# c't NETZWERKE

## Heimnetze optimal einrichten

## Schnelles WLAN nutzen

Mesh & Repeater optimal auswählen

Das bringen Wi-Fi-6E und Wi-Fi-7

## Netzwerke bauen

Preisgünstig verdrahten

Tipps & Tricks · schnelle Switches

## VPN modernisieren

Peer-to-Peer statt VPN-Zentrale

Mit speziellen VPNs die Privatsphäre schützen


# Fritzbox einrichten und tunen

Kaufberatung: Die beste Fritzbox für jeden Anschluss

SmartHome: Zigbee- und DECT-Geräte kombinieren

Per WireGuard-VPN das Heimnetz unterwegs nutzen

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

4 196982 314900 04

# Editorial

**Liebe Leserin, lieber Leser,**

dieses Sonderheft deckt wichtige aktuelle Netzwerkthemen ab. Es behandelt exemplarisch alle Ebenen der PC-Vernetzung, angefangen beim ersten Kabel, führt über Router-, Mesh- und Switch-Tests bis hin zur Konfiguration eines eigenen VPN.

Den Schwerpunkt bilden umfassende Beiträge zum beliebten Fritzbox-Router und zu seinem erneut stark verbesserten FritzOS. Zu den praktisch abgehandelten Themen gehören die vielseitige WireGuard-VPN-Vernetzung, ein schonungsloser Vergleich mit anderen IPv6-fähigen Routern und ausführliche Beiträge zur Fritzbox als Smart-Home-Zentrale mitsamt Konfigurationsbeispielen.

Das Heft erklärt Grundlagen und Hintergründe zur Mesh-Vernetzung mit dem aktuellen Wi-Fi 6 und hilft bei der Kaufentscheidung mit einem fundierten Test von Mesh-Kandidaten. Und es blickt mit dem ersten gründlichen Test auf das kommende Wi-Fi 7 voraus.

Falls Sie gerade ein neues Netzwerk aufsetzen, etwa vor einem Umzug, soll das Heft Ihnen als kompetenter Ratgeber zur Seite stehen, der durch die korrekte Installation leitet. Dabei hilft es mit einer Auswahl von günstigen Komponenten zur Verdrahtung, Einkaufslisten inklusive.

Aber egal, ob Sie Ihr eigenes kleines Netz als persönliches Bastelprojekt betreiben oder in Ihrem Betrieb das Netzwerk in Gang halten: Oft will man auf die Netzwerkgeräte auch von unterwegs per VPN zugreifen. Hier hat sich Entscheidendes getan, die modernsten VPNs ersparen Ihnen den zentralen Server. Was bedeutet: ein Flaschenhals weniger.

Viel Spaß beim Netzwerken wünscht

Dušan Živadinović

# Inhalt

## FRITZBOX EINRICHTEN UND TUNEN

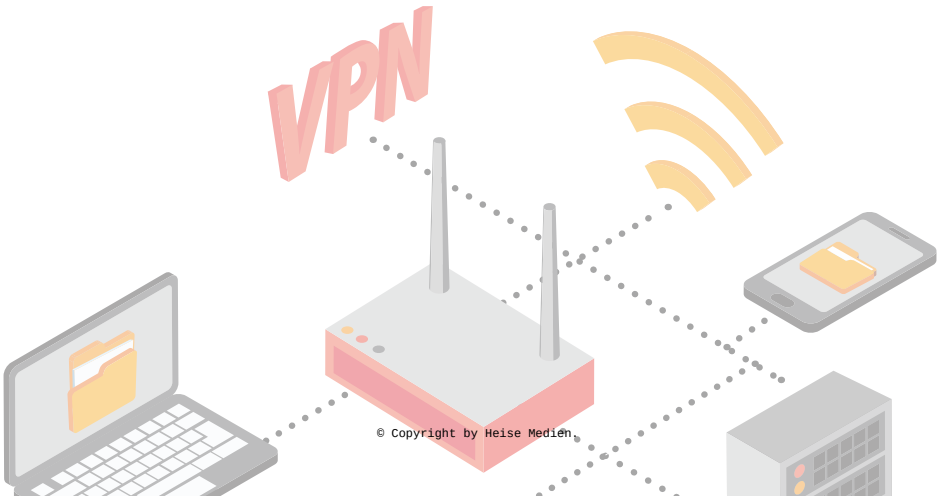
**Fritzbox-Router bekommt man für alle üblichen Internetanschlüsse. Doch eine Fritzbox im Werkszustand ist wie das Internet ohne Webseiten – lesen Sie, wie Sie die Einstellungsvielfalt rund um WireGuard, MyFritz und Smart Home beherrschen.**

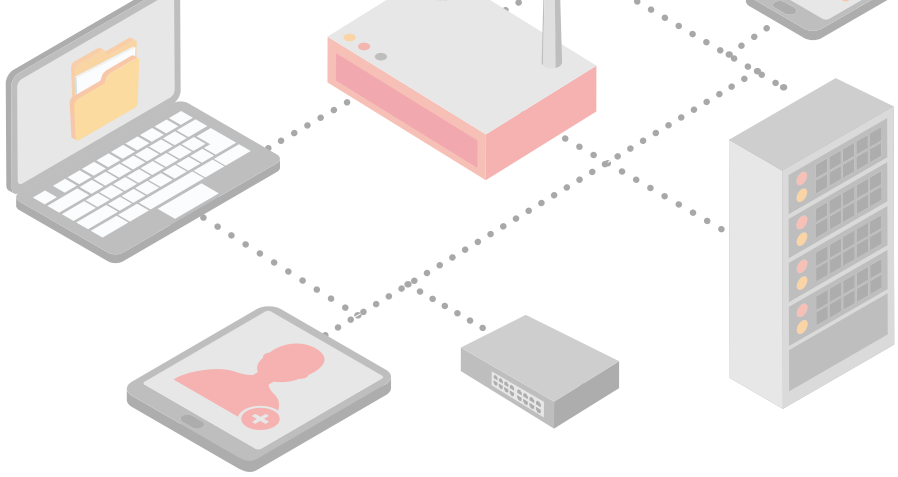


## SCHNELLES WLAN NUTZEN

**Mesh-Systeme erleichtern die Abdeckung von Wohnungen zwar enorm, aber am Markt kämpfen teils sehr unterschiedliche Kandidaten um die Käufergunst. Wir ordnen den Stand der Technik ein und helfen mit gründlichen Tests bei der Kaufentscheidung.**







## NETZWERKE BAUEN

**Egal, ob Sie Teile der Verkabelung modernisieren, das Netz erweitern oder gar völlig neu aufsetzen: Unser Ratgeber weist den Weg zu einem funktionalen, aber dennoch preisgünstigen Netzwerk und liefert Lösungen für viele aktuelle Netzwerkprobleme.**



## VPN MODERNISIEREN

**Die VPN-Technik entwickelt sich in unerwartete Richtungen. Peer-to-Peer-VPNs ersparen neuerdings den zentralen Server und locken mit stark vereinfachter Einrichtung. Und Google mischt ernsthaft mit und verhindert das Erstellen von Surf-Profilen.**



## ZUM HEFT



# Zwei große Updates für Fritzboxen

**Alle paar Jahre bekommen AVMs Router gratis ein großes Firmware-Update, das die vielseitigen Geräte noch nützlicher macht. AVM hat nun binnen Jahresfrist FritzOS 7.50 und 7.56 herausgebracht: Sie bringen unter anderem mehr Wumms ins VPN, machen das Telefonieren komfortabler und das Smart Home schlauer. Hier schildern wir, was FritzOS derzeit kann.**

Von **Ernst Ahlers und Dušan Živadinović**

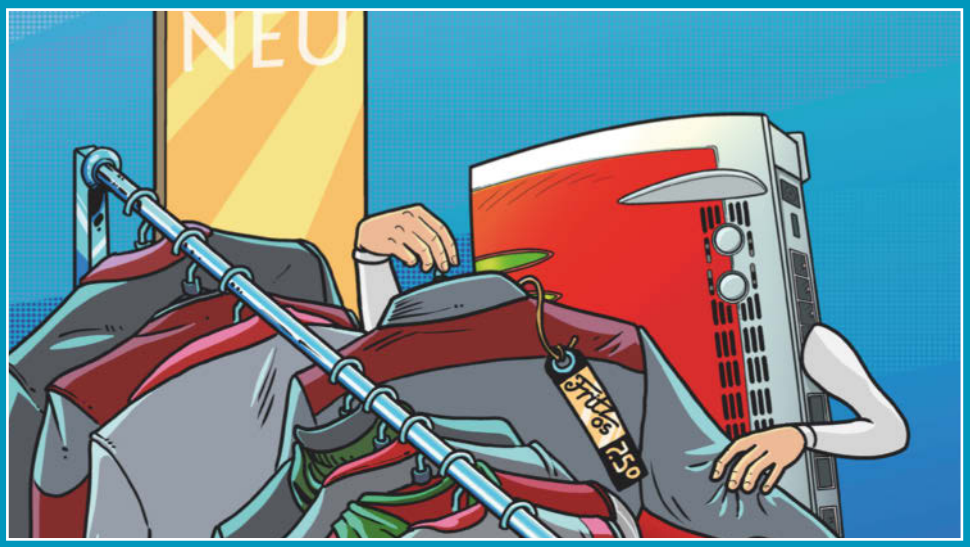



Bild: Michael Vogt

AVM hat in diesem Jahr nach dem großen Update FritzOS 7.50 noch einige weitere Verbesserungen mit 7.56 herausgebracht. Vor allem 7.50, aber auch 7.56 enthalten viele nützliche Funktionen. Weil das große Update auf FritzOS 7.50 die meisten Neuigkeiten bringt, widmen wir uns diesem zuerst: Auf den ersten Blick unterscheidet es sich nur wenig vom Vorgänger, FritzOS 7.3x. AVM hat das Browsermenü dezent modernisiert, sodass es auf großen Bildschirmen besser lesbar ist. Falsche Klicks, durch die man bei älteren FritzOS-Versionen Änderungen ungewollt verworfen hat, kommen dank geschickter angeordneten „Übernehmen“- beziehungsweise „Verwerfen“-Knöpfen nicht mehr vor.

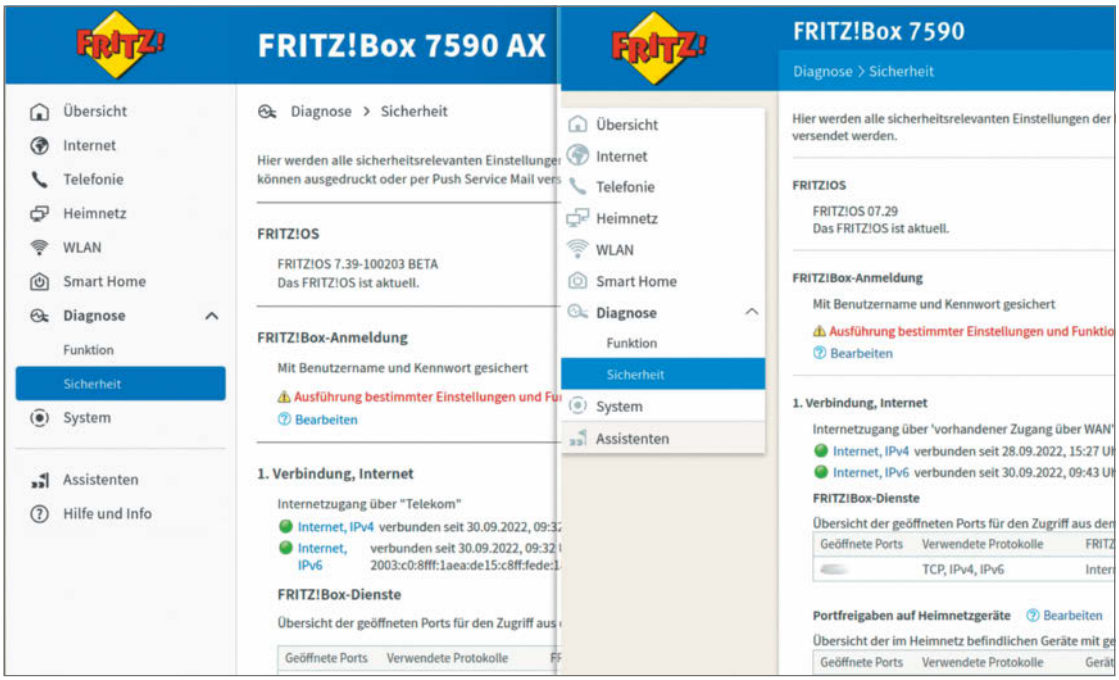
Mehr Neuerungen stecken unter der Haube: AVM hat mit FritzOS 7.50 weit über hundert Funktionen verbessert und Fehler behoben. Dazu kommen 17 neue Funktionen und 27 Änderungen. Das Update haben nicht nur alle zurzeit vertriebene Fritzboxen und WLAN-Repeater erhalten, sondern auch einzelne ältere Modelle wie die verbreitete 7490. Ist Ihr Router nicht darunter, liefern wir im nachfolgenden Artikel Tipps, wie Sie eine passende neue Fritzbox für Ihren Anschluss finden.

Mit einem virtuellen privaten Netz (VPN) kann man über eine verschlüsselte Verbindung beispielsweise aus der Ferne den Schwiegereltern Hilfestellung geben. In Unternehmen verschaffen VPNs Heimarbeitern Zugriff auf Ressourcen im Firmennetz.

Das ist die größte Neuerung von FritzOS 7.50: WireGuard ist nun der moderne Kompagnon des alten IPsec-basierten Fritz-VPN. Der VPN-Neuling hat sich in den letzten Jahren rasant ausgebreitet und ist auch in den Linux-Kernel eingezogen, was auf Linux beschleunigte Verarbeitung gewährleistet.

Bei WLAN-Routern war die Deutsche Telekom der hiesige WireGuard-Pionier: Schon im Frühjahr 2020 erschien in Speedport-Geräten die erste Umsetzung für einen einzigen Zugang. Inzwischen lassen sich fünf definieren, aber nach wie vor können Speedports WireGuard erstens nur alternativ zu IPsec nutzen und zweitens VPN-Tunnel nur über IPv4 als Trägerprotokoll aufbauen [1].

Vielleicht hat das Telekom-Vorpreschen AVM dazu bewegt, WireGuard ebenfalls einzubauen. Das haben die Berliner dann gleich richtig angegangen, mit prinzipiell unbeschränkter Anzahl an Zugängen (genaueres dazu finden Sie im Artikel „Tipps & Tricks“ bei „Maximale Anzahl der Site-2-Site-Verbindungen“), parallelem Betrieb beider VPN-Typen und sowohl IPv4 als auch IPv6 als Trägerprotokolle. Schon die erste FritzOS-Laborversion auf der Fritzbox 7590 überraschte




**Auf großen Bildschirmen sind die Fritzbox-Konfigurationsseiten ab FritzOS 7.5x (links) besser lesbar.**

uns [3]: Wir maßen seinerzeit mit WireGuard den doppelten VPN-Durchsatz (Down/Upstream-Mittelwert 146 Mbit/s) gegenüber IPsec (70 Mbit/s).

## VPN mit Wumms

Inzwischen nutzt AVM je nach Verfügbarkeit fürs Ver- und Entschlüsseln auch Hardware-Kryptobeschleuniger oder geeignete Befehlssatzerweiterungen der Router-Prozessoren. Das steigert den VPN-Durchsatz noch mal deutlich. Kleiner Rückblick: Mit der Laborversion 7.39-100202 von Ende September 2022 maßen wir auf der 7590 gegenüber dem Jahresanfang satte 69 Prozent mehr WireGuard-Durchsatz (247 statt 146 Mbit/s). IPsec legte auf ihrem MIPS-Dualcore-Prozessor sogar um 80 Prozent zu (126 statt 70 Mbit/s). Und die Fritzbox 7520, eine Providervariante der 7530 mit ARM-Quadcore-Prozessor, kam mit 7.39-100201 bei WireGuard sogar auf 352 Mbit/s. Mit IPsec schaffte sie indes nur 107 Mbit/s.

Wie man WireGuard auf Fritzboxen einrichtet und verwendet, haben wir inzwischen für mehrere Anwendungszwecke detailliert beschrieben [2,3,4]. Weitere Praxistipps speziell für WireGuard auf Fritzboxen finden Sie im Artikel „Tipps & Tricks“.

Jedoch hat die VPN-Entwicklung in den letzten Jahren auch ganz neue Architekturen hervorgebracht, die auf Peer-to-Peer-Techniken gründen. Was genau sie von WireGuard und IPsec unterscheidet und welche Vorteile der Peer-to-Peer-Ansatz bringt, lesen Sie im VPN-Schwerpunkt in diesem Heft.

## IPv6-Nachrüstungen

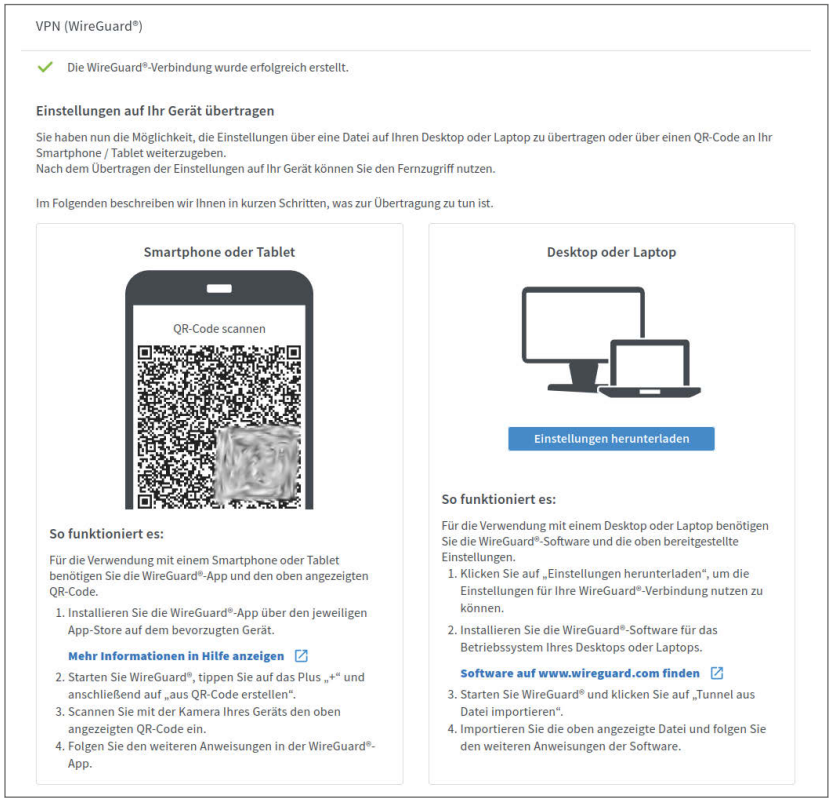
Übrigens kann IPsec nun auch IPv6 als Trägerprotokoll verwenden. Damit können Nutzer, deren Internet-per-TV-Kabel- oder Glasfaseranschlüsse wegen DS-Lite oder CG-NAT keine öffentliche IPv4-Adresse haben, jetzt wahlweise mit IPsec oder mit WireGuard von außen ins Heimnetz gelangen. Das setzt voraus, dass der Client ebenfalls per IPv6 ins Internet kommt, denn an DS-Lite-Anschlüssen sind keine öffentlichen IPv4-Adressen erhältlich, sodass alle daran angeschlossenen Router nur über IPv6 erreichbar sind. Gut, dass Fritzboxen IPv6 beim Einrichten aller Internetzugangstypen nun endlich automatisch aktivieren – doch obacht, auch beim Upgraden der Firmware.

Falls Sie den Adressbereich fürs interne Netz ändern wollen, etwa von 192.168.178.1 auf 192.168.59.1, dann tun Sie das vor der VPN-Konfiguration. Denn das Ändern des Bereiches macht die VPN-Einstellungen hinfällig und Sie müssen von vorn anfangen. Die Adressänderung können Sie sich sparen, wenn Sie nur einzelne Geräte per VPN ankoppeln wollen, Laptops oder Smartphones beispielsweise. Aber bei Site-to-Site-Kopplungen von Fritzbox zu Fritzbox ist das unumgänglich, um Adresskollisionen zu vermeiden.

