; KRISHNAN, Suresh  
online: <https://tools.ietf.org/html/rfc4941>
- [RFC5006] IETF  
**RFC 5006** - *IPv6 Router Advertisement Option for DNS Configuration*  
Internet Engineering Task Force (IETF), 2007  
JEONG, Jaehoon Paul ; PARK, Soohong Daniel ; BELOEIL, Luc ; MADANAPALLI,  
Syam  
online: <https://tools.ietf.org/html/rfc5006>
- [RFC6177] IETF  
**RFC 6177** - *IPv6 Address Assignment to End Sites. Best Current Practice*  
Internet Engineering Task Force (IETF), 2011  
NARTEN, Thomas ; HUSTON, Geoff ; ROBERTS, Rosalea G.  
online: <https://tools.ietf.org/html/rfc6177>
- [RFC6264] IETF  
**RFC 6264** - *An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition*  
Internet Engineering Task Force (IETF), 2011  
JIANG, Sheng ; GUO, Dayong ; CARPENTER, Brian  
online: <https://tools.ietf.org/html/rfc6264>
- [RFC6333] IETF  
**RFC 6333** - *Dual-Stack Lite: Broadband Deployments Following IPv4 Exhaustion*  
Internet Engineering Task Force (IETF), 2011

- DURAND ; ALAIN ; WOODYATT ; JAMES ; DROMS ; RALPH ; LEE ; L, Yiu  
online: <https://tools.ietf.org/html/rfc6333>
- [RFC6598] IETF  
**RFC 6598 - IANA-Reserved IPv4 Prefix for Shared Address Space**  
Internet Engineering Task Force (IETF), 2012  
WEIL, Jason ; KUARSINGH, Victor ; DONLEY, Chris ; LILJENSTOLPE, Christopher ;  
AZINGER, Marla  
online: <https://tools.ietf.org/html/rfc6598>
- [RFC791] DEFENSE ADVANCED RESEARCH PROJECTS AGENCY  
**Internet Protocol - DARPA Internet Program Protocol Specification**  
University of Southern California. Marina del Rey, California, 1981  
POSTEL, Jon  
online: <https://tools.ietf.org/html/rfc791>
- [RSL02] RUPP, Stephan ; SIEGMUND, Gerd ; LAUTENSCHLAGER, Wolfgang  
**SIP - multimediale Dienste im Internet - Grundlagen, Architektur,  
Anwendungen**  
1. Aufl. Heidelberg : dpunkt-Verl., 2002
- [SB16] SCHLEDE, Frank-Michael ; BÄR, Thomas  
**IPv6 im Praxis-Check bei Telekom und Co: - Ratgeber: IPv6 in Deutschland**  
computerwoche.de, 2016  
online: <https://www.computerwoche.de/a/ratgeber-ipv6-in-deutschland,3217923>
- [Tel15] TELEKOM DEUTSCHLAND AG  
**Das Netz der Zukunft - Chancen und Nutzen der IP-Technologie**  
Telekom Deutschland AG. Bonn, 2015  
online:  
[https://geschaeftskunden.telekom.de/blobCache/umn/uti/290136\\_1493193273000/blobBinary/netz-der-zufunft.pdf](https://geschaeftskunden.telekom.de/blobCache/umn/uti/290136_1493193273000/blobBinary/netz-der-zufunft.pdf)
- [Vyn17] VYNCKE, Eric  
**Statistik zu IPv6 Webservern.** online, 2017  
VYNCKE, Eric  
online: <https://www.vyncke.org/>
- [Ziv17] ZIVADINOVIC, Dusan  
**IPv6: Tunneldienst SixXS schließt die Tore endgültig**  
Heise Medien, 2017  
online: <https://www.heise.de/newsticker/meldung/IPv6-Tunneldienst-SixXS-schliesst-die-Tore-endgueltig-3663270.html>

## Anhang

In Kapitel 3.3 - Internet Service Provider (ISP) wurden verschiedene Provider angeschrieben, um eine gegenüber der Internetrecherche zuverlässigere Ermittlung der für IPv6 relevanten Anschlüsseigenschaften zu erhalten. Dafür wurden alle Provider um Beantwortung des folgenden Fragebogens gebeten:

### Fragebogen

zu  
IPv6-fähigen Internetanschlüssen

robert brocke

Tel.: +49 (151) 550566-26  
Mail: robertbrocke@gmx.de

Bitte beantworten Sie die folgenden Fragen:  
Vielen Dank!