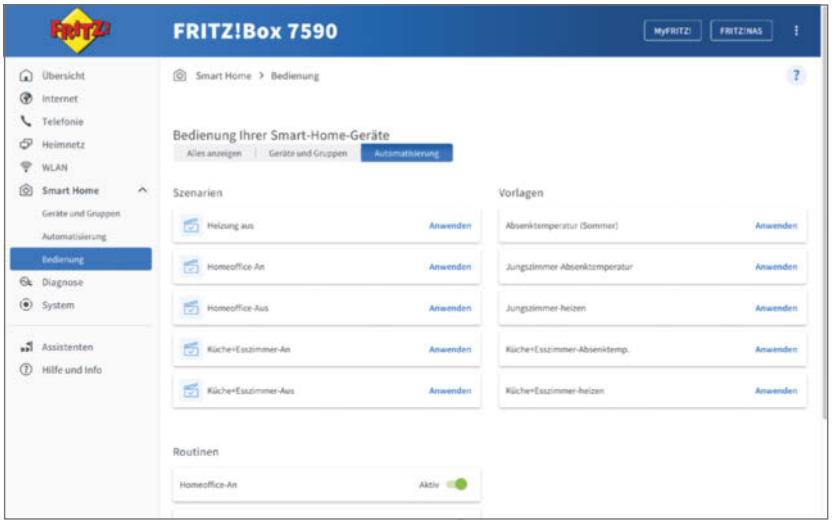
Nützlich wäre noch, wenn sich die Info-Leuchte der Fritzboxen so konfigurieren ließe, dass sie auch „VPN-Tunnel aufgebaut“ signalisiert. Dann sähe man auch ohne Browser, ob gerade jemand von außen im Heimnetz ist.

## Smarteres Smart Home

AVM hat im Laufe einiger Jahre eine Handvoll Smart-Home-Geräte auf der Basis der Schnurlostechnik DECT herausgebracht, sodass man etwa die Heizung, das Licht oder elektrische Verbraucher automatisch steuern kann, etwa gemäß dem Wochenverlauf. Bisher führte jedes der Geräte weitgehend ein Eigen-




**Einfacher geht es kaum, einen VPN-Tunnel zur Fritzbox auf dem Smartphone zu erzeugen: QR-Code mit der WireGuard-App fotografieren, fertig.**




**Das Smart Home wird mit Wenn/Dann-Regeln schlauer. Damit kann man nun beispielsweise den Taster von Schaltsteckdosen verwenden, um mehrere Stromverbraucher gleichzeitig zu schalten und die Temperatur einer Gruppe von Thermostaten umzuschalten.**

leben, ob Heizkörperthermostat (FritzDECT 301/302), intelligentes Leuchtmittel (FritzDECT 500) oder schaltbare Steckdose (FritzDECT 200/210).

Zwar kann man beispielsweise mehrere Thermostate zu einer Gruppe zusammenfassen und gemeinsam umschalten, aber die ganze Gruppe bekommt dieselben Absenk- und Komforttemperaturen. Das geht an der Praxis vorbei, wenn man etwa im Flur und Bad nur mäßig heizen möchte, im Arbeitszimmer aber 20 Grad haben und alle drei zu gleichen Zeitpunkten umschalten will.

Ab FritzOS 7.5x bleibt die Gruppenbindung erhalten, aber man kann mittels individueller Vorlagen, Szenarien und Routinen mehrere Geräte und auch Gruppen mit unterschiedlichen Temperaturen gemeinsam schalten. Dafür bieten sich die FritzDECT-Schalter 400 und 440 an. Wer eine fernschaltbare Fritz-Steckdose hat, kann sich die Taster sparen und hat damit sogar mehr Optionen.

## Sensor-Mehrwert

Denn mit den neuen Wenn/Dann-Regeln kann man den Schalttaster der Fritz-Steckdosen nun als Sensor für Smart-Home-Routinen nutzen. So kann ein Tipp darauf alle an einer Steckdosenleiste angeschlossenen Bürogeräte wie PC, Monitor und Drucker gemeinsam anwerfen und zusätzlich etwa Smart-Lampen ein- und Thermostaten umschalten. Das funktionierte in unserem Versuch tadellos und erleichtert das Familienleben, wenn man die unmittelbare Kontrolle bevorzugt.

Anders als bei den DECT-Tastern gibt es sogar eine visuelle Rückmeldung: Leuchtet die Schalt-LED, ist das Homeoffice in Betrieb, beleuchtet und beheizt. Ist sie aus, sind nicht nur die Homeoffice-Geräte vom Strom getrennt und die LED-Leuchte aus, sondern auch die Thermostate abgesenkt.

Die mit älteren FritzOS-Versionen eingebrachten Automatiken, etwa für Urlaubsabwesenheiten, kann man weiter nutzen und mit den neuen Routinen kombinieren. Der Fritzbox-Admin sollte sich für derartigen Komfortgewinn ein wenig Zeit zur Einarbeitung nehmen und vor Beginn der Konfiguration eine Tabelle mit sinnvollen Begriffen für Vorlagen, Szenarien und Routinen anfertigen. Das erleichtert die Übersicht und die spätere Erweiterung.

Praktisch auch: Der Browser bleibt mit der Fritzbox so lange verbunden, bis man nach üblicherweise 20 Minuten wegen Inaktivität automatisch abgemeldet wird. Währenddessen zeigt er an, wenn sich Betriebszustände ändern, etwa eine per Smartphone-App ausgeschaltete Steckdose.

## Anruferansage

Mit dem neuen „Sprachklingeln“ lernen AVM-Schnurlostelefone, Anrufer statt eines Düdelüt mit ihren im Telefonbuch hinterlegten Namen zu melden. Bei unterdrückter Rufnummer hört man „Anruf von Unbekannt“. Die Funktion steckt im Menü bei „Telefoniegeräte“. Über den „Bearbeiten“-Stift kommt man zum „Klingeltöne“-Reiter eines an die Box gekoppelten DECT-Telefons.

### Literatur

[1] Ernst Ahlers, FaserSpezi, Telekom-Router Speedport Smart 4 Plus für Glasfaser-Internet getestet, c't 22/2022, S. 72

[2] Dušan Živadinović, Tunnelbeschleuniger, Fritzbox-VPN: Warum WireGuard cool ist, wie man es konfiguriert, c't 23/2022, S. 68

[3] Ernst Ahlers, VPN-Turbo, WireGuard verdoppelt VPN-Geschwindigkeit bei Fritzbox 7590, c't 4/2022, S. 35

[4] Andrijan Möcker, Fritz'sche Brücke, WireGuard-VPN zwischen Fritzboxen und OpenWrt-Routern, c't 8/2023, S. 150

Das Sprachklingeln lauert weit unten in den Ausklappern für die zugewiesenen Rufnummern. Die Wahl zwischen männlicher oder weiblicher Stimme sowie der optional einschaltbare Zusatzklingelton gelten immer für alle Telefone. Einen akustischen Hinweis auf unterschiedliche Rufnummern (Privat, Mobil, Geschäftlich) eines Eintrags gibt es nicht, diese Information erscheint wie vorher nur im Display.

Zurzeit funktioniert das Sprachklingeln nur bei aktiviertem MyFritz-Konto. AVMs verlinkte Datenschutzerklärung verrät, dass die Fritzbox noch nicht zu lokal gespeicherten Soundschnipseln konvertierte Namen mittels eines AVM-Clouddienstes übersetzt. Die Box soll dabei nur die zu wandelnde Zeichenkette übermitteln. Kennt der AVM-Dienst diese nicht, fragt er beim Amazon-Dienst Polly an.

## Positiv durchgelassen

Weiterleitungen und Rufsperren für ankommende Anrufe kann man nun auf eine einzelne eigene Rufnummer beschränken. Mit dem neuen Rufnummernbereich „Nicht im Telefonbuch“ weist die Box unbekannte Anrufer generell ab und leitet ihre Anrufe nicht weiter. So wird das Telefonbuch zu einer Positivliste für erwünschte Kontakte.

Mit der neuen Firmware bekommen AVM-Telefone einen Terminkalender dazu. Einträge erzeugt man übers Telefonmenü bei den „Komfortdiensten“. Komfortabler ginge das Befüllen des Kalenders freilich per Browser übers Fritzbox-Menü. Die Krönung wäre das Synchronisieren mit Smartphones und externen Diensten über das CalDAV-Protokoll. Termine wie auch Weckrufe sagen die Fritz-Fons auf Wunsch ebenfalls an. Kurzwahlen für die Tasten 2 bis 9 lassen sich am Telefon jetzt per langem Drücken anlegen.

## Mobilfunk-Bonbons

Fritzboxen können schon länger Mobilfunksticks per Failover/Fallback als zweiten Internetzugang nutzen, um Ausfälle des Hauptanschlusses (DSL, TV-Kabel etc.) zu überbrücken. Das klappte nun erstmals auch über den USB-C-Port eines 5G-Mobilfunkrouters, in unserem Versuch ein Zyxel NR2101.

Zwar hat dieser Router auch einen Gigabit-Ethernet-Port, sodass man ihn an den WAN-Port einer Fritzbox hängen könnte. Aber USB ist praktischer, weil der Mobilrouter darüber auch Strom bezieht und das Netzteil erspart.

Fritzboxen mit eingebautem Mobilfunkmodem können jetzt eine der SIM-Karte zugeordnete Rufnummer in die Fritzbox-Telefonie einbinden. Auf einer 6850 5G war der Vorgang mit drei simplen Klicks erledigt. Dazu muss der zur Karte gehörende Tarif den Telefoniedienst über VoLTE enthalten.

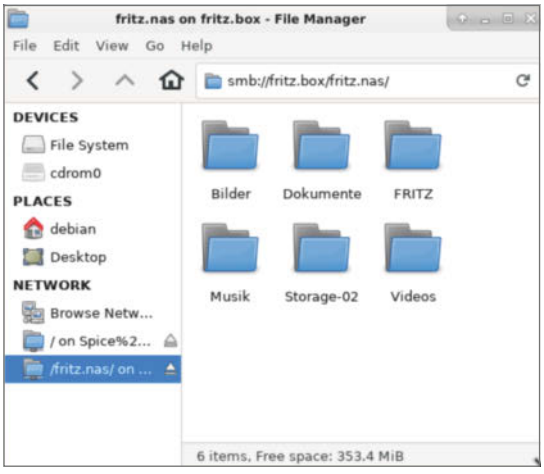
## Geschmeidiger vernetzt

Seit FritzOS 7.50 sendet die Fritzbox auch Bonjour-Annoncen, um ihre Dienste im internen Netz zu annoncieren. Das nutzen Fritz-Apps, um Fritzboxen schneller zu finden. Nicht nur Windows, sondern jetzt auch Linux- und macOS-Anwender sehen in der Netzwerkübersicht automatisch die Fritzbox-Angebote und können mit einem Klick auf NAS-Inhalte und das Webinterface zugreifen, ohne den Hostnamen oder die IP-Adresse des Routers kennen zu müssen. Ferner annonciert die Fritzbox Dienste, die für Programmierer interessant sein dürften, darunter den für Skript-Projekte genutzten TR-064-Port (http://fritz.box:49000/tr64desc.xml).

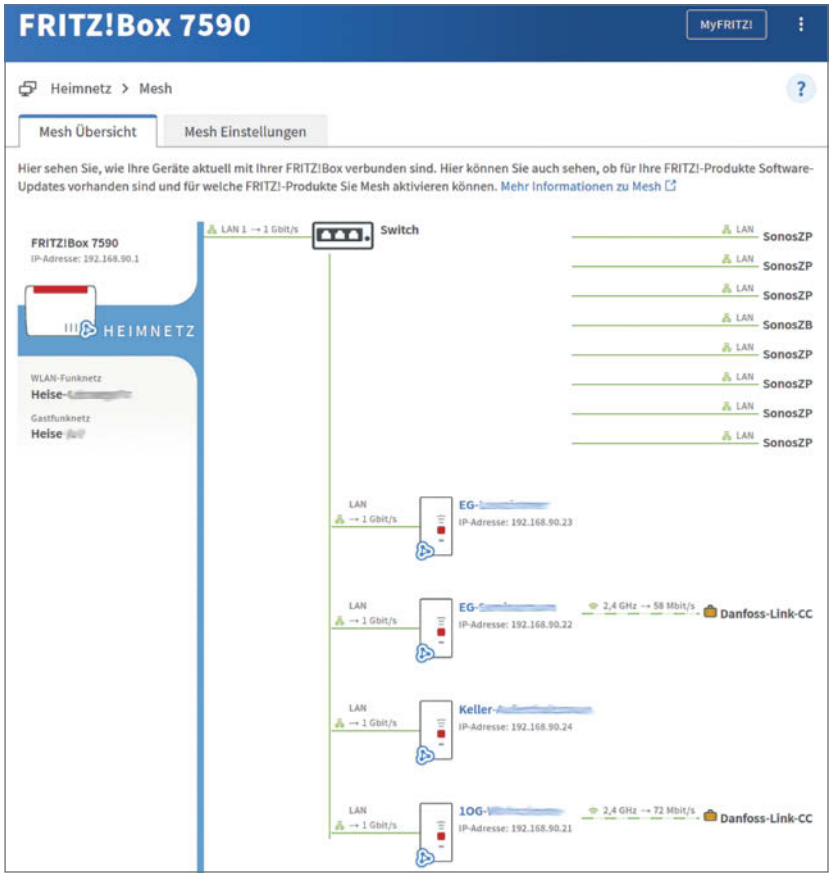
Die veraltete Provider-Fernwartung gemäß TR-069 hat AVM durch die flexiblere und abwärtskompatible Variante TR-369 ersetzt. So muss man sich jetzt nicht mehr per Browser direkt auf der Fritzbox anmelden, sondern kann über den MyFritz-Dienst aus der Ferne Statusinformationen der Box – etwa Verbindungs- und Anschlussparameter – auslesen oder Firmware-Updates anstoßen.

## Netz-Feinschliff

Für aktuelle Fritzbox-Modelle hat AVM eine automatische Priorisierung im internen Netz und im Gastnetz eingeführt. Die Funktion soll die verfügbare




**Fritzboxen kündigen ab FritzOS 7.50 Dateifreigaben auch per mDNS an. Die finden macOS- und Linux-Systeme ebenso wie Windows 11 automatisch und bieten sie in der Netzwerkübersicht zum Einbinden an.**




**In der Mesh-Übersicht zeigt FritzOS auch Switches an. Hier hat es einen solchen aber mit den Koax/Ethernet-Adaptern fürs Weiterleiten des LANs übers TV-Kabelnetz verwechselt.**

Internetbandbreite fairer verteilen. Diese und die schon vorher mögliche Priorisierung einzelner Netzwerkgeräte wirkt nun auch auf IPv6-Verkehr.

Im 5-GHz-Band stört oft ein erzwungener Kanalwechsel. Er führt zu einer kurzen WLAN-Unterbrechung, wenn die Fritzbox Radarsignale erkennt. Dann wechseln viele Clients auf das 2,4-GHz-Band, wo der Verkehr wegen frequenzmäßig schmalerer Signale und mehr Nachbar-Konkurrenz deutlich langsamer fließt. Das optimiert AVM nun bei mehr Boxen mit Zero-Wait-DFS. Nach dem Erkennen eines Radarpulses wechselt der Router vorübergehend auf die 5-GHz-Kanäle 36 bis 48, sucht im Hintergrund nach radarfreien Frequenzen und geht dann auf höhere, schwächer belegte Kanäle.

Fritzboxen können schon länger als Mesh-Repeater arbeiten, um die WLAN-Abdeckung des Routers am Internetanschluss zu vergrößern. Als Mesh-Repeater halten sie die Verbindung zur Zentrale aber nur in einem WLAN-Band. Zuerst lernt die 7590 mit der neuen Firmware, dynamisch beide Funkbänder zu nutzen. Das soll die Mesh-Performance optimieren.

## FritzOS 7.56

Mit FritzOS 7.56 führt AVM einen neuen Stromsparmodus und einen Assistenten ein, der den Wechsel auf eine neue Fritzbox erleichtert.

Funktionen des neuen Stromsparmodus findet man auf einer neuen Einstellungsseite, im Menü System/Energiemonitor. Diese vereint die schon länger vorhandenen Energieeinstellungen an einer Stelle. Nun kann man sie auch mit einem einzelnen Sammelschalter aktivieren. Damit werden sowohl das WLAN als auch die LAN- und USB-Schnittstellen gedrosselt, was zu etwas geringerer elektrischer Leistungsaufnahme führt. Beispielsweise übertragen die Ethernet-Ports dann nur noch 100 statt 1000 Mbit/s.

Der neue Wechselassistent übernimmt laut AVM alle wichtigen Einstellungen des bisher genutzten Routers samt angeschlossener DECT-Telefone und anderer Herstellerprodukte, etwa Smart-Home-Geräte. Der Konfigurationsstand einer Fritzbox lässt sich schon seit Jahren in eine Datei exportieren und auf einem neuen Router importieren. Dafür musste man vor FritzOS 7.56 manche Einstellungen kontrollieren und händisch nachstellen. Der neue Assistent tut dasselbe, holt aber auch an den alten Router gekoppelte DECT-Schnurlostelefone (Fritzfons) und Fritz-Repeater zur neuen Box. Bisher musste man solche Fritz-Peripherie manuell neu koppeln.

## Fazit

Die beiden FritzOS-Updates verbessern und beschleunigen die Bedienung der Fritzbox. Dazu tragen auch Details wie Bonjour-Annoncen oder TR-369 sowie die Verbesserungen bei Telefonie und Smart-Home bei. Neben den Arbeiten am modernen VPN WireGuard hat AVM das alte Fritz-VPN nicht vernachlässigt. Es bekam einen Leistungsschub und hat gelernt, auch IPv6 als Tunnel-Transporter zu nutzen.

So demonstriert AVM erneut, dass Produktpflege mehr bedeuten kann, als nur eine kurze Zeit lang bestenfalls gravierende Fehler auszubügeln. Davon dürfen sich andere Routerhersteller gern anregen lassen. (ea) c't

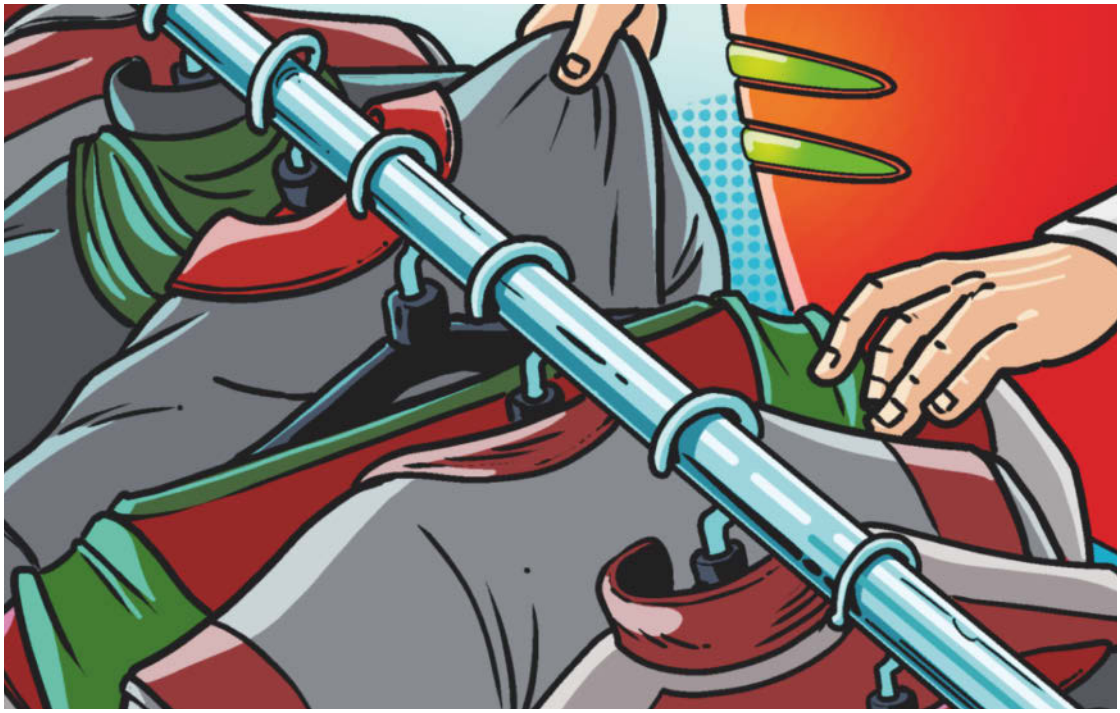


Bild: Michael Vogt

# Die richtige Fritzbox für jeden Zweck

**Wenn ein neuer Router her muss, liegt der Griff zu einer Fritzbox nahe. Die Marke glänzt seit Langem mit vielen Funktionen und stabilem Betrieb. Doch AVMs Produktpalette ist auch im Herbst 2023 schwer überschaubar. Wir schlagen eine Schneise durch den Boxen-Dschungel.**

Von **Ernst Ahlers**

Gründe für einen neuen Router gibt es viele: Der alte fällt aus, der Wechsel zu einem attraktiveren Internetangebot mit anderem Leitungstyp steht an oder der aktuelle Internetverteiler hat Macken in seiner Firmware, die neuen Wünschen im Weg stehen – IPv6 lässt grüßen, mehr dazu im nachfolgenden Artikel. Bei der Routerwahl locken Fritzboxen mit ihren ausgefeilten Funktionen und der bekannt langen Produktpflege.

Die Router berlinischer Herkunft sind zu Recht keine Sonderangebote, was sich auch an hohen Preisen im Gebrauchtmarkt zeigt. Doch erwägen Sie gründlich, ob beim Routerwechsel eine Fritzbox aus zweiter Hand genügt.

Zwar arbeiten die Geräte oft jahrelang stabil. So läuft eine 2013 erworbene Fritzbox 7360 seit einigen Jahren bei den Schwiegereltern mit sehr wenigen Neustarts. Beim Schreiben dieses Artikels war der Router ein halbes Jahr durchgehend online.

Gebrauchtboxen fallen aber früher aus dem Hersteller-Support heraus als Neugeräte. Sie bekommen hernach nur in seltenen Ausnahmen Firmware-Updates, die dann allenfalls kritische Lücken stopfen [1], aber keine neuen Funktionen wie die im vorigen Artikel geschilderten mitbringen.

Ältere Boxen nutzen tendenziell auch ältere WLAN-Technik, weshalb sie sehr schnelle Internetanschlüsse bestenfalls ansatzweise ausschöpfen. Und wenn der Router im Zweitjob mit einem USB-Massenspeicher als zentraler Datentümpel der Familie fungiert, nervt ein veralteter USB-Port mit gemächlichen 480 Mbit/s beim Speichern großer Dateien übers LAN ungemein.

Wer sich für einen neuen Router entscheidet, steht bei AVM vor einer großen Palette. Im Herbst 2023 führt die Website 16 Modelle auf. Wir haben die nützlichsten zehn herausgesucht und ihre wichtigsten Eigenschaften in der Tabelle zum leichteren Vergleich versammelt.

Das wichtigste Auswahlmerkmal ist die Art Ihres (neuen) Internetanschlusses: Telefonleitung (DSL), TV-Kabel (DOCSIS), Mobilfunk (LTE/5G), Glasfaser oder Ethernet. Fritzboxen der letzteren Kategorie kann man über ein separates Modem an beliebigen Anschlüssen verwenden oder kaskadiert zu verschiedenen Netzwerkzonen. Das wird beispielsweise in Wohngemeinschaften nützlich, wo sich mehrere Leute einen Internetanschluss teilen, aber separate (W)LANs haben möchten.

Ein zusätzlicher WAN-Port kann an einem zweiten Internetanschluss beim Ausfall der Hauptverbindung als Failover dienen. Das ist für kleine Firmen und Selbstständige nützlich, die auf den Zugang zum Internet angewiesen sind. Alternativ können sie einen USB-Mobilfunk-Stick oder einen Mobilfunkrouter mit USB-Anschluss an Fritzboxen als Notnagel betreiben. Das Modell 6890 LTE beherrscht den Failover mit seinen DSL- und LTE-Modems ab Werk.

Die Glasfaser-Fritzboxen 5530 und 5590 liefert AVM mit zwei SFP-Steckmodulen für unterschiedliche Anschlusstypen aus. Das für Active Optical Network (AON) arbeitet mit 1 Gbit/s in beide Richtungen. Jenes für Gigabit Passive Optical Network (GPON) überträgt 2,5 Gbit/s im Downstream (Internet ins Haus) und 1,25 Gbit/s im Upstream. Die Boxen haben indes einen SFP+-Slot, der auch Module für 10 Gbit/s aufnimmt, was zur sehr hohen Internetdatenrate in der Tabelle führt.

## WLAN-Wahl

Ein neuer Router sollte heute nach dem aktuellen WLAN-Standard Wi-Fi 6 alias IEEE 802.11ax in beiden wichtigen Frequenzbändern 2,4 und 5 GHz funken,

**Zehn Router für fünf Internet-Anschlusstypen (von links nach rechts, vorn zuerst): Fritzbox 7530AX und 7590AX für DSL, 6660 und 6690 für TV-Kabel, 6850 5G und 6890 LTE für Mobilfunk, 5530 und 5590 für Glasfaser, 4040 und 4060 für Ethernet. Bis auf die Mobilfunkrouter und das Ethernet-Modell 4040 im rot-silbernen Kleid funken alle mit dem modernen Wi-Fi 6.**

## Aktuelle Fritzboxen für fünf Anschlusstypen

| Modell | Internet-Typ | Maximale Datenrate | WAN-Port | WLAN 2,4 GHz | MIMO-Streams | Maximale Bruttorate | WLAN 5 GHz | MIMO-Streams | Maximale Bruttorate | LAN-Ports[1] | davon 2,5 Gbit/s | USB-Ports | DECT-Basis |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7530 AX | DSL | 300 Mbit/s | – | Wi-Fi 6 (11ax) | 2 | 600 Mbit/s | Wi-Fi 6 (11ax) | 3 | 1800 Mbit/s | 4 | – | 1×480 Mbit/s | ✓ |
| 7590 AX | DSL | 300 Mbit/s | 1 Gbit/s | Wi-Fi 6 (11ax) | 4 | 1200 Mbit/s | Wi-Fi 6 (11ax) | 4 | 2400 Mbit/s | 4 | – | 2×5 Gbit/s | ✓ |
| 6660 | TV-Kabel | 6000 Mbit/s | – | Wi-Fi 6 (11ax) | 2 | 600 Mbit/s | Wi-Fi 6 (11ax) | 2 | 2400 Mbit/s | 5 | 1 | 1×480 Mbit/s | ✓ |
| 6690 | TV-Kabel | 6000 Mbit/s | – | Wi-Fi 6 (11ax) | 4 | 1200 Mbit/s | Wi-Fi 6 (11ax) | 4 | 4800 Mbit/s | 4 | 1 | 2×5 Gbit/s | ✓ |
| 6850 5G | Mobilfunk | 1300 Mbit/s | – | Wi-Fi 5 (11ac) | 2 | 400 Mbit/s | Wi-Fi 5 (11ac) | 2 | 867 Mbit/s | 4 | – | 1×5 Gbit/s | ✓ |
| 6890 LTE | Mobilfunk + DSL | 300 + 300 Mbit/s | 1 Gbit/s | Wi-Fi 5 (11ac) | 4 | 800 Mbit/s | Wi-Fi 5 (11ac) | 4 | 1733 Mbit/s | 4 | – | 1×5 Gbit/s | ✓ |
| 5530 | Glasfaser | 10 Gbit/s[2] | – | Wi-Fi 6 (11ax) | 2 | 600 Mbit/s | Wi-Fi 6 (11ax) | 2 | 2400 Mbit/s | 3 | 1 | – | ✓ |
| 5590 | Glasfaser | 10 Gbit/s[2] | 2,5 Gbit/s[3] | Wi-Fi 6 (11ax) | 4 | 1200 Mbit/s | Wi-Fi 6 (11ax) | 4 | 2400 Mbit/s | 4[3] | –[3] | 2×5 Gbit/s | ✓ |
| 4040 | Ethernet | 1000 Mbit/s | – | Wi-Fi 5 (11ac) | 2 | 400 Mbit/s | Wi-Fi 5 (11ac) | 2 | 867 Mbit/s | 4 | – | 1×5 Gbit/s, 1×480 Mbit/s | – |
| 4060 | Ethernet | 2500 Mbit/s | – | Wi-Fi 6 (11ax) | 4 | 1200 Mbit/s | 2×Wi-Fi 6 (11ax) | 2×4 | 2×2400 Mbit/s | 3 | – | 1×5 Gbit/s | ✓ |

[1] ein LAN-Port zu WAN umkonfigurierbar [2] Maximum mit passenden Optikmodulen, siehe Text [3] WAN-Port zu LAN wandelbar

was erfreulicherweise die meisten der gelisteten Modelle tun. Das seit Sommer 2021 erlaubte 6-GHz-Band spielt noch keine große Rolle: Wi-Fi-6E-Clients sind noch rar und eine größere Auswahl an Produkten für den nächsten WLAN-Standard Wi-Fi 7 wird es wohl frühestens 2024 geben.

Wi-Fi 6 bringt besonders in dicht besiedelten Gegenden mit vielen konkurrierenden Netzen mehr Durchsatz und stabilere Verbindungen als die älteren Standards [2]. Bei den Mobilfunk-Boxen ist das schon 10 Jahre alte Wi-Fi 5 (11ac) noch akzeptabel. Denn LTE und auch 5G liefern im Alltag oft nur einige dutzend Mbit/s an, allenfalls ausnahmsweise mal wenige hundert Mbit/s oder mehr.

Die Anzahl der MIMO-Streams entspricht der Zahl der verwendeten Antennen [3]. Sie bestimmt neben dem verwendeten Standard und der Funksignalbreite über die maximal erreichbare Datenrate. Mehr ist besser, aber dann braucht auch die Gegenseite mehr. Notebooks, Tablets und Smartphones funken heute jedoch bestenfalls über zwei WLAN-Antennen.

Dennoch sind Router mit drei oder vier MIMO-Streams die geschicktere, wenn auch teurere Wahl. Sie eignen sich besser, um mit passenden Repeatern ein Mesh-WLAN aufzubauen, das größere Wohnungen lückenlos abdeckt. Außerdem können sie mit der WLAN-Funktion Multi-User-MIMO (MU-MIMO) Daten an mehrere Clients gleichzeitig schicken. Das steigert den Summendurchsatz in der Funkzelle, was allen nützt, auch wenn dieser Fall in der Praxis eher selten eintritt.

## Schnelleres LAN

Lange Zeit war Ethernet mit 1 Gbit/s (Gigabit-Ethernet, GE) die Standardtechnik fürs lokale Netz. Die damit möglichen 115 MByte/s beim Übertragen großer Dateien liegen heute aber weit hinter der Maximalgeschwindigkeit von Festplatten (über 200 MByte/s) und erst recht SSDs (550 MByte/s bei SATA und bis 7500 MByte/s bei NVMe).

Deshalb breitet sich Multigigabit-Ethernet in PCs, Netzwerkspeichern (NAS) und eben auch Routern immer weiter aus [4], jedoch derzeit nur in der kleinsten Evolutionsstufe mit 2,5 Gbit/s (280 MByte/s). Der zugehörige NBase-T-Standard (IEEE 802.3bz) definiert indes auch 5 Gbit/s und 10 Gbit/s.

Soll der neue Router nur das Internet mit höchstens 1000 Mbit/s ins Haus holen, dann genügt GE weiterhin. Wer absehbar einen schnelleren Anschluss buchen will, der profitiert von den Fritzboxen mit 2,5-Gbit/s-Ports. Selbstständige, die dauernd riesige Dateien wie Images virtueller Maschinen im LAN hin und her schieben oder auf dem NAS-lagernde Videos bearbeiten, schaffen sich mit separaten NBase-T-Switches die passende Infrastruktur.

Wenn dereinst ein Internet-Upgrade auf 10 Gbit/s ansteht, die auch im (W)LAN ankommen sollen, dann

genügt keine heute erhältliche Fritzbox. Denn mehr als 2,5 Gbit/s kann aktuell keine an einen einzelnen Host weiterreichen.

## Wi-Fi 7 und Matter vor der Tür

Die oben erwähnten USB-Ports mit 5 Gbit/s, früher als USB 3.0 bezeichnet, heute USB 3.2 Gen 1, haben gegenüber der langsameren Variante (USB 2.0) einen weiteren Vorteil. Sie liefern mehr Strom (0,9 statt 0,5 Ampere) und eignen sich deshalb besser für stromhungrige USB-Geräte, etwa jene ebenfalls erwähnten Mobilfunksticks als Reserve-Internetzugang und USB-Festplatten.

Ein zweiter USB-Port erlaubt, parallel zu solchen Devices auch einen Drucker im Netz zu teilen, falls der nicht selbst WLAN hat. Über die Fritzbox-Funktion „USB-Fernanschluss“ kann man schließlich auch andere Geräteklassen wie beispielsweise Scanner zentral bereitstellen. Indes hat das günstige Glasfasermodell 5530 gar keinen USB-Port.

Ein ISDN-S0-Port etwa für alte Telefonanlagen ist heute eine Seltenheit: Aus unserer Auswahl haben lediglich eine der in zwei Ausführungen erhältlichen Fritzbox 7590 AX und die 6890 LTE den Oldie noch.

Klassischerweise haben Fritzboxen als All-in-one-Router eine Basis für DECT-Funk, über die sie Schnurlostelefone anbinden. Wer nicht übers Festnetz telefoniert, kann darauf verzichten. Soll die Fritzbox aber über DECT-ULE (Ultra Low Energy) Smart-Home-Gadgets wie Lampen, Schaltsteckdosen oder Thermostate steuern, dann fallen Modelle ohne DECT-Basis heraus.

Eine DECT-Basis setzt AVM auch für die Smart-Home-Erweiterung mit Zigbee voraus; die bekommt man in Gestalt des Fritzsmart Gateway, das wir im Artikelschwerpunkt zur Fritzbox als Smart-Home-Zentrale näher vorstellen. Wer damit liebäugelt, sollte im Sinn behalten, dass AVM Anfang 2024 die neuen Fritzboxen 5690 Pro, 5690 XGS und 6670 Cable einführen will, die nicht nur mit nagelneuem Wi-Fi 7 locken, sondern neben DECT auch mit dem Smart-Home-Funk Zigbee. Später sollen sie per Update auch den neuen Smart-Home-Standard Matter erhalten.

Schließlich noch eine kleine Warnung: Es mag reizen, eine Fritzbox vom Provider zu mieten oder gar gratis gestellt zu bekommen. Doch bei „gebrandeten“ Fritzboxen mit angepasster Firmware hängen die Provider mit Updates oft Monate hinterher. Das ist lediglich lästig, wenn es um neue Funktionen geht, aber fahrlässig bis gefährlich, wenn AVM spontan Sicherheitslücken stopfen muss wie Anfang September 2023. Mit einer eigenen Box sind Sie meist besser bedient.

## Fazit

Mit seinem Produktportfolio ist AVM überwiegend auf der Höhe der Zeit. Es gibt Router für alle wesentlichen Internet-Anschlusstypen und die meisten Fritzboxen funken mit dem modernen Wi-Fi 6. Wi-Fi 6E im 6-GHz-Band spielt weltweit noch keine große Rolle. Die Berliner haben sich entschieden, diesen Schritt auszulassen und gleich auf Wi-Fi 7 zu gehen.

Wer jetzt eine neue Fritzbox sucht, wird mit etwas Umsicht das optimale Modell finden, das mindestens für die nächsten fünf Jahre gut ist. Währenddessen kommen gewiss einige nützliche Firmware-Updates und es gibt modernisierte Geräte, wenn der nächste Routerwechsel ansteht. (ea) c't

### Literatur


[1] Ernst Ahlers, Ronald Eikenberg, Jetzt updaten!, Router-Lücke gefährdet viele Fritzbox-Nutzer, c't 6/2014, S. 39

[2] Dr. Guido R. Hiertz, Dr. Sebastian Max, Volle Packung, Wie die Verbesserungen von Wi-Fi 6 wirken, c't 3/2020, S. 112

[3] Ernst Ahlers, WLAN: Häufige Fragen und Antworten, c't 11/2021, S. 178, auch: ct.de/-6033808

[4] Ernst Ahlers, LAN extraflott, Multigigabit-Ethernet für mehr Netzwerkdurchsatz, c't 16/2020, S. 52


# 25 Router auf IPv6 getestet

**Das Internet Protocol Version 6 ist inzwischen essenziell, nicht nur, wenn man im Netz der per DS-Lite angebundenen Schwiegereltern PC-Service leisten will. Doch selbst zehn Jahre nach dem öffentlichen Start in Deutschland scheitern manche Router schon daran, einfach nur Internet per IPv6 bereitzustellen. Wir haben 25 Geräte in vier Szenarien erprobt und schildern, auf welche Details es zu achten gilt.**

Von **Alexander Traud**

Wahrscheinlich ist es Ihnen nicht bewusst, weil es meistens einfach funktioniert: IPv6 ist längst Alltag. So sind Googles Server aus deutschen Netzen schon zu einem hohen Prozentsatz über das moderne Protokoll erreichbar (google.de/ipv6). Doch viele aktuelle WLAN-Router setzen IPv6 falsch um. Dann droht eine aufwendige Fehlersuche.

Deshalb haben wir die IPv6-Funktionen preisgünstiger Wi-Fi-6-Router untersucht. 25 Modelle wohlbekannter wie weniger geläufiger Marken von Amazon bis Zyxel fanden ihren Weg auf den Testtisch.

Es sind überwiegend Geräte für den Anschluss über ein externes Modem, die man in kleinen Netzen typischerweise als alleinigen Router einsetzt.

Vier Marken fehlen: Bei QNAP bietet nur die QHora-Serie überhaupt IPv6, aber das Testmuster traf zu spät ein. Die Geräte von GL.iNet beherrschen nur NAT6 für Mobilfunk-Verbindungen sowie PPPoE-Passthrough und funktionieren damit nicht im deutschen Festnetz, was der Hersteller seit 2019 weiß [1]. Mikrotik schied schon in der Akquise aus, weil deren Router seit 2013 immer noch nicht sauber mit dynamischen IPv6-Präfixen umgehen. Die Speedports der Deutschen Telekom blieben unberücksichtigt, weil sie unter anderem wegen des Point-to-Point-Protocol-over-Ethernet (PPPoE) als alleinigem WAN-Protokoll stark auf das DT-Netz zugeschnitten sind.

Den Rest haben wir in vier zunehmend komplexen Szenarien geprüft: einfaches Websurfen (Internet per PPPoE mit VLAN), Routerkaskaden mit Präfixdelegation (DHCPv6-PD), Routerkaskaden mit PPPoE-Passthrough und Betrieb eines aus dem Internet per IPv6 erreichbaren Servers im internen Netz.

Dabei scheiterten erstaunlicherweise alle Kandidaten irgendwann: meist früh an Selbstverständlichkeiten, manchmal erst spät an Spezialitäten, was wir im Folgenden schildern. Denn aus den Patzern der Firmware-Programmierer können Admins kleiner Netze Nützliches lernen.

Die wichtigsten Dinge erläutern wir en passant in diesem Artikel, tiefergehende Grundlagen und Praxis zu IPv6 liefert [2]. Weil die Testergebnisse so schlecht ausfielen, haben wir auf eine zusammenfassende Benotung diesmal verzichtet.

## Alles variabel

Manche Hersteller führen mehrere Serien auf unterschiedlichen Software-Grundlagen. Deshalb muss beispielsweise Ihr Netgear-Router nicht dieselben Macken haben wie der hier untersuchte, möglicherweise hat er ganz andere. Auch die jeweils aktuelle Version der Router-Firmware spielt eine Rolle.

Unser Blick ist zwangsweise eingeschränkt, denn wir haben nur den Betrieb in den Netzen der Deutschen Telekom und 1&1 ausprobiert. Selbst der Magenta-Riese zeigt kein einheitliches Verhalten, denn er hat Regio-Tarife, die auf eine andere Infrastruktur bauen. Ebenso muss die IPv6-Implementierung der anderen Internetanbieter auch nicht überall gleich sein.