Zurücksetzen

1. **Anbieter:** \_\_\_\_\_
2. **Produkt:** \_\_\_\_\_
3. **Technologie des Produktes:**  
(Mehrfachnennung möglich)
  - DSL       VDSL
  - Kabelanschluss (DOCSIS \_\_\_)
  - Glasfaser (FTTx)
  - LTE
  - Andere \_\_\_\_\_
4. **Kundensegment:**  
(Mehrfachnennung möglich)
  - Geschäftskunden       Privatkunden
5. **Unterstützte IP-Protokolle:**
  - nur IPv4
  - IPv4 und IPv6 (DualStack)     IPv4 und IPv6 (DS-Lite, IPv4 mittels CG-NAT)
  - IPv4 und IPv6 (andere Technologie: \_\_\_\_\_)
  - nur IPv6
  - Unterstützung für IPv6 muss beantragt werden, ist im Standardprodukt nicht enthalten, kann aber (ggf. kostenpflichtig) eingerichtet werden.
6. **Anzahl öff. IPv4-Adressen:** \_\_\_\_\_ (  dyn. Zuordnung )
  - eine feste öff. IPv4-Adresse kann (  kostenpflichtig ) beantragt werden
  - bitte geben Sie bei Verwendung privater IPv4-Adressen hinter einem CarrierGrade-NAT die Anzahl „0“ an.
7. **Bereich zugeordneter IPv6-Adressen:** / \_\_\_\_\_ (  dyn. Präfix )
  - eine fester IPv6-Adressraum kann (  kostenpflichtig ) beantragt werden
8. **Umfasst das Produkt Telefoniedienste?**
  - nein
  - ja, als SIP-Profile für einzelne Rufnummern
  - ja, als SIP-Trunk zur Einrichtung auf einem VoIP-TK-System
  - ja, als Mobilfunkrufnummer
9. **Kontakt für Rückfragen:**

Name: \_\_\_\_\_

Kontaktadresse (Mail/Telefon): \_\_\_\_\_

Robert Brocke • Friedrich-Naumann-Straße 6 • 39108 Magdeburg • Tel.: +49 (151) 550566-26 • Mail: robertbrocke@gmx.de

Abbildung 58: Fragebogen zur Ermittlung der IPv6-Fähigkeiten aktueller ISP-Anschlüsse

## Danksagung

Ich möchte mich bei allen Personen bedanken, die durch ihre fachliche oder persönliche Unterstützung zum Gelingen dieser Arbeit beigetragen haben.

Insbesondere möchte ich mich bei Prof. Dr. Eduard Siemens für die akademische Betreuung und die Freiräume bei der Bearbeitung des Themenbereichs bedanken. Er unterstützte mich durch seine hilfreichen Ratschläge und Anregungen. Ohne ihn gäbe es diese Arbeit nicht.

Mein Dank gilt ebenfalls Dr. Dmitry Kachan, der als Zweitprüfer unterstützend zur Seite stand.

Ein großes Dankeschön geht an Matthias Kunert und das Unternehmen cubeoffice, die mir neben meiner Berufstätigkeiten oft die nötigen Freiräume verschafften um diese Arbeit fertigzustellen.

Mein Dank gilt ganz besonders den Mitgliedern meiner Familie, die mir stets den notwendigen Rückhalt gaben und mich motivierten, wann immer es nötig war.