Durch immer neue Provider, etwa bei der jetzt vielerorts eingezogenen Glasfaser, werden die Feldtests für die Hersteller aufwendiger. So hatte selbst Lancom Systems lange Zeit IPv6-Probleme im Netz der Deutschen Glasfaser.

## Internet per PPPoE mit VLAN

Schon beim einfachsten Anwendungsfall Websurfen versagte ein Teil der Testmuster, wenn das Internet über die Telefonleitung (DSL) mittels PPPoE ins Haus kommt. Dieses WAN-Protokoll ist bei DSL-Anschlüssen gebräuchlich, weil es anders als DHCP (Dynamic Host Configuration Protocol, auch IP over Ethernet, IPoE) die Zugangskontrolle per Nutzername und Passwort ermöglicht.

Seit 2007 bietet der größte deutsche Provider, die Deutsche Telekom (DT), in seinem DSL-Netz parallel zum Internet auch Live-Fernsehen über Multicast an (MC-IPTV). Die beiden Dienste laufen über Datenpakete, die mit unterschiedlichen VLAN-Tags markiert sind, Internet mit der VLAN-ID 7, Fernsehen mit ID 8. Inzwischen schwimmt das MC-IPTV zwar auch im Internetdatenstrom mit, aber den gibts nach wie vor nur per VLAN 7.

### v6-Check

Ob Ihr Gerät eine IPv6-Internetverbindung hat, prüfen Sie durch Aufrufen einer Testseite wie icanhazip.com im Browser. Zeigt diese eine IPv6-Adresse mit Doppelpunkten, dann ist alles gut. Erscheint hingegen eine IPv4-Adresse mit Punkten, dann fehlt IPv6. Denn moderne Browser und Betriebssysteme ziehen für den Verbindungsaufbau IPv6 dem alten IPv4 vor.

Lenken Sie Ihren Browser auf die Konfigurationsseite des Routers. Dort halten Sie nach IPv6 im Modus „Automatisch“, „Nativ“ oder „PPPoE“ Ausschau. Oft erscheint die Option erst nach einem Klick auf „Erweitert“ oder einen ähnlich benannten Knopf. Bei Synologys Routern müssen Sie IPv6 nicht nur auf dem WAN-Port, sondern obendrein in den internen Netzen extra aktivieren: Wählen Sie dazu in den Einstellungen der Netzwerkzonen ein Präfix aus. Zwar zeigt der Router die aktuellen GUAs (Global Unicast Addresses) an, aber merkt sich das Subnetz der gewählten.

Weitere Praxistipps zu IPv6 liefert [2]. Doch falls Sie DSL-Kunde von Vodafone sind, gibts nur Internet light: Dieser Provider hatte IPv6 zum Testzeitpunkt in seinem DSL-Netz immer noch nicht aktiviert.

Doch das dafür nötige VLAN-Tagging auf dem WAN-Anschluss (Wide Area Network, Internet) beherrschten in unserem Test längst noch nicht alle Router (siehe Tabelle), obwohl es weltweit einige andere Provider ebenfalls einsetzen.

Solche Geräte kann man trotzdem an Zugängen mit VLAN-Tagging einsetzen, wenn das Modem die VLAN-Marke in den vom Router herausgehenden Verkehr hineinstopft und aus dem hereinkommenden herauszupft. Das tun auf Wunsch beispielsweise die xDSL-Modems von Draytek. Bei anderen Modellen kann man einen konfigurierbaren Switch zwischen Modem und Router schalten, der das erledigt, aber auch zusätzlich Strom kostet.

Manche Hersteller unterstützen zwar VLANs, aber die Einrichtungsassistenten ihrer Router übergehen diese Funktion, darunter beispielsweise die Geräte von Netgear, Wavlink und Xiaomi. Folglich hat man mit jenen Herstellern Probleme, überhaupt eine Internetverbindung herzustellen, ganz unabhängig von IPv6.

Viele Provider erlauben keine dauerhafte Internetverbindung, sondern trennen sie von sich aus nach einer bestimmten Frist, manchmal 24 Stunden, manchmal ein halbes Jahr. Dann muss der Router den Uplink von sich aus automatisch wieder aufbauen, wobei sich das vom Provider zugeteilte IPv6-Adresspräfix ändert. Damit kommen auch nur jene Router klar, die in der Tabellenzeile „PPPoE-Zwangstrennung“ zwei Haken haben.

Sie müssen das alte Präfix invalidieren, damit die Geräte im internen Netz wissen, dass sie sich eine neue IPv6-Adresse setzen müssen. Dafür sollten Router-Advertisement-Pakete ausreichen (Stateless Address Autoconfiguration, SLAAC). Aber manche älteren Betriebssysteme, beispielsweise Windows 8, erwarten zusätzlich einen DHCPv6-Server, der einen per IPv6 erreichbaren DNS-Resolver mitteilt.

## Adresszwang

Deshalb enthalten die meisten Router auch einen DHCPv6-Server. Manche zwingen die (W)LAN-Geräte aber auch unnötigerweise per Stateful DHCPv6, sich ihre IPv6-Adresse dort zu holen.

Verbindet der Router sich neu, dann ändert sich das Präfix und damit die IPv6-Adressen des Routers und seiner Hosts. Nun müsste der DHCPv6-Server von sich aus seine Clients neu konfigurieren können, wofür DHCPv6 den optionalen Nachrichtentyp „Reconfigure“ kennt. Dummerweise unterstützen viele Betriebssysteme wie macOS und Ubuntu das nicht.

Um ein Präfix invalidieren zu können, darf der Router daher nicht auf DHCPv6 bestehen, sondern muss „Stateless DHCPv6“ anbieten. Damit weist er dem Host keine Adresse zu, sondern teilt nur Zusatzinformationen mit, etwa Serveradressen, um Domains in IP-Adressen (DNS) aufzulösen und die Zeit zu synchronisieren (NTP). Setzt der Router hier seine eigene global gültige IPv6-Adresse mit dem aktuellen Präfix ein (Global Unicast Address, GUA, siehe auch [3]), also das IPv6-Äquivalent der öffentlichen IPv4-Adresse, dann kann er diese Information ebenfalls nicht invalidieren. In der Folge kennt der Client nach der Zwangstrennung nur einen unerreichbaren DNS-Server.

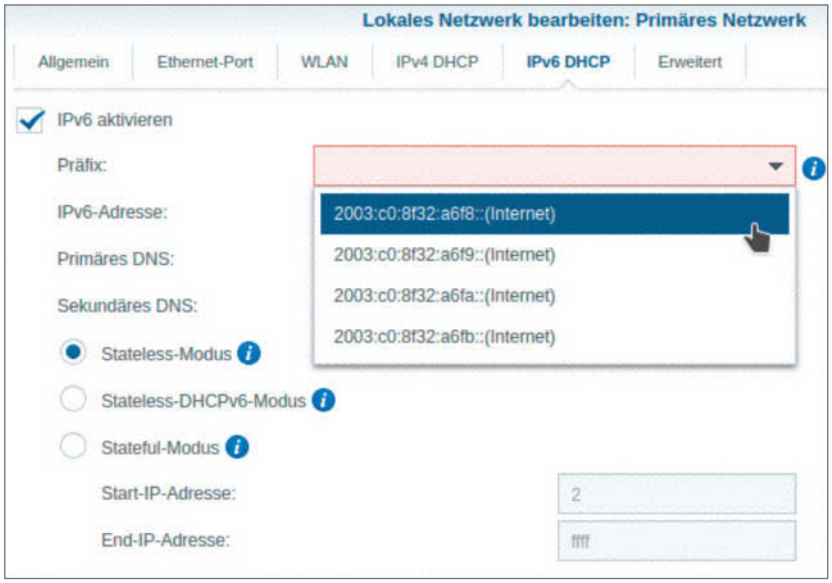
Dann fährt eine pragmatische Nutzerin den Computer herunter, startet den Router neu und danach den PC. Der planerische Kunde greift zur Brechstange, hängt seinen Router an eine Zeitschaltuhr und startet ihn so jede Nacht neu.

Schlauer ist, auf DHCPv6 zu verzichten, indem der Router den DNS-Server über die RDNSS-Option (Recursive DNS Server) in seinen Router-Advertisements mitteilt. Das geht beispielsweise beim Huawei-Router, indem man „Stateful DHCPv6“ ausschaltet und „SLAAC mit RDNSS“ nutzt.

## Verbindungsaussetzer

Netgears RAX40 bewarb nach einer Zwangstrennung sowohl das alte als auch das neue Präfix. Ubuntu arbeitete einfach weiter, weil es zufälligerweise das zweite und damit neue Präfix nutzt. macOS hingegen blieb beim ersten und damit alten Präfix, IPv6 ging kaputt. Ferner fiel uns beim RAX40


**Mikrotik hat es seit 2013 nicht geschafft, seinem RouterOS den korrekten Umgang mit den bei Privatanschlüssen üblichen dynamischen IPv6-Präfixen beizubringen.**




**Bei Synologys Routern muss man IPv6 für Internet und LAN einzeln aktivieren. So kann man festlegen, welche der bis zu fünf internen Netzwerkzonen (VLANs mit eigenen Subnetzen) IPv6 bekommen sollen, wenn das delegierte Präfix zu klein für alle ist.**

auf, dass der Router nach einem Neustart, beispielsweise nach einem Stromausfall oder Firmware-Update, den Provider nicht mehr nach IPv6 fragt.

Amazons eero 6+ versuchte nach der Zwangstrennung, das alte Präfix zu erneuern, selbst nach einem Neustart. Da hilft nicht einmal die Zeitschaltuhr, sondern man muss jedes Mal IPv6 über die Konfiguration aus- und wieder einschalten.

Zyxels Mesh-Router geriet nach der Zwangstrennung komplett durcheinander und versuchte in Dauerschleife erfolglos, die PPPoE-Verbindung wieder aufzubauen. KuWFis AX1800 mochten wir wegen seiner fehlenden Firewall nicht längere Zeit am Internet betreiben. Deshalb ließ sich nicht überprüfen, wie er auf Zwangstrennungen reagiert.

Google Wifi fragte beim Verbinden den Internetanbieter mit der DHCPv6-Option IA_NA nach einer dauerhaften IPv6-Adresse (Non-temporary Address). Dieses Verfahren nutzt aber kein europäischer Provider und ohne IA_NA-Antwort reichte Google Wifi das per DHCPv6 bezogene IPv6-Präfix nicht ins interne Netz weiter.

Apropos Google: Android-Geräte und Chromebooks haben keinen DHCPv6-Client. Solche Hosts können den DNSv6-Server folglich nur aus den Router-Advertisements lernen. Das wissen anscheinend unter anderem Juplink, Tenda und TP-Link nicht. Bei deren Routern muss man den ab Werk aktivierten DHCPv6-Server ausschalten, damit SLAAC mit RDNSS greift. In der Praxis fällt das normalerweise gar nicht auf, denn Domainnamen werden auch über DNSv4 zu IPv6 aufgelöst; das Netz läuft notfalls ohne DNSv6.

Schließlich macht gelegentlich das PPPoE-Passwort Probleme, das man bei vielen Providern im Kundencenter glücklicherweise ändern kann. 1&1 beispielsweise akzeptiert dafür bis zu 40 Zeichen und den vollständigen 7-Bit-ASCII-Zeichensatz. Mit manchen Routern scheiterte dann die Internetverbindung, leider meist ohne klare Ansage der Ursache.

Weil das PPPoE-Passwort beim Verbindungsaufbau im Klartext fließt, konnten wir sieben Geräte identifizieren, die ein langes und komplexes Passwort auf ihrer Konfigurationsseite zwar akzeptierten, dann aber falsch weitergaben (Belkin, D-Link, Google, Linksys, Netgear, Juplink, Synology). Pragmatiker schließen den alten Router vorübergehend wieder an und ändern im Kundencenter das PPPoE-Passwort. Das Testfeld hat uns gelehrt: maximal 15 Zeichen aus dem Vorrat „[a-z][A-Z][0-9]-_@!.“.

## Router-Kaskade mit DHCPv6-PD

Mit als Kaskade hintereinander geschalteten Routern kann man das interne Netz in mehrere Zonen aufteilen. Das nützt beispielsweise Wohngemeinschaften, die sich einen Internetanschluss teilen wollen, wobei aber dennoch jeder Bewohner sein

### Literatur

[1] Andrijan Möcker, Reisefunker, Kompakte WLAN-Router für unterwegs, c't 6/2019, S. 148

[2] Dušan Živadinović, Kleine Expedition, IPv6-Grundlagen und Streifzug durch Ihr eigenes Netz, c't 7/2022, S. 56

[3] IPv6-Adresstypen: ct.de/-3484199

[4] Peter Siering, V6-Fritz, Portfreigaben, IPv6 und DynDNS-Namen auf Fritzboxen nutzen, c't 23/2021, S. 150

## Fritz-Fehlerchen

Wenn sich ein DHCPv6-Client beim Router für Reconfigure anmeldet, dann soll der gemäß der IETF-Norm RFC 8415 das Reconfiguration Key Authentication Protocol (RKAP) nutzen. Doch genau das unterlassen die AVM-Router. Korrekt implementierte DHCPv6-Clients verwerfen deshalb Fritzens Reconfigure-Nachrichten und damit neue Präfixe. Selbst der Trick, den OpenWrt-Client odhcp6c so zu ändern, dass er das fehlende RKAP ignoriert, scheiterte. Denn das weitere Verhalten der Fritzboxen folgt nicht dem einschlägigen RFC 9096. AVM will das Zusammenspiel mit anderen Routern verbessern.

eigenes (W)LAN bekommen soll. Dazu muss der vordere, direkt am Internet hängende Router einen Teil seines vom Provider erhaltenen Präfixes weitergeben (DHCPv6-PD, Prefix Delegation) und sein DHCPv6-Server idealerweise DHCPv6-Reconfigure beherrschen. Beides boten im Testfeld allein AVM und Wavlink.

Ferner muss der vordere Router in seiner Firewall die delegierten Präfixe ausnehmen (Tabellenzeile „Firewall lässt delegierte Präfixe durch“). Nur so kann

### IPv6-Eigenschaften gängiger WLAN-Router mit Wi-Fi 6 (Teil 1)

| Hersteller | Amazon | Asus | AVM | Belkin | Cudy | D-Link |
|---|---|---|---|---|---|---|
| Modell | eero 6+ | RT-AX53U | Fritzbox 5530 Fiber | RT1800 | X6 | R15 |
| Hardware-Version | k. A. | 1.0 | k. A. | k. A. | k. A. | Rev. A |
| Firmware-Version | 6.11.1-46 | 3.0.0.4.386 | 7.29 | 1.1.00 Build 16 | 1.13.6 | 1.06.07 |
| **WAN-Funktionen (Internetanschluss)** | | | | | | |
| IPoE / PPPoE / VLAN-Tagging | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| IPv6-Firewall | ✓ | ✓ | ✓ | ✓ (abschaltbar) | ✓ (abschaltbar mit IPv4) | ✓ (einschaltbar) |
| PPPoE-Zwangstrennung WAN / LAN ok | –/–[2] | ✓/–[3] | ✓/✓ | ✓/✓ | ✓/–[3] | ✓/–[4] |
| PPPoE-Passwort vollständiges 7-Bit-ASCII | ✓ | ✓ | ✓ | – | ✓ | – |
| **LAN und WLAN (internes Netz)** | | | | | | |
| Netzwerkzonen / auch im LAN / mit verschiedenen IP-Subnetzen | 2/–/(✓)[6] | 4/–/– | 2/–/✓ | 2/– /✓ | 2/–/(✓)[6] | 2/–/✓ |
| SLAAC ohne DHCPv6 / Stateless / Stateful | ✓/–/– | –/✓/✓ | ✓/✓/✓ | ✓/–/– | –/–/✓ | ✓/✓/✓ |
| RDNSS in SLAAC | ISP-GUAs | Router-GUA | Router-ULA | ISP-GUAs | Router-GUA | ISP-GUAs |
| ULA | ✓ (immer) | – | ✓ (immer möglich) | ✓ (immer) | – | – |
| DNS-Server vorgebbar / für Gastnetz / für Router selbst | –/–/✓ | –/–/✓ | ✓/–/✓ | IPv4/–/– | ✓/✓/✓ | ✓/✓/✓ |
| LLA transparent zwischen LAN und WLAN | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Funktionen für Server und Kaskaden** | | | | | | |
| DynDNS: IPv4 / IPv6 / per URL / für LAN-Hosts | ✓[7]/–/–/– | ✓/–/–/– | ✓/✓/✓/✓ | ✓/–/–/– | ✓/–/–/– | ✓/GUA/–/GUA |
| Exposed Host bei IPv4 / IPv6 | –/– | ✓/– | ✓/✓ | ✓/– | ✓/– | ✓/✓ |
| Portfreigaben getrennt für IPv4+IPv6 / Portumleitung / IID | ✓/✓/– | ✓/✓/– | ✓/✓/✓ | ✓/✓/– | IPv4/✓/– | ✓/✓/– |
| DHCPv6-PD ins LAN | – | – | ✓ | – | ✓ | – |
| Firewall lässt delegierte Präfixe durch | – | – | ✓ | – | – | – |

✓ ja/vorhanden – nein/nicht vorhanden k. A. keine Angabe
[1] IPv6 fehlerhaft [2] kennt keine dynamischen Präfixe [3] DNSv6 ist GUA [4] altes Präfix nicht invalidiert [5] siehe Text [6] nur IPv4, kein IPv6 [7] mit Secure+-Abo

man Hosts in den Netzen der nachgelagerten Router aus dem IPv6-Internet direkt erreichbar machen, was wiederum nur bei AVM nach etwas Wühlen in den Einstellungen klappte.

Fritzboxen schicken zwar nach einem Präfixwechsel ein Reconfigure an alle DHCPv6-Clients, die sich dafür angemeldet haben. Wegen eines Bugs (siehe Kasten „Fritz-Fehlerchen“) funktionierte das im Test aber nur zwischen Fritzboxen. Damit eignete sich kein einziger Prüfling uneingeschränkt als vorderer Router in einer Kaskade.

Ein extra herangeschaffter DrayTek-Router bot zwar alle nötigen Protokollerweiterungen und -abläufe, aber der Präfixwechsel löste ein Reconfigure nicht automatisch aus. Wir mussten es manuell anstoßen. Ähnlich verhält es sich bei Lancom, deren Router dieses Szenario erst seit dem Sommer 2022 mit LCOS 10.70 beherrschen. Hier kann man aber das Reconfigure in einem Skript hinterlegen, das bei jedem Verbindungsaufbau ausgeführt wird. Deshalb diente ein Lancom-Gerät für die folgende Prüfung als vorgelagerter Router.

## IPv6 achteraus

Wenn die Prüflinge nicht als vorderer Router in einer Kaskade taugen, tun sie dies vielleicht als hinterer, der eine Zone abteilt. Hier fallen all jene gleich durch, die schon beim einfachen Websurfen über PPPoE versagt haben.

Ein nachgelagerter Router in einer Kaskade baut seinen Internet-Uplink typischerweise per IPoE auf, womit WAN-seitig DHCP und DHCPv6 inklusive DHCPv6-Reconfigure gefordert sind. Damit blieben als hintere Kaskadenrouter genau zwei übrig, AVMs Fritzbox und Ubiquitis AmpliFi.

## Kaskade mit PPPoE-Passthrough

Wenn die Kaskade per DHCP/DHCPv6 scheitert, bleibt als Ausweg, dass der hintere Router selbst eine Internetverbindung per PPPoE aufbaut. Dazu muss der vordere Router dieses Protokoll durchlassen (PPPoE-Passthrough).

Solch eine Mehrfach-Einwahl erlaubt aber nicht jeder Provider: Bei 1&1 gehts, bei der Deutschen Telekom nicht. Wieder fallen alle durch, die schon beim Websurfen versagten und wir müssen nur jene Router betrachten, die VLAN-Tagging beherrschen und zwei Häkchen bei „PPPoE-Zwangstrennung“ haben.

Diesmal patzte ausgerechnet jener Kandidat, der neben der Fritzbox bei der Router-Kaskade glänzte: Ubiquitis AmpliFi machte parallel zu PPPoE immer auch IPoE (DHCP), was in der Konfiguration nicht abschaltbar war. So bekamen Hosts im AmpliFi-Netz gleich zwei IPv6-Präfixe und damit zwei IPv6-Internetzugänge, einmal jenen über die PPPoE-Verbindung und außerdem den per DHCPv6 vom vorgelagerten Router bezogenen.

## Internet-Server

Manche wollen einen eigenen, aus dem Internet erreichbaren Server im internen Netz betreiben, sei es für die private Cloud, E-Mail oder auch nur den SSH-Zugang für Wartungseingriffe [4]. Dafür muss ein Router mindestens in seiner IPv6-Firewall einstellbare Dienstfreigaben anbieten. Idealerweise betreibt sein Hersteller einen IPv6-fähigen DynDNS-Dienst, der aus dem internen Hostnamen mit der

| | Dynalink | Edimax | Google | Huawei | Juplink | Keenetic |
|---|---|---|---|---|---|---|
| | DL-WRX36 | BR-6473AX | Wifi | AX3 | RX4-1800 | Carrier |
| | k. A. | 1.0 A | AC-1304 | WS7200 | k. A. | KN-1711 |
| | 1.10.01.222 | 1.0.23 | 14150.43.81 | 11.0.5.5 | 1.1.H | 3.9 Alpha 5 |
| | | | | | | |
| | ✓ / (✓)[1] / – | (✓)[1] / ✓ / – | ✓ / (✓)[1] / nur 2, 7, 10 | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ |
| | ✓ (abschaltbar) | – | ✓ | ✓ (abschaltbar mit IPv4) | ✓ (abschaltbar) | ✓ |
| | – / –[6] | ✓ / –[3] | ✓ / –[5] | ✓ / ✓[5] | ✓ / –[3] | ✓ / ✓ |
| | – | – | – | ✓ | ✓ (max. 15 Zeichen) | ✓ |
| | | | | | | |
| | 2 / – / – | 2 / – / (✓)[6] | 2 / – / ✓ | 2 / – / (✓)[6] | 2 / – / – | 7 / ✓ / (✓)[6] |
| | – / ✓ / ✓ | – / – / ✓ | – / ✓ / – | ✓ / – / ✓ | – / ✓ / ✓ | ✓ / – / – |
| | ISP-GUAs + Link-Local | Router-GUA | Router-GUA | Link-Local | – | Link-Local |
| | – | – | – | – | – | – |
| | IPv4 / – / ✓ | – / – / – | – / – / ✓ | – / – / IPv4 | – / – / ✓ | IPv4 / – / IPv4 |
| | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | | | | |
| | ✓ / – / – / – | – / – / – / – | – / – / – / – | ✓ / – / – / – | ✓ / – / – / – | ✓ / – / ✓ / – |
| | ✓ / ✓ | ✓ / – | – / – | ✓ / – | ✓ / – | ✓ / – |
| | ✓ / ✓ / – | ✓ / – / – | ✓ / ✓ / – | IPv4 / ✓ / – | ✓ / ✓ / – | IPv4 / ✓ / – |
| | – | – | – | – | – | – |
| | – | – | – | – | – | – |

## IPv6-Eigenschaften gängiger WLAN-Router mit Wi-Fi 6 (Teil 2)

| Hersteller | KuWFi | Linksys | Netgear | Strong | Synology | Tenda | TP-Link |
|---|---|---|---|---|---|---|---|
| Modell | AX1800 | MR7350 | RAX40 | Mesh 2100 | RT6600ax | TX9 Pro | AX55 |
| Hardware-Version | DM2-T-MB5EU | 1.0 | 1.0.5 | RN510 | k. A. | k. A. | 1.0 |
| Firmware-Version | 2020-Dec-05 | 1.1.7. 09317 | 1.0.5. 104_1.0.1 | 3.1.0.11 | 1.3.1-9346 | 22.03.02.10 | 1.1.0.64552 |
| **WAN-Funktionen (Internetanschluss)** | | | | | | | |
| IPoE / PPPoE / VLAN-Tagging | ✓/✓/– | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/– | ✓/✓/✓ | ✓/✓/– | ✓/✓/✓ |
| IPv6-Firewall | – | ✓ (abschaltbar) | ✓ | ✓ (einschaltbar) | ✓ | ✓ | ✓ |
| PPPoE-Zwangstrennung WAN / LAN ok | n. t.[4] | ✓/–[3] | –/–[4] | ✓/–[5] | ✓/✓ | ✓/–[5] | ✓/✓ |
| PPPoE-Passwort vollständiges 7-Bit-ASCII | – (max. 32 Zeichen) | – | ✓ | – (max. 32 Zeichen) | – (max. 31 Zeichen) | – | ✓ |
| **LAN und WLAN (internes Netz)** | | | | | | | |
| Netzwerkzonen / auch im LAN / mit verschiedenen IP-Subnetzen | 2/–/(✓)[8] | 2/✓ (nur VLAN3) / ✓ | 2/–/– | 2/–/– | 5/✓/✓ | 2/–/(✓)[8] | 2/–/– |
| SLAAC ohne DHCPv6 / Stateless / Stateful | –/–/✓ | –/✓/– | –/✓/✓ | –/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ |
| RDNSS in SLAAC | defekt | Router-GUA | ISP-GUAs + Link-Local | ISP-GUAs | Link-Local | Router-GUA (nur wenn DHCPv6 ausgeschaltet ist) | Router-GUA (nur wenn DHCPv6 ausgeschaltet ist) |
| ULA | ✓ (immer) | – | – | – | – | – | – |
| DNS-Server vorgebbar / für Gastnetz / für Router selbst | –/–/IPv4 | IPv4/–/– | –/–/✓ | ✓/–/– | ✓/✓/– | IPv4/–/IPv4 | IPv4/–/✓ |
| LLA transparent zwischen LAN und WLAN | ✓ | –4 | ✓ | ✓ | ✓ | ✓ | ✓ |
| **Funktionen für Server und Kaskaden** | | | | | | | |
| DynDNS: IPv4 / IPv6 / per URL / für LAN-Hosts | –/–/–/– | ✓/–/–/– | ✓/–/–/– | ✓/–/✓/– | ✓/✓/–/– | ✓/–/–/– | ✓/–/–/– |
| Exposed Host bei IPv4 / IPv6 | ✓/– | ✓/– | ✓/– | ✓/– | ✓/✓ | ✓/– | ✓/– |
| Portfreigaben getrennt für IPv4+IPv6 / Portumleitung / IID | IPv4/✓/– | ✓/✓/– | IPv4/✓/– | IPv4/✓/– | ✓/✓/– | IPv4/✓/– | IPv4/✓/– |
| DHCPv6-PD ins LAN | – | – | – | – | – | – | – |
| Firewall lässt delegierte Präfixe durch | – | – | – | – | – | – | – |

✓ ja/vorhanden – nein/nicht vorhanden k. A. keine Angabe n. t. nicht testbar
[1] über OpenWrt-LuCI-Oberfläche [2] IPv6 fehlerhaft [3] DNSv6 ist GUA [4] siehe Text [5] altes Präfix nicht invalidiert [6] nur Stateful [7] PPPoE-Wiederanwahl in Dauerschleife [8] nur IPv4, kein IPv6

individuellen Domain des Routers einen globalen Namen fürs Freigabeziel zusammenbaut.

Edimax' BR-6473AX hatte gleich gar keine IPv6-Firewall: Zwar braucht man so keine Freigaben einzurichten, aber seine (W)LAN-Hosts müssen sich selbst gegen Angriffe aus dem IPv6-Internet schützen. KuWFis AX1800 machte als Firewall-Placebo IPv6-NAT. Das schirmte zwar die IPv6-Hosts im (W)LAN ab, aber der Router selbst stand in Richtung Internet komplett offen. Bei D-Link war die IPv6-Firewall ab Werk deaktiviert. Die „Simple Security Firewall" – der Begriff stammt aus einem IETF-RFC – lässt sich mit einem Klick aktivieren.

Dienstfreigaben brauchen als Ziel eine Interface-ID (IID) des Servers. Die vollständige GUA taugt bei dynamischen Präfixen nicht, weil die Dienstfreigabe nach dem nächsten Wiederverbinden wegen des neuen Präfixes nicht mehr funktionieren würde.

Die IID ist die hintere, 64 Bit lange Hälfte der IPv6-Adressen, das im (W)LAN individuelle Merkmal jedes Hosts. Diesen Teil kombiniert der Router mit dem IPv6-Subnetz (8 Bit bei einem delegierten /56-Präfix, im internen Netz meist 0x00) und dem aktuellen Providerpräfix zur Server-GUA. An diese Adresse soll die Router-Firewall anhand von separat anzugebenden Dienst-Ports ausgewählten Verkehr durchlassen.

Weil der ausgehende Verkehr eines Hosts bei aktiven Privacy Extensions wechselnde IIDs enthält, muss der Router eine Eingabemöglichkeit für eine konstante IID bieten [4]. Er darf nicht die erste gesehene als konstant annehmen. Das alles machte im Test nur AVMs Fritzbox richtig, alle anderen Kandidaten versagten in Sachen IPv6-Dienstfreigaben.

Wer dem Betriebssystem des Servers vertraut, kann ihn bei defekten IPv6-Freigaben auch als Ex-

| | Turris | Ubiquiti | Wavlink | Xiaomi | ZTE | Zyxel |
|---|---|---|---|---|---|---|
| | Mox | AmpliFi Instant Router | WL-WN531AX2 | AX3200 | T3000 | Multy M1 |
| | k. A. | AFi-INS-R | Rev. A | RB01 | k. A. | WSM20 |
| | 5.3.11 (HBS) | 3.6.4 RC 1 | 2021-Dec-27 | 1.0.83 | 1.0.0B02 | 1.00(ABZF.4)C0 |
| | | | | | | |
| | ✓/✓/–[1] | ✓/✓/✓ | ✓/✓/✓ | ✓/✓/✓ | (✓)[2]/(✓)[2]/– | ✓/✓/– |
| | ✓ | ✓ | ✓ | ✓ | n. t. | ✓ (abschaltbar) |
| | ✓/–[6] | ✓/✓ | ✓/–[6] | ✓/–[6] | n. t. | –/–[7] |
| | ✓ | ✓ | – (max. 31 Zeichen) | ✓ | – (max. 30 Zeichen) | ✓ |
| | | | | | | |
| | 2/✓/✓ | 2/–/– | 2/–/– | 1/n. v./n. v. | 2/–/– | 2/–/– |
| | –/–/✓ | ✓/–/– | –/–/✓ | –/–/✓ | ✓/–/– | ✓/✓/✓ |
| | Router-ULA | Router-ULA | Router-ULA | Link-Local | – | ISP-GUAs |
| | ✓ (immer) | ✓ (immer) | ✓ (immer) | – | – | – |
| | –/–/✓ | –/– / IPv4 | –/– / IPv4 | IPv4/–/✓ | –/–/– | IPv4/– / IPv4 |
| | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| | | | | | | |
| | –/–/–/– | –/–/–/– | –/–/–/– | ✓/–/–/– | ✓/–/–/– | ✓/–/–/– |
| | –/– | –/– | ✓/– | ✓/– | ✓/n. t. | ✓/– |
| | –/–/– | IPv4/–/– | IPv4/✓/– | IPv4/✓/– | ✓/✓/n. t. | ✓/✓/– |
| | ✓ | – | ✓ | – | – | – |
| | – | – | – | – | – | – |

posed Host komplett freigeben. Das boten im Testfeld nur AVM, D-Link und Synology. Als Notnagel, der höchstens kurzzeitig für Versuche eingeschlagen werden sollte, schaltet man die IPv6-Firewall ganz ab. Diese Option bieten viele Router (siehe Tabelle), aber bei Cudy und Huawei ging dabei immer auch die IPv4-Firewall aus.

## IPv6-Extras

Die Tabellenzeile „Netzwerkzonen“ gibt an, ob neben dem Heim- und dem Gastnetz weitere bei IPv4 und IPv6 voneinander getrennte Bereiche im WLAN möglich sind und ob diese auch als verkabeltes LAN bereitstehen.

Normalerweise können Fritzboxen ihr Gastnetz über einen LAN-Port herausleiten, aber nicht das getestete Modell 5530. Linksys' MR7350 schaltete keinen Port um, sondern aktivierte das VLAN 3 auf den Ethernet-LAN-Buchsen für das Gastnetz.

Die Zeile „ULA“ betrifft die dritte, im internen Netz wichtige IPv6-Adressart neben den GUA (2000::/3, also 2000:0000:0000:0000:0000:0000:0000:0000 bis 3fff:...:ffff, mit Ausnahmen, siehe [3]) und den nur auf Layer 2 (MAC-Schicht) gültigen Link-Local-Adressen (LLA, fe80::/10). Unique Local Addresses (fc00::/7) erlauben, mehrere lokale IPv6-Netze auch ohne ein öffentliches Präfix zu verbinden. Sie sind sozusagen die IPv6-Entsprechung der privaten IPv4-Adressen.

Router mit mehreren internen Schnittstellen, die zum selben Subnetz gehören, müssen Daten zwischen den Interfaces weiterleiten. So sollten IPv6-Pings mit link-lokalen Adressen zwischen WLAN und LAN fließen. Ob das funktioniert, haben wir bei „LLA transparent ...“ verzeichnet. Die Ausnahme war Linksys' MR7350. Bei ihm scheiterte mit PPPoE am Telekom-VDSL nicht nur der IPv6-Ping von LAN zu WLAN, sondern sogar der von LAN zu LAN, und auch IPv6 nach draußen. Mit IPoE hinter einer Fritzbox pingte es hingegen.

Soll im internen Netz ein Werbeblocker wie Pi-hole als DNS-Resolver laufen, macht man ihn den Clients geschickterweise mit seiner ULA bekannt. Denn schon mit dem Browser kommt man IPv6-mäßig nur per wechselnder GUA oder konstanter ULA auf die Konfigurationsseite des Pi-Hole. Dafür muss der Router das Überschreiben des per RDNSS und DHCPv6 angekündigten DNS-Servers mit einer ULA zulassen (Tabellenzeile „DNS-Server vorgebbar“), optional auch separat fürs Gastnetz und den Router selbst.

## Fazit

Nach zehn Jahren öffentlichen IPv6-Betriebs in Deutschland patzte selbst der Klassenprimus Fritzbox immer noch bei Details. Am anderen Ende der Skala waren die Router von Edimax und KuWFi aus unserer Sicht wegen der fehlenden IPv6-Firewall schlicht unbrauchbar. Jene, bei denen IPv6 nach der ersten Zwangstrennung nicht mehr funktioniert, scheiden für den unbeaufsichtigten Alltagsbetrieb aus.

Rechnen Sie bei den übrig bleibenden Modellen spätestens dann mit Problemen, wenn Sie das einfachste Szenario Websurfen hinter sich lassen. Das alles ist indes nur eine Momentaufnahme. Die Hersteller dürften nach unseren Hinweisen an Verbesserungen arbeiten. Einige haben die Anregungen jedenfalls kooperativ angenommen. (ea) c't


Bild: Albert Hulm

# Abschied von der Fritzbox

**Fritzboxen schneiden in vielen Routertests überdurchschnittlich ab und gelten daher als sehr gute Wahl, wenn man einen Router fürs Heimnetz sucht. Profi-Ansprüchen genügen sie aber nicht immer. Ein Leser schildert in diesem Erfahrungsbericht, weshalb und wie er die Hauptfunktionen seiner Box nach und nach mit anderer Hard- und Software ersetzt hat.**

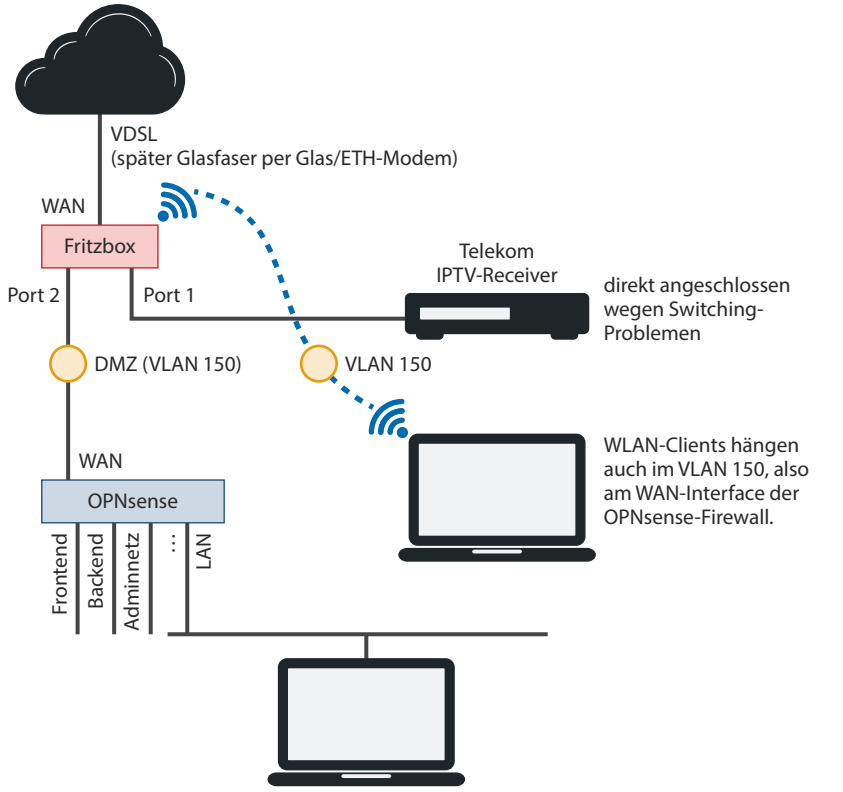
Von **Sebastian Piecha**

Seit der ISDN-Zeit, also vor der kommerziellen Internet-Ära, nutze ich Produkte der Berliner Firma AVM, zuerst ISDN-Karten, später dann mit der Verbreitung von privaten Internetanschlüssen die Fritzboxen als Zugangsrouter. Hatten AVMs ISDN-Produkte die eine oder andere kleine Macke – der CAPI-Treiber zickte gelegentlich –, stellten sich die Fritzbox-Router aus meiner Sicht als Diven mit Starallüren dar. So finden sich in meinem Archiv seit 2006 rund 280 E-Mails zu den unterschiedlichsten Fritzbox-Problemen, über die ich mich mit dem Support des Herstellers ausgetauscht habe. Die Bugs, die mich gestört haben, stecken in den Firewall- und NAT-Implementierungen, in der Telefonie und manchen Apps.

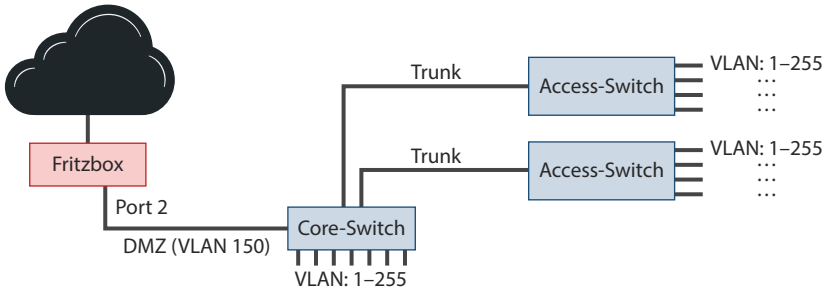
Als berufsbedingt häufiger Fernost-Reisender brauchte ich einen sehr zuverlässigen Router, der

# Netzplan mit Internetzugang via VDSL

Heimnetze können sehr komplex sein. In diesem Beispiel ist eine Infrastruktur mit einer Fritzbox und mehreren Sicherheitszonen zu sehen, welche die Firewall OPNsense aufbaut, denn Fritzboxen eignen sich für maximal zwei Zonen. Im oberen Teil der Grafik ist der logische Aufbau zu sehen, im unteren der physische, beschränkt auf die Switch-Kaskade. Unschön: IPTV-Streams kamen nicht immer an und WLAN-Clients sowie Server standen auf verschiedenen Seiten der Firewall.




Physisch realisiert durch kaskadierte Switches mit mehreren VLANs



möglichst ohne Reparatur aus der Ferne so funktioniert, wie ich ihn konfiguriert habe. Das war bei der Fritzbox nicht immer der Fall. Deshalb suchte ich Alternativen und lagerte mehr und mehr Funktionen auf andere Geräte und Dienste aus.

## IPTV-Hürden

Ursprünglich hat die Fritzbox bei mir als Router den Internetzugang an einem VDSL-Anschluss aufgebaut und per Ethernet und WLAN im Heimnetz verteilt (siehe Grafik „Netzplan mit Internetzugang via VDSL“). Gleichzeitig nutzte ich die eingebaute Telefonanlage und koppelte schnurlose DECT-Telefone von AVM an, auch manche VoIP-Telefone anderer Hersteller. Anfangs handelte es sich um eine Fritzbox 7170 mit vorgeschaltetem VDSL-Modem. Das klappte bis 2017 reibungslos. Nachdem die Telekom ihre IPTV-Architektur umgestellt hatte, blieben Multicast-Pakete stecken, sodass IPTV-Streams nicht zum Wiedergabegerät gelangten.

AVM schrieb dazu sinngemäß, dass T-Home ihr VDSL-Netz von der herkömmlichen Startnetzarchitektur auf eine neue Zielnetzarchitektur umstellt. Nach dieser Umstellung sei die Nutzung von T-Home-Entertain nicht mehr möglich, wenn der Media-Receiver mit der Fritzbox verbunden ist und die Fritzbox die Internetverbindung über ein separates VDSL-Endgerät herstellt.

Somit musste ich die 7170 und das externe VDSL-Modem ersetzen, um IPTV-Streams empfangen zu können. Ich entschied mich für eine Fritzbox 7490.

Aber auch damit holperte die IPTV-Wiedergabe. Der interne Switch der 7490 sollte ja erkennen, an welchem Port der IPTV-Receiver hing und die IPTV-Pakete nur dort ausgeben. Doch er gab sie auch an anderen Ports aus (Multicast-Flooding). Das fiel mir auf, als ich den Verkehr auf meinen nachgeschalteten und zu einer Kaskade verkoppelten Switches analysierte. AVM war überzeugt, dass meine Switches das Problem verursachten, und leistete keinen Support.

Meine vielen Serverdienste (VPN, Mail, Web, Backup, etc.) betrieb ich aus Sicherheitsgründen in mehreren Subnetzen (Netzwerkzonen). Die Fritzbox spannt aber höchstens zwei Zonen auf: Für das Hauptnetz ab Werk den Adressbereich 192.168.178.x und für das Gastnetz den Bereich 192.168.189.x. Die für meine Zwecke erforderliche Subnettierung habe ich daher der Software-Firewall OPNsense übertragen. Dafür richtete ich die Firewall in einer virtuellen Maschine auf einer Server-Hardware ein (Intel Core i5 mit Server-SATA- und Server-Netzwerkkarten).

Den Abschnitt zwischen Fritzbox und OPNsense habe ich zunächst als Transportnetz ausgelegt, der nur für WLAN-Clients zugänglich war (siehe Grafik „Port-Weiterleitung wackelt“). Das war umständlich für die Kommunikation mit den Servern, weil die Clients vor der Firewall standen, die Server aber dahinter. Um mit den Servern zu kommunizieren, schickten sie ihre IP-Pakete an das WAN-Interface der OPNsense und diese leitete die Pakete weiter in die internen Netze. Für Clients aus dem Internet habe ich in der Fritzbox zahlreiche Portweiterleitungen zu den Servern angelegt.

Doch ab 2017 führte ein Bug in FritzOS 6.x dazu, dass die Fritzbox die Weiterleitungen im Abstand von einigen Wochen vergaß oder verschob. Ich schickte AVM einen Bugreport. Die Firma wollte aber anscheinend keine Updates für einzelne Fehler ausspielen und reparierte die Portweiterleitung zusammen mit anderen Bugs erst im Monate später verteilten Update auf FritzOS 7.

## Knistern im NAT-Gebälk

Das dauerte mir zu lange und deshalb schaltete ich die Port-Weiterleitung der Fritzbox ab und richtete hilfsweise eine Exposed-Host-Regel ein: Dabei leitete die Fritzbox sämtliche Pakete, die von außen eingingen, aber von innen nicht angefordert waren, einfach an meine Firewall weiter. Dort bekam jeder Server und Service eine angepasste NAT-Regel, sodass ich fortan zuverlässig aus dem Internet darauf zugreifen konnte.

Auf Dauer ist das aber nicht schön, weil es Pflegeaufwand an zwei Stellen erfordert, in der Fritzbox und in OPNsense. Außerdem nährten die Probleme bei mir Zweifel an der Sicherheit der NAT-Implementierung – ich wollte der Fritzbox diese Aufgabe gar nicht mehr anvertrauen.

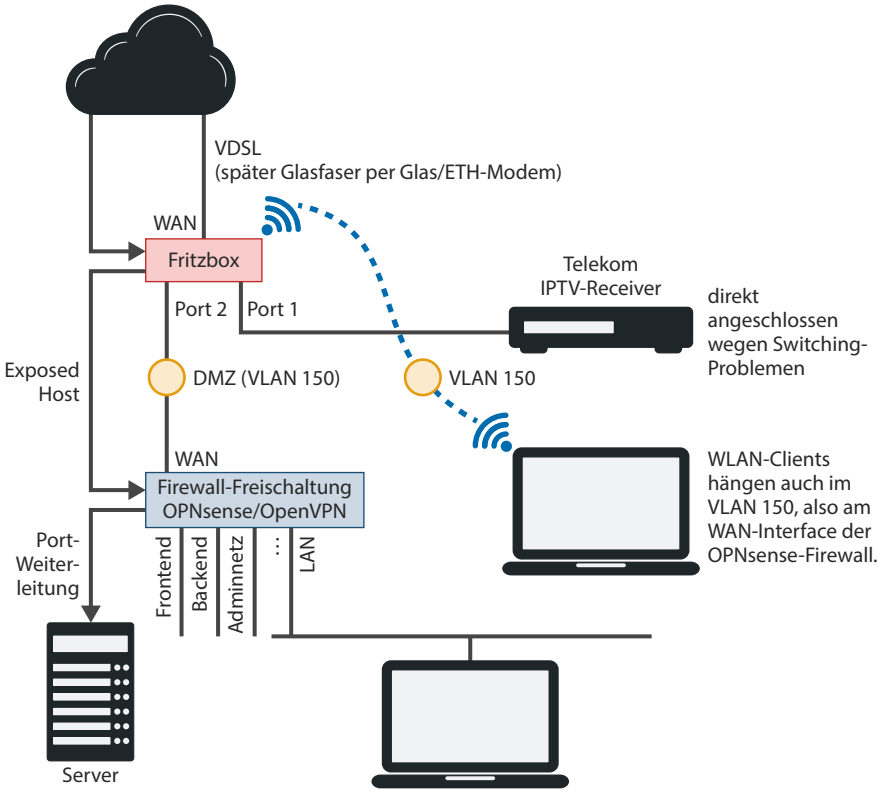
Vor allem, weil mit FritzOS 6.x der Zugriff auf meinen eigenen VPN-Server nur unzuverlässig klappte, habe ich der Fritzbox 2020 schlussendlich die Router-Aufgabe entzogen; auch FritzOS 7.x wollte ich diese Aufgabe nicht anvertrauen. Stattdessen baut nun die OPNsense-Firewall den Internet-Zugang per PPPoE über ein vorgeschaltetes Modem auf (inzwischen Glasfaser statt VDSL).

Seitdem funktionieren NAT und Subnettierung mit dedizierten Regeln zwischen den einzelnen Netzen zuverlässig; ich habe seit der Umstellung keinen einzigen Ausfall dieser Funktionen registriert.

Auch Anforderungen wie mehrere DynDNS-Provider, Priorisierung oder Drosselung unterschiedli-

## Port-Weiterleitung wackelt

Ab 2017 führte ein Bug in FritzOS 6.x dazu, dass die Fritzbox bei Dauerbetrieb Port-Weiterleitungen nach einigen Wochen vergaß oder verschob, sodass beispielsweise der VPN-Server nicht mehr erreichbar war. Anstatt der Port-Weiterleitungen dienten eine Weile lang eine Exposed-Host-Regel und Port-Weiterleitungen in OPNsense als Ersatz.




cher Netzsegmente oder so etwas Banales wie ein DNS mit vorgebbaren Namen und sogar mit unterschiedlichen Antworten für unterschiedliche Zonen erfüllt OPNsense.

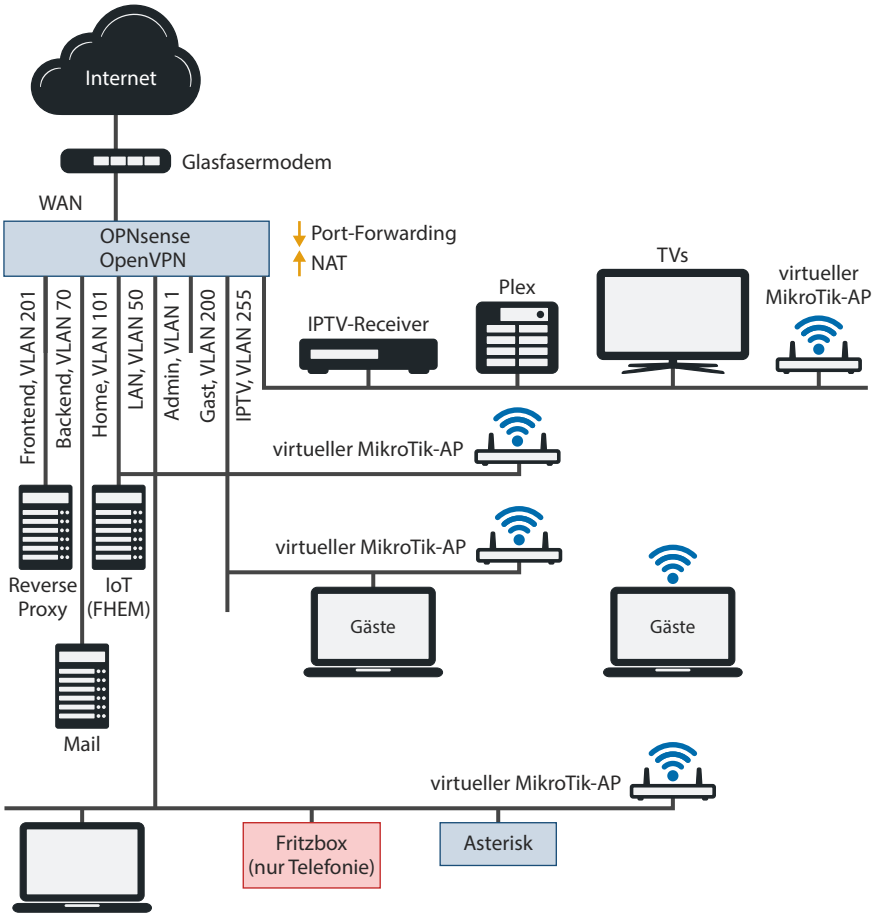
## WLAN-Diät

Die Fritzbox arbeitete fortan nur noch als WLAN-Access-Point und TK-Anlage. Bei WLAN störte aber, dass sie keine individuellen Passwörter je Client, kein WPA2-Enterprise (mit Username/Passwort oder Zertifikat) und vor allem keine Zuordnung von WLAN-Clients zu VLANs beherrscht. Diese Anforderungen mögen für die meisten Nutzer überflüssig sein, sind aber beileibe keine exotischen Funktionen, wie Produkte anderer Hersteller zeigen (Bintec, MikroTik, Grandstream, TP-Link, Ubiquiti, siehe [1]).

So ersetzte ich die WLAN-Funktion der Fritzbox schließlich durch MikroTik-Geräte. Seitdem hat bei mir jeder WLAN-Client ein eigenes Profil, meldet sich mit individuellen Zugangsdaten an (auch Zertifikaten) und landet dann in dem ihm zugewiesenen Netzsegment – eine Trennung nach privaten Geräten, Gästen und heimtelefonierenden IoT-Schachteln ist

## Zonentrennung und WLAN mit individuellen Passwörtern

Die MikroTiks sind als VLAN-fähige APs konfiguriert, die zwei SSIDs ausstrahlen – eine für normale Anmeldung per Passwort (wobei jeder Client ein eigenes Passwort hat) und eine andere für Enterprise-Auth per Zertifikat oder Username/Passwort (nicht alle Clients können sich per Zertifikat authentifizieren). Ein MikroTik-AP hängt einen Client je nach Authentifizierung in das zugehörige VLAN. Die Fritzbox und Asterisk stecken wegen der Telefonie zusammen im LAN.




damit auch im WLAN ein Leichtes. Damit brauchte ich auch das WLAN der Fritzbox nicht mehr und schaltete es ab.

Seitdem läuft auf der Box nur noch der Telefondienst, was sie aus meiner Sicht mal mehr und mal weniger gut erledigt. Beispielsweise habe ich neben der Festnetztelefonie eine Zeit lang auch den Mobilfunk per UMTS-Stick genutzt. Leider kann die Fritzbox nur einen davon einbinden, also auch nur eine Mobilnummer. Und ich erinnere mich noch ungern daran, dass die Fritzbox manchmal unerwartet neu startete, wenn ein USB-Gerät zu viel Strom vom USB-Port zog.

Aber es war eine andere Macke, die den nächsten Diensteumzug auf andere Hardware auslöste: Bei

eingehenden Mobilfunkanrufen signalisierte die Fritzbox nicht die tatsächliche Nummer des Anrufers, sondern die vom vorhergehenden Gespräch. Anfangs fragte ich mich, „Wieso ruft der jetzt schon wieder an?“, bis mir klar wurde, dass die Box meine Schnurlostelefone mit falscher Anrufer-ID fütterte.

Auch diesen Fehler hatte ich AVM gemeldet und wartete anschließend auf den Bugfix. Anders als ich gehofft hatte, kam er aber nicht innerhalb weniger Wochen. Deshalb richtete ich auf einem Raspberry Pi die Soft-Tk-Anlage Asterisk ein. Sie steuert nicht nur einen, sondern gleich mehrere USB-Sticks für mehrere Mobilnummern an. Das gesamte Raspi-Asterisk-Gewerk bindet über Bande mit der Fritzbox auch meine DECT-Telefone ein, sodass ich damit sowohl eingehende als auch ausgehende Mobilfunkgespräche führen kann [2]. Das brauchte ich, weil das Mobilfunksignal bei mir im Haus nicht bis zum Keller reicht, aber durchaus das DECT-Signal der Fritzbox.

So kann ich in beliebigen Räumen des Hauses alle eingehenden Gespräche an irgendeinem der Telefone annehmen und auch entsprechend der eingehenden Verkehrsart zurückrufen – übers Festnetz oder mobil. Auch eine Diktatfunktion, die eingehende Sprachnachrichten zu Text transkribiert und per Signal und Mail verteilt, läuft auf dem Raspi. Außerdem nimmt Asterisk auf dem Raspi eingehende SMS an und leitet sie auf mehrere Handys weiter.

Die Fritzbox baute nur noch die SIP-Verbindung zu den Telefonieservern meines Providers auf und hielt den Kontakt zu den Schnurlos- und Schreibtischtelefonen.

Aber auch so lief nicht immer alles fehlerfrei: Unvergessen die SIP-Probleme nach dem Upgrade von FritzOS 6.x auf FritzOS 7.x. Es hagelte Fehler beim SIP-Connect zwischen Fritzbox und Asterisk auf dem Raspi.

Ich fand damals eine ungewöhnliche Lösung: Ich kompilierte eine freetz-Firmware (mit selbst zusammengestellter Toolchain) auf Grundlage des offiziellen FritzOS 7.x. Dieses FritzOS funktionierte einwandfrei mit Asterisk und verlängerte den Einsatz der Fritzbox um einige weitere Jahre. Ich beließ es dabei, obwohl AVM den Bug einige Wochen nach Einführung von FritzOS 7 behoben hatte.

Ein Fehler blieb: Wenn Anrufer A von außen das Ziel Z bei uns im Haus anrief, haben die DECT- und SIP-Telefone korrekt geklingelt. Wenn ich aber das Gespräch annahm und während des Gesprächs ein anderer Anrufer B ebenfalls Z anrief, dann klingelten nur noch die DECT-, nicht aber die SIP-Telefone.

An den SIP-Telefonen lag es nicht. In Traces war zu sehen, dass die Fritzbox einfach keine Nachrichten an die SIP-Telefone verschickte und es halfen weder Neustarts noch Resets. Also zog ich die betreffenden Geräte von der Fritzbox zur Asterisk-TK um. Und da die Fritzbox immer mal wieder beim Aufbau verschlüsselter Verbindungen zu Telekom-SIP-Servern scheitert, wird sie auch diesen Part bald an Asterisk abgeben.

Derweil bin ich auf ein weiteres Telefonieproblem gestoßen: Ich wollte die FritzFon-App nutzen, um Festnetztelefonate per Smartphone zu führen. Mit AVMs DECT-Telefonen ging das sehr gut, aber sie sind etwas in die Jahre gekommen. Außerdem fallen die DECT-Repeater nach ein paar Jährchen Dauerbetrieb gelegentlich aus und arbeiten erst nach Neustarts wieder normal. Zudem kann man die Schnurlostelefone nur per Hand in eine Nachbarzelle einbuchen – ein Gesprächs-Handover etwa beim Treppengang vom Dachboden zum Keller klappt bei uns im Haus deshalb nicht. Die Fon-App in Verbindung mit guter WLAN-Versorgung sollte es richten. Doch rätselhafterweise klappten damit nur ausgehende Anrufe. Sie klingelten aber gar nicht erst, wenn Anrufe eingingen.

AVM empfahl, die Fritzbox auf Werkseinstellungen zurückzusetzen, was nichts brachte. Auch nach mehrfachem Reset nach AVM-Vorschrift blieben Spuren von freetz auf der Fritzbox 7490 übrig. So schickte mir AVM ein Ersatzexemplar. Aber weder mit der neuen 7490, noch mit einer 7590 klappte das. Schließlich kam heraus: AVM signalisiert Anrufe über einen eigenen Server und damit man mit der Fon-App nicht nur ausgehende, sondern auch eingehende Telefonate führen kann, muss in der Fritzbox die übliche NAT-Betriebsart eingeschaltet sein. Das geht bei mir nicht, weil die Fritzbox im Client-Modus arbeitet und die Router-Funktionen an OPNsense delegiert sind.

## TK-Anlage gesucht

Für meine 7490 bleibt damit immer weniger zu tun. Leider gibt es in Android 12 keine direkte Integration des SIP-Clients mehr, sonst hätte ich die DECT-Telefone mit Handys ersetzt, die mit der Asterisk-TK-Anlage auf dem Raspi sprechen. Vielleicht wird doch nochmal eine eigenständige DECT-TK-Anlage mit einigen wenigen Telefonen und einer Fax-VoIP-Schnittstelle hermüssen. Sie muss nicht viel können, denn das meiste macht sowieso Asterisk. Die Fritzbox wird dann wohl ausgemustert. (dz) c't

### Literatur


[1] Sebastian Piecha, Funkkutscher, Zentrale WLAN-Steuerung für günstige Access-Points, c't 07/2020, S. 100

[2] Sebastian Piecha, Dušan Živadinović, Quadriga, Raspi, Smartphone, Telefon und Fritzbox zum Mobilfunk-Gateway kombinieren, c't 11/2020, S. 26

Bild: Andreas Martini

# Fritzbox als Smart-Home-Zentrale

**Die Fritzbox hat sich mit großem Funktionsumfang und hoher Zuverlässigkeit einen festen Platz in deutschen Haushalten erobert. Hersteller AVM will beim Thema Smart Home Gas geben, doch die Konkurrenz hat schon ein paar Runden Vorsprung.**

Von **Sven Hansen**

Einst hielt das Internet in den meisten Haushalten mit einem Sammelsurium an kleinen Kisten Einzug: zunächst ISDN-NTBA, Splitter, Router, vielleicht eine kleine ISDN-Telefonanlage und später DSL-Modem, Router und manchmal das WLAN noch obendrauf. Dann kombinierte die Fritzbox als erste vor fast 20 Jahren DSL-Modem und Router. Eine Box für alles – das war ihr Versprechen.

Seitdem ist der Funktionsumfang stetig gewachsen und die Fritzbox kommt spätestens dann ins Spiel, wenn ein wenig mehr als Internet und WLAN gefragt ist. In rund jedem zweiten Haushalt Deutschlands steht eine Fritzbox, so AVM. Überprüfen lässt sich das nicht, aber schauen Sie mal bei sich unter den Schreibtisch, beim Nachbarn in den Keller oder bei Ihrer Mutter unter die Telefonbank. Spätestens,

wenn man die Rolle des Familien-Admins innehat, streut man schon wegen der bequemen Fernwartungsoption weitere AVM-Router.

Das Thema Smart Home hatten die Berliner bisher recht stiefmütterlich behandelt. Bis auf die Zwischenstecker DECT 200 und 210, zwei Heizungsthermostate und immerhin eine Retrofit-Lampe war nicht viel geboten. Versuche, den eigenen Funkstandard DECT-ULE außerhalb der AVM-Welt zu etablieren, blieben erfolglos. DECT Ultra Low Energy (ULE) bietet zwar Vorteile im Smart-Home-Bereich. Ursprünglich für die DECT-Telefonie entwickelt, liegt er zum Beispiel außerhalb des stark belegten 2,4-GHz-Funkbandes. Aber derzeit gibt es nur eine Handvoll Komponenten aus dem Smart-Home-Universum der Deutschen Telekom, die kompatibel sind. Panasonic hat seine DECT-ULE-Produkte zurückgezogen und Gigaset nutzt für seine Elements-Serie eine inkompatible Variante.

## Smart-Home-Appetit

Die Energiekrise hat das Spiel geändert, denn Funksteckdosen und Heizungsthermostate verkauften sich im vergangenen Jahr wie geschnitten Brot. Und wo die Fritzbox ohnehin schon an der Wand hängt, warum nicht zu den Produkten von AVM greifen? Zeitweise waren die Komponenten schlichtweg ausverkauft. Ein solches Wachstum macht Appetit auf mehr – das und die Ankündigungen rund um den Smart-Home-Standard Matter brachten frischen Schwung ins AVM-Smart-Home.

Mit dem nun erhältlichen Fritzsmart-Gateway säen die Berliner in genau dem Smart-Home-Feld nach, das von ihnen bisher unbeackert war: Das für rund 70 Euro erhältliche Smart Gateway kann Komponenten über den Funkstandard Zigbee ansprechen, der vorwiegend in smarten Leuchten und Lampen zum Einsatz kommt. Wer ins Gateway investiert, kann nun dutzende Alternativen zur E27-Birne FritzDECT500 in die Fritzbox-Oberfläche einbinden und per Webinterface, App oder DECT-Telefon bedienen. Darüber hinaus erhöht das Gateway sowohl die Abdeckung als auch die maximal mögliche Anzahl von DECT-ULE-Geräten an der Fritzbox.

Das Gateway ist eine Erweiterung für Fritzboxen, auf denen FritzOS 7.5.x läuft. Künftig soll Zigbee in vielen Routern direkt integriert sein, drei Modelle hat AVM bereits für dieses Jahr angekündigt: die 5690 Pro (Internet per Glasfaser oder DSL), 5690 XGS (Glasfaser) und 6670 Cable (TV-Kabel), allesamt zudem Wi-Fi-7-tauglich (mehr dazu im Artikel „Wi-Fi 7: Die nächste WLAN-Generation“). Nach dem Produktstart will AVM sowohl in das Gateway als auch in die neuen Fritzboxen den Smart-Home-Standard Matter implementieren und als kostenloses Update nachreichen. Wie man AVMs Smart Gateway einrichtet, absichert und welche Zigbee-Komponenten anderer Hersteller wie gut funktionieren, erklären die zwei nachfolgenden Artikel.

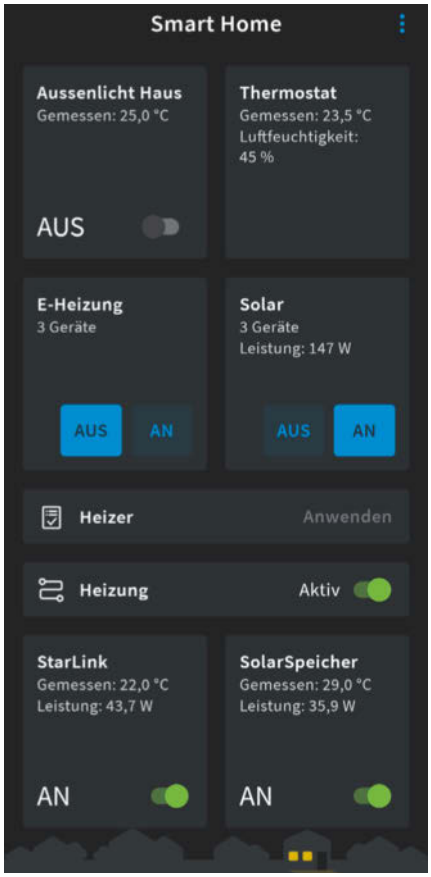
Bild: AVM


**Drei für dieses Jahr angekündigte Fritzboxen werden Zigbee bereits integriert haben und Matter nachreichen, im Bild die 5690 Pro für Glasfaser und DSL-Anschluss.**

## Smarter Vergleich

Doch was leistet das AVM-System im Vergleich zu anderen Smart-Home-Zentralen am Markt? Größter Vorteil des Fritz-Universums: Meist ist die Box schon da. Ein Router läuft ohnehin dauernd, warum ihn also nicht mit Smart-Home-Aufgaben betrauen? Zudem haben viele Nutzer vielleicht schon ein Fritz-Fon gekoppelt, das als Smart-Home-Steuergerät eine gute Figur macht. Ein genauer Blick zeigt die Möglichkeiten, aber auch die Grenzen der um Zigbee erweiterten Fritzbox-Hardware.

Zunächst sollte man sich verdeutlichen, was die Fritzbox nicht ist: Der erweiterte Router ersetzt keine voll integrierten Smart-Home-Systeme wie KNX, Loxone oder Homematic (IP). Wer als Häuslebauer in smarte Technik investiert und Rollladensteuerung, Klimatisierung, Beleuchtung und Alarmtechnik unter einen Hut bringen will, wird kaum zur Fritzbox greifen.




**Mit der für iOS und Android erhältlichen Fritz-App Smart Home steuert man Komponenten auch aus der Ferne an.**

Dafür ist die Auswahl an Komponenten zu mager und das Router-Betriebssystem ist nicht für komplexe Steuerungen gedacht.

Anders schaut es aus, wenn man die Fritzbox mit den ebenfalls geschlossenen Systemen von Aquara, Elesion, Tuyas Smart Life oder mit der Home Base 2 der Telekom vergleicht. Zwar haben diese wiederum weitaus mehr smarte Gerätekategorien im Angebot, aber die Fritzbox-Lösung bietet einen entscheidenden Vorteil: Sie kommt ohne Cloud-Anbindung aus.

Bei der AVM-Lösung werden alle Sensoren und Aktoren per DECT ULE oder über die Zigbee-Bridge lokal verbunden und angesteuert. Die Daten bleiben in der Box oder stecken in einzelnen Komponenten; in jedem Fall verbleiben sie in den eigenen vier Wänden. Trotzdem kann man das AVM-Smart-Home aus der Ferne steuern. Den kryptografisch gesicherten Zugriff für die Fernadministration bringt der Router von Haus aus mit und AVM betreibt für den komfortablen Zugriff darauf einen eigenen DynDNS-Dienst. Mit der für iOS und Android erhältlichen Fritz-App „Smart Home“ klappt das auch vom Handy aus problemlos.

Das Webinterface arbeitet zwar zuverlässig, man muss allerdings Geduld aufbringen. Selbst mit einer eigens aufgesetzten Fritzbox 7590 v2 braucht es Sekunden, bis der Smart-Home-Bereich im Browser erscheint. Über das Webinterface klickt man also vielleicht Smart-Home-Regeln zusammen, für die Bedienung ist es nur ein Notnagel. Das geht besser per Handy, mittels vielleicht sowieso schon überall griffbereit verteilter Fritzfons oder über die FritzDECT-Schalter.

## Brückenbauer

Eine weitere Aufgabe im Smart Home ist es, die Inseln zu verknüpfen, die man sich mit verschiedenen Herstellern eingebrockt hat: etwa die Klima-Sensoren von Netatmo, smarte Schlösser von Nuki oder das Lichtsystem von Philips Hue. Die Fritzbox konkurriert hier mit Spezialisten fürs Verknüpfen, den Steuerzentralen wie Homey, Homeassistant, ioBroker oder OpenHab.

Letztere drei bieten weitaus mehr Integrationsmöglichkeiten als die AVM-Lösung, sind allerdings auch ungleich anspruchsvoller in Konfiguration, Bedienung und Systempflege. Homey hingegen bekommt einfache Bedienung, komplexe Regeln und eine breite Unterstützung smarter Systeme unter einen Hut. Alle vier benötigen allerdings eine ständig durchlaufende Zentrale und kosten damit ab 15 Euro Strom im Jahr.

Anders herum lässt sich die Fritzbox in diese Steuerzentralen einbinden. Die Benutzerverwaltung des Routers erlaubt es, Zugriffsrechte ausschließlich auf seinen Smart-Home-Teil zu beschränken. So lassen sich alle an die Fritzbox angeschlossenen Komponenten über ein solches Sonderkonto steuern oder die von ihnen erhobenen Daten an anderer Stelle speichern. Entsprechende Plug-ins für AVM-Router sind für alle oben erwähnten Smart-Home-Zentralen erhältlich. Hat man sie installiert, lassen sich AVM-Geräte zusammen mit Geräten anderer Hersteller steuern und in Regeln einbinden. Wenn schon eine andere ZigBee-Bridge läuft, braucht man kein Fritzsmart-Gateway.

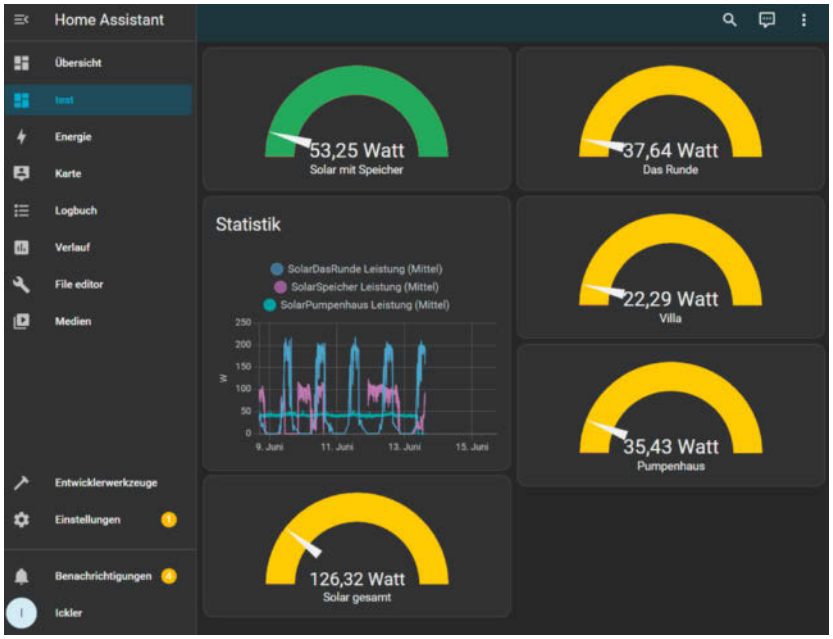
## Matter-Demo auf der IFA

AVM arbeitet an der Matter-Integration von Gateway und Routern, sodass die an die Fritzbox angebundenen Geräte per Matter ansprechbar sind, selbst wenn Zigbee nicht zu den von Matter direkt unterstützten Funkstandards gehört. So kann man das Smart Home mit beliebigen Matter-kompatiblen Apps verwalten, ohne erneutes Anlernen aller Komponenten. Auf der IFA-Ausstellung in Berlin führte die Firma im September vor, wie sie sich die Matter-Integration vorstellt: Auf einem Tablet und in einer Smartwatch läuft Googles Home-App, die Matter-Befehle an das Fritzsmart sendet. Dieses kann dann nicht nur Zigbee-Geräte schalten, sondern auch die in der Demo aufgebauten DECT-Geräte: Leuchtmittel, Heizkörperthermostaten und Steckdosen.

Bis die Implementierung in fertigen Produkten landet, lassen sich AVM-Komponenten über Umwege in Plattformen wie Amazon Alexa, Google Home oder HomeKit integrieren. So macht etwa die App „Homebridge“ die Gerätschaften in der Apple-Welt greifbar, „FB Smart Home“ erledigt den Job für den Google Assistant und Alexa. AVM verlinkt letzteren Drittanbieter sogar direkt auf seiner Support-Seite. Sicherer wäre es, wenn das Angebot direkt von AVM käme.

Wer Zigbee-Komponenten etwa von Philips Hue oder IKEA statt über die Hersteller-Gateways direkt an der Fritzbox anlernt, muss mit Funktionseinbußen rechnen. Die Fritzbox spricht zwar Grundfunktionen an – im Falle eines Leuchtmittels etwa die Helligkeit –, während Feinheiten wie Farbtemperatur bei Weißlicht oder die Farbanzahl bei RGB-Lampen nur in grober Abstufung funktionieren. Viele Zusatzfeatures wie sanft animierte Lichtstimmungen über mehrere Leuchtmittel hinweg oder ein Partymodus fehlen.

Zum derzeitigen Stand heißt es: entweder Hersteller-Gateway oder AVMs Smart Home Gateway. Ein Parallelbetrieb wie bei Ubisys’ Zentrale G1 ist nicht vorgesehen. Wer schon heute von den Möglichkeiten der Hue-App und den zahlreichen kompatiblen Apps von Drittherstellern regen Gebrauch macht, wird daher mit seiner bestehenden Lichtinstallation kaum ins Fritz-Universum umziehen wollen.




**Smart-Home-Zentralen wie Homeassistant greifen über die Fritzbox auf AVM-Zwischenstecker zu und können sie in flexiblen Dashboards bündeln oder statistisch auswerten.**

## Smart-Home-Zukunft

Energie, Komfort, Sicherheit: In zwei von drei Feldern ist AVMs Smart-Home-Angebot durch die Zigbee-Integration nun gut aufgestellt. Das Fritzsmart-Gateway ist eine spannende Option für Fritzbox-Nutzer, die mit der Anzahl ihrer DECT-ULE-Komponenten bereits an die Grenzen ihrer Box gestoßen sind und das System erweitern wollen. Über die Zigbee-Schiene können sie zusätzlich zahlreiche Lichtkomponenten in allen gängigen Bauformen einbinden, die im Fall von IKEA nicht einmal viel kosten.

Auf ein flottes Webinterface wie bei ausgewachsenen Smart-Home-Zentralen muss man verzichten, dafür laufen die Fritz-Apps für iOS und Android rund und manch ein Kunde erfreut sich an der Steuerung per DECT-Knochen. Wer in Zukunft eine neue Fritzbox kauft, braucht bezüglich der Smart-Home-Eigenschaften wahrscheinlich nicht viel zu grübeln. Viel spricht dafür, dass künftige Fritzboxen das Feature gleich an Bord haben.

Die Integration von Zigbee ist nur ein erster Schritt. Spannend wird die konkrete Umsetzung des Matter-Standards: Kann man einmal angelernte Komponenten im Nachhinein flexibel verschieben? Muss man sich mit Basisfunktionen begnügen oder kann man alle Funktionen ansprechen? Erst dann wird sich zeigen, ob das AVM-Versprechen auch im Smart Home aufgeht: eine Box für alles. (sha) c't


Bild: Andreas Martini

# Smart Home mit der Fritzbox einrichten

**Für den Start bringen Smart-Home-Geräte wie die Fritzbox-Erweiterung Fritzsmart gute Anleitungen mit, aber wie man sie optimal betreibt, dazu schweigen sich die Hersteller aus. Daher fassen wir zusammen, was bei uns in der Praxis gut funktioniert hat. Das dürfte auch Leser interessieren, die als Zaungäste nur mal schauen wollen, was in der Fritzbox-Welt Smart-Home-mäßig so abgeht.**

Von **Dušan Živadinović**

Normalerweise startet eine Praxisanleitung für den Smart-Home-Betrieb ohne Umschweife mit der Problemstellung, fügt Klick-Rezepte zur Lösung an und ist damit schnell auserzählt. Und tatsächlich besteht dieser Artikel größtenteils aus Abschnitten zur Konfiguration der Fritzbox-Dienste MyFritz und Push-Mails, inklusive einiger Besonderheiten für den Smart-Home-Betrieb im Zusammenspiel mit AVMs neuem FRITZ!Smart-Gateway, der Kürze halber folgend nur Fritzsmart.

Aber seit Amazon, Apple, Google, Samsung und viele andere Firmen die Flegeljahre der Smart-Home-Technik mit dem Universalstandard Matter beenden wollen, ist das Thema in aller Munde. Matter soll Apples HomeKit, Googles Nest, Zigbee und Bluetooth und andere Smart-Home-Systeme vereinen, was die Auswahl, Einrichtung und Bedienung der diversen Geräte erleichtern soll. Bisher hat aber kein Protagonist schlüssig erklärt, wie die Bedienoberfläche eines Routers und dessen Smartphone-App aussehen könnte, der grundverschiedene Smart-Home-Systeme unter denselben Hut bringen soll. Die Deutsche Telekom bietet zwar mit Home Base 2 ein Gateway für vier verschiedene Smart-Home-Systeme an, aber es stützt sich auf eine Cloud, die man aus Sicherheitsgründen vermeiden will.

Da kommt der Vorstoß des Routerherstellers AVM gerade recht: Die Berliner päppeln jetzt nicht nur das Smart-Home-Mauerblümchen DECT ULE, sondern binden mit dem im Mai erschienenen Router-Kompagnon Fritzsmart auch Zigbee-Geräte in das Smart Home der Fritzbox ein, beides ohne Cloud. Deshalb blicken wir während der Grundeinrichtung auch darauf, was man mit der Integration zweier Smart-Home-Systeme gewinnen oder verlieren kann.

Interessant ist AVMs Zigbee-Gateway auch, weil es für Fritzbox-Nutzer als wichtiger Schritt auf dem Weg zu Matter gilt. Es soll ebenso wie die drei kommenden Fritzbox-Modelle eine Matter-Firmware erhalten, womöglich aber erst 2024. Was man heute schon aus dem Zigbee-Gateway herausholen kann, haben wir in einem mehrwöchigen Praxistest untersucht. Unsere Erkenntnisse beschreiben wir im nachfolgenden Artikel.

Doch bei allem Interesse an AVMs Gateway sollte man nicht vergessen, dass sich jeder Router für ein Smart Home auf Zigbee-Grundlage mit Gateways anderer Hersteller ergänzen lässt; Fritzsmart eignet sich hingegen ausschließlich für Fritzbox-Router. Preisgünstige Zigbee-Gateways bieten zum Beispiel Ikea, Philips und der Discounter Lidl. Lidl hat sogar zwei SilverCrest-Gateways für 20 oder 25 Euro im Angebot. Zigbee-Bausteine wie Leuchten oder schaltbare Steckdosen gibt es im europäischen Handel ab rund 15 Euro. Der China-Basar AliExpress liefert beispielsweise Steckdosen auch schon für unter 10 Euro, wenngleich mit wochenlanger Lieferfrist.


**Das Fritzsmart-Gateway rüstet für Fritzboxen Smart-Home-Funktionen gemäß Zigbee nach, kann aber über die gleiche Taste auch DECT-ULE-Geräte ankoppeln.**

## Nutzen und Spaßeffekt

Der Nutzen wie auch der Spaßeffekt sind offensichtlich: Lampen leuchten in zur Stimmung passenden Farben (zum Beispiel Partyflackern) und die Steckdose schaltet Haushaltsgeräte wie Lüfter oder Waschmaschine auf Signale des Smartphones oder zu geplanter Tageszeit. Steckt in der Dose eine Leistungsmessung, erfasst die zugehörige Smartphone-App auch die Energieaufnahme, vulgo Stromverbrauch.

Dafür verkabelt man das Zigbee-Gateway mit dem Router und konfiguriert und verwaltet das Zigbee-Netz über die zugehörige Smartphone-App. So läuft das bei den Systemen von Philips (Hue), Ikea (Trådfri), Lidl (SilverCrest) und vielen anderen.

Für Fritzbox-Nutzer war bisher daran unschön: Entweder man ließ das DECT-basierte Smart Home zugunsten des großen und oft preisgünstigeren Zigbee-Angebots brachliegen oder administrierte zwei Systeme mit unterschiedlichen Anwendungen. Mit Fritzsmart vereint man beide Welten unter demselben Webinterface der Fritzbox, jedoch zum gehobenen Preis von 80 Euro. Die Zigbee-Geräte wie Lampen, Steckdosen, Taster oder Unterputzmodule meldet man dann ausschließlich bei Fritzsmart an.

Wer schon ein anderes Zigbee-Gateway an der Fritzbox betreibt, kann es zu Gunsten des AVM-Gateways abstöpseln und eine Weile verwahren, bis klar ist, ob man mit dem AVM-Konzept auskommt. Aber vorweg: Es macht durchaus Spaß, auf der Fritzbox DECT-ULE- und Zigbee-Clients in gemeinsamen Routinen zusammenzufassen und etwa Zigbee-Steck-

dosen mit DECT-Tastern zu schalten. Mehr dazu erfahren Sie im nachfolgenden Artikel.

Das stärkste Argument für Zigbee à la AVM ist, dass man damit dem Cloud-Zwang gängiger Zigbee-Anbieter entgeht. Clouds und auch der Verkehr zwischen Heimnetzen und Clouds sind lohnende Angriffsziele. Gelingt es Angreifern, eine der beiden Stellen zu knacken, haben sie Zugriff auf das gesamte Heimnetz. Es wäre aber fatal, wenn sie beispielsweise Fensterkontakte und Bewegungsmelder kontrollieren könnten. Auch ist bei manchen Cloudbetreibern unklar, ob sie die Smart-Home-Daten ihrer Kunden ausschlachten. Nebenbei sorgen lahme Clouds gelegentlich für Irritationen: Wenn erst einige Sekunden nach dem Tastendruck das Licht angeht, denkt man womöglich an einen verlorenen Befehl, drückt vorsorglich nochmal und steht kurz darauf wieder im Dunkeln.

Im Weiteren gehen wir davon aus, dass Sie Smart-Home-Geräte mit der Fritzbox entweder auf DECT-ULE- oder auf Zigbee-Grundlage verwalten wollen. Wenn Zigbee, dann braucht man dafür Fritzsmart von AVM und dieses setzt eine Fritzbox mit DECT-Basis und FritzOS 7.5x voraus. Darauf gründet auch die nachfolgend geschilderte Konfiguration. Sie funktioniert unabhängig davon, ob Sie DECT ULE in Kombination mit Zigbee verwenden oder nur eines der beiden Systeme.

## Weniger Störungen, bessere Abdeckung

Wenn Sie für Zigbee den Fritzsmart-Beiwagen an die Fritzbox koppeln wollen: Nehmen Sie wenn möglich ein Ethernet-Kabel. Bei WLAN kommen Verzögerungen oder Fehler bei Zigbee-Schaltbefehlen um so häufiger vor, je größer die Distanz zwischen Gateway und Fritzbox ist. Das kann man zwar mit kürzerer Strecke zur Fritzbox abmildern, aber dann opfert man etwas von der besseren DECT-ULE-Abdeckung, die Fritzsmart ermöglicht. Mehr zur Strategie beim Aufstellen lesen Sie im nachfolgenden Artikel.

Ist das Gateway an der Fritzbox angemeldet, koppelt man damit Smart-Home-Clients (DECT ULE oder Zigbee) schnell und bequem: Gerät in den Kopplungsmodus bringen, Connect-Knopf des Gateways drücken und nach einigen Sekunden ist der Vorgang abgeschlossen – so soll es sein.

Anschließend können Sie Schaltfunktionen testen, Regeln und Automatisierungen einrichten, auch gemischte mit DECT-ULE und Zigbee-Geräten. Der Taster FritzDECT 400 funktioniert zum Beispiel prima als Funkschalter für Zigbee-Steckdosen. Vorbildlich finden wir, dass AVM alle Inhalte des Smart-Home-Menüs vom Gateway zur Fritzbox spiegelt und umgekehrt. So hat man auf beiden Geräten denselben Stand einschließlich aller Geräte, Automatisierungsregeln oder Statusanzeigen, egal, ob es sich um DECT-ULE- oder um Zigbee-Geräte handelt. Kommende Matter-Implementierungen sollten sich eine Scheibe davon abschneiden.

## MyFritz

Übliche Zigbee-Gateways wie das SilverCrest SGWZ1A1 verbinden sich stillschweigend mit der zugehörigen Cloud – erst diese ermöglicht einer Zigbee-App den Zugriff aus der Ferne über die Router-Firewall hinweg. Auf das Smart Home der Fritzbox greift man hingegen ohne Cloud-Umweg zu, wahlweise per Browser auf dem PC oder per Smartphone-App.

Dafür ist lediglich die IP-Adresse der Fritzbox erforderlich. Die können Apps und Browser wie bei anderen Routern über zuvor konfigurierte DynDNS-Dienste abfragen. AVM unterhält speziell für Fritzboxen selbst einen davon, den MyFritz-Dienst. Hat eine Anwendung die IP-Adresse abgefragt, baut sie dorthin eine TLS-gesicherte Verbindung auf (Transport Layer Security) und man kann dann je nach Anwendung entweder die Fritzbox konfigurieren oder direkt eines der Smart-Home-Geräte.

Falls Sie MyFritz noch nicht eingerichtet haben: Für den Start genügt eine E-Mail-Adresse. Und falls Sie MyFritz bereits auf anderen Fritzboxen verwenden, können Sie dieselbe Mailadresse nehmen; einem Konto lassen sich mehrere Fritzboxen zuordnen. Haben Sie mehrere Adressen, nehmen Sie eine, die Sie dauerhaft nutzen wollen, um wichtige Fritzbox-Mails auch in Jahren zuverlässig zu erhalten.

Wenn die Wahl getroffen ist, melden Sie sich an der Fritzbox an, öffnen das Menü Internet und dort den Punkt MyFritz-Konto. Tragen Sie die Mailadresse ein, öffnen Sie Ihren Mail-Client und darin die inzwischen eingetroffene Mail, die der MyFritz-Dienst zur Bestätigung der Adresse geschickt hat. Klicken Sie auf „Fritzbox registrieren“. Der Browser öffnet dann die Domain myfritz.net und damit ist das MyFritz-Konto angelegt.

Klicken Sie anschließend auf „MyFritz-Konto einrichten“ und vergeben Sie ein sicheres Kennwort; verwahren Sie es sicher in einem Schlüsselbund. Wenn Sie dann auf „Vorgang abschließen“ klicken, ist das Konto betriebsbereit und Sie können darüber unterwegs auf die Fritzbox zugreifen.

Die Fritzbox ist aber auch direkt anhand ihres MyFritz-Hostnamens erreichbar. Das ist eine 16-stellige erwürfelte Zeichenkette, die man sich schlecht merken kann. Legen Sie sie als Bookmark in Ihrem Browser ab oder, falls Sie eine eigene DNS-Domain verwalten, tragen Sie dort einen Alias-Namen Ihrer Wahl für den MyFritz-Namen ein (CNAME, zum Beispiel fbox.meinedomain.de, siehe dazu auch ct.de/wdd5).

Unter anderem kann man auf myfritz.net auch alle mit einer Fritzbox verknüpften Smart-Home-Geräte anzeigen lassen. Bedienen lassen sie sich über diese Webseite nicht; das wäre ja die unerwünschte Cloud-Kommunikation. Stattdessen klickt man auf die Fritzbox und verbindet sich direkt mit ihr.

## Mail-Benachrichtigung

Der „Push Service“ im System-Menü der Fritzbox ist nützlich, um sich auch außerhalb des Heims über Vorgänge informieren zu lassen oder Vorgänge zu archivieren; dann lässt sich später beispielsweise ermitteln, seit wann ein Fehler auftritt. Dafür braucht man wiederum ein Mail-Konto.

Mit der Mailadresse und dem zugehörigen Passwort meldet sich die Fritzbox beim SMTP-Server (Simple Mail Transfer Protocol) Ihres Mailanbieters an. Den Namen des Servers und den Port, über den er angesprochen wird, führt Ihr Mailanbieter auf seinen Webseiten auf. Falls Sie per Google suchen: SMTP und der Name Ihres Mailanbieters führen meist schnell zur Webseite mit den benötigten Angaben. Wenn dort angeboten, verwenden Sie den TCP-Port 465, andernfalls den vom Anbieter angegebenen. Speichern Sie die Einträge und lassen Sie die Fritzbox prüfen, ob sie damit arbeiten kann. Anschließend können Sie weiter unten den Absendernamen nach Bedarf ändern.

Zurück auf der Seite „Push Service“ setzen Sie nun zumindest für „Smart Home“ das Häkchen für den Mailversand. Wenn Sie dann rechts auf Details klicken, öffnet die Box eine Tabelle mit den aktuell konfigurierten Smart-Home-Geräten, für die Sie den Push-Dienst aktivieren können. Falls die Seite noch leer ist, Sie aber ein neues Gerät zur Hand haben, melden Sie es über das Menü „Smart Home/Geräte und Gruppen“ und den Knopf „Gerät anmelden“ an.

Machen Sie sich mit den verschiedenen Push-Varianten vertraut. Wenn der Dienst lediglich im Menü „System/Push Service“ aktiviert ist, informiert die Fritzbox schon mal über Smart-Home-Anmeldevorgänge.

### Lebensdauer DECT-Smart-Home

Manche Bastler unken, dass die Nahfunktechnik DECT bald aussterben könnte, weil die Genehmigung der Regulierungsbehörde 2025 ausläuft und bisher nicht verlängert wurde. Das wäre fatal, weil damit auch die Betriebsgenehmigung für installierte DECT-Geräte erlöschen würde.

Ein Sprecher der Bundesnetzagentur antwortete auf unsere Nachfrage, dass die Behörde viele Zuteilungen erst wenige Monate vor Fristablauf prüft. Speziell für DECT seien „derzeit keine Gründe bekannt, die gegen eine Verlängerung sprechen“. Auch sei die Zuteilung in Deutschland durch die EU-Richtlinie 91/287/EWG gestützt, sodass nach derzeitigem Stand DECT-Geräte „auch über das Jahr 2025 hinaus genutzt werden können“. Fritzbox-User, die ihr Smart Home auf DECT-Basis aufgebaut haben, können sich also zurücklehnen.

Zusätzlich kann man im Menü „Smart Home/Geräte und Gruppen“ Push-Mails für einzelne Aktionen eines Geräts aktivieren. Dann gibt sie etwa über Schaltvorgänge von Steckdosen Bescheid. Zusätzlich kann man für einzelne Geräte auswählen, über welche Aktionen die Fritzbox informieren soll, etwa über kurze und lange Tastendrücke des Tasters Fritz-DECT 400. Solche Informationen bekommt man auch aufs Smartphone, wenn man die Fritz-App Smart Home entsprechend eingerichtet hat.

Nützlich ist der Push-Service jedenfalls oft erst dann, wenn es knirscht. Wenn etwa eine entfernte Zigbee-Lampe zickt, kann das an einem instabilen Funkkontakt liegen. Solchen Fehlern kommt man leichter auf die Spur, wenn man für alle Geräte Push-Optionen einschaltet und sich über Verbindungsverluste per Mail informieren lässt. Hat man seine Pappenheimer wieder im Griff, schaltet man die Push-Mails wieder ab.

Wenn alles zur Zufriedenheit läuft, sichern Sie die Einstellungen über „System/Sicherung“ auf Ihrem PC. Tragen Sie dort auch ein Passwort ein, denn darüber wird die Konfigurationsdatei verschlüsselt, sodass Fremde sie nicht manipulieren können. Falls Sie später eine Einstellungsdatei wiederherstellen: Das läuft wie bei der Fritzbox ab, aber alle Zigbee-Geräte müssen anschließend neu angemeldet werden (Menü „Smart Home/Geräte und Gruppen“, Button „Geräte erneut anmelden“).

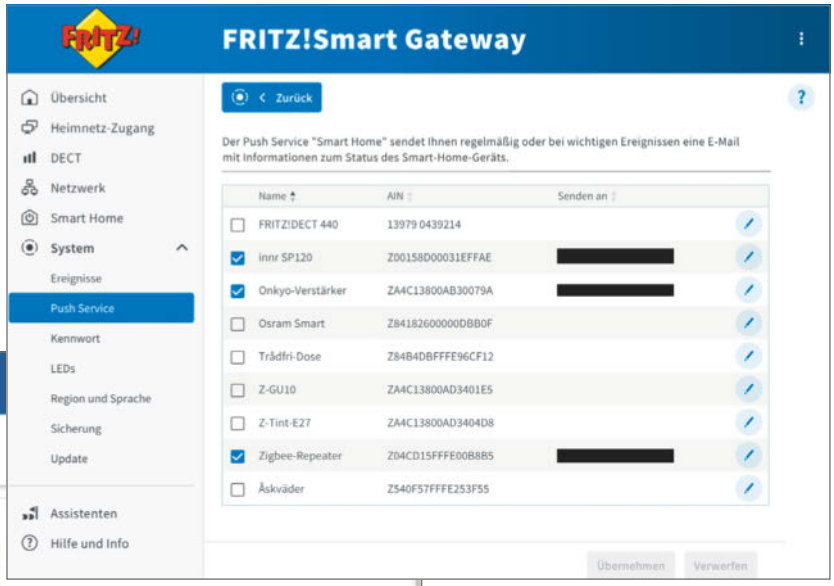
## Fritz-App Smart Home

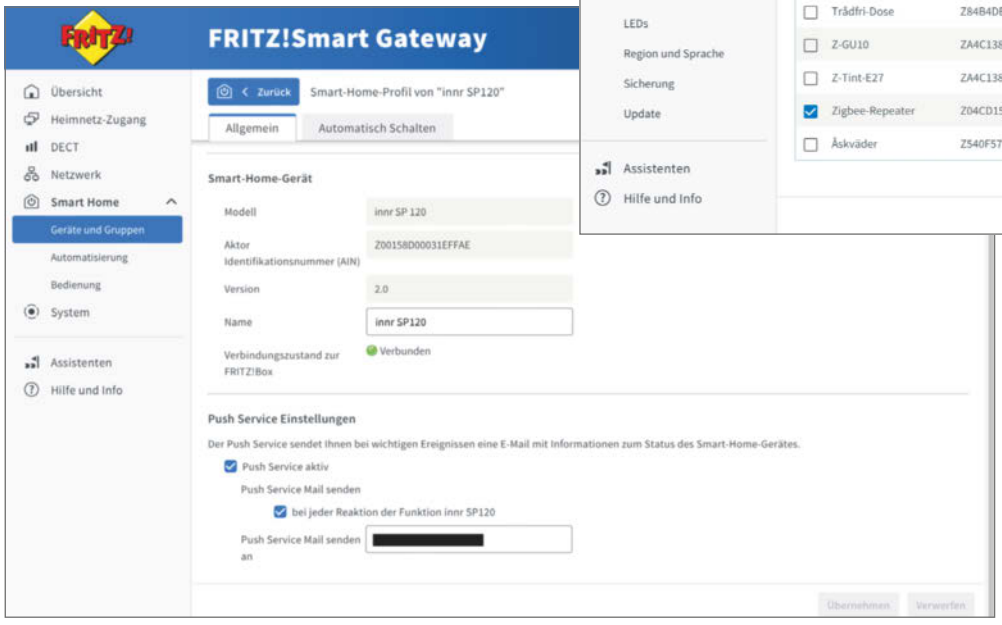
Über einen Browser können Sie auf die Fritzbox bereits aus dem LAN oder per MyFritz aus der Ferne zugreifen. Damit das per Smartphone-App abgesichert klappt, richten Sie am besten in der Benutzerübersicht der Box ein Konto ein, das nur das Smart Home bedienen darf. Unter den Feldern für den Namen und das Passwort aktivieren Sie dann nur die Anwendung „Smart Home“ und ganz unten „Zugang aus dem Internet erlaubt“.

Installieren Sie die FritzApp Smart Home vom Google-Play- oder von Apples App-Store auf Ihr Smartphone und stellen Sie sicher, dass das Smartphone im WLAN Ihrer Fritzbox eingebucht ist. Geben Sie nach dem Start der App die IP-Adresse der Fritzbox ein (bei Werkseinstellung: 192.168.178.1). Tippen Sie auf den Fritzbox-Eintrag und melden Sie sich mit den Zugangsdaten an, die Sie gerade angelegt haben.

Nicht wundern: Bei Clients, die wegen grenzwertiger Distanz zum Gateway die Verbindung gelegent-

**Über die wichtigsten Statusänderungen von Smart-Home-Clients informieren Fritzboxen beispielsweise per Mail. Das lässt sich nutzen, um Funktionsstörungen auf die Spur zu kommen, die wackeligen Funkverbindungen geschuldet sind.**




**Hauseigenen Zwischensteckern spendiert AVM mehr Funktionen als fremden. Beispielsweise kann man die Steckdose innr SP120 über das Webinterface der Fritzbox nicht manuell schalten.**

lich verlieren, lässt die App rund fünf Minuten verstreichen, bis sie dafür „Keine Verbindung zur Fritzbox“ einblendet. Wenn man vor Ende dieser Frist mit der App einer Steckdose ein Schaltsignal schickt, zeigt sie mit dem Button-Zustand zunächst Vollzug an. Der Knopf springt aber ein Sekündchen später auf den Ausgangszustand zurück. Das ist kein Programmierfehler, sondern erwartetes Verhalten, denn der Befehl wurde ja verschickt, aber die Ausführung nicht quittiert.

## Was fehlt, was hakt

Fremde Schaltsteckdosen behandelt AVM noch stiefmütterlich: Anders als bei den eigenen (FritzDECT 200 und FritzDECT 210) bekommen die fremden im Menü „Smart Home/Geräte und Gruppen“ nur das Zusatzmenü „automatisch schalten“. Für die hauseigenen blendet AVM dort Statusangaben und Funktionen zum manuellen Schalten ein.

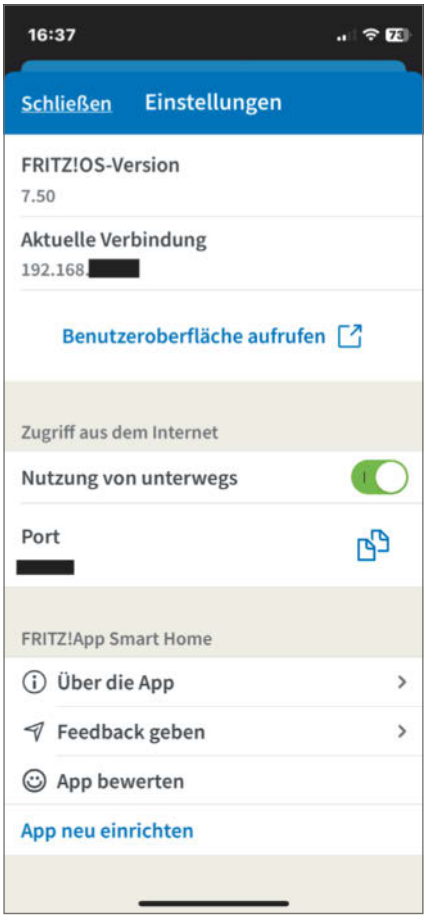
Manuell schalten kann man solche Steckdosen per Browser immerhin über das Menü „Smart Home/Bedienung“ und auch per Smartphone-App oder Smart-Home-Taster, wenn man einen dafür programmiert. Auch liest die Fritzbox anders als bei hauseigenen Steckdosen die Leistungsaufnahme angeschlossener Verbraucher nicht aus. Falls Sie also eine Zigbee-Dose zum Messen angeschafft haben, bleibt Ihnen nur übrig, diese am Gateway des Herstellers zu belassen.

Gleiches gilt für Zigbee-Lampen, die zu einer Party flackern oder gemütliche Lichtstimmungen liefern – Fritzsmart lässt solche Funktionen brachliegen. Möglicherweise ergänzt AVM noch das eine oder andere, aber wann, das steht in den Sternen (siehe c’t-Interview mit AVM, ct.de/wdd5). Wenn man solche Funktionen nutzen und sich nicht an einen Hersteller binden will, ist das Open-Source-Projekt Zigbee 2MQTT einen Blick wert, was aber Bastelarbeit nach sich zieht.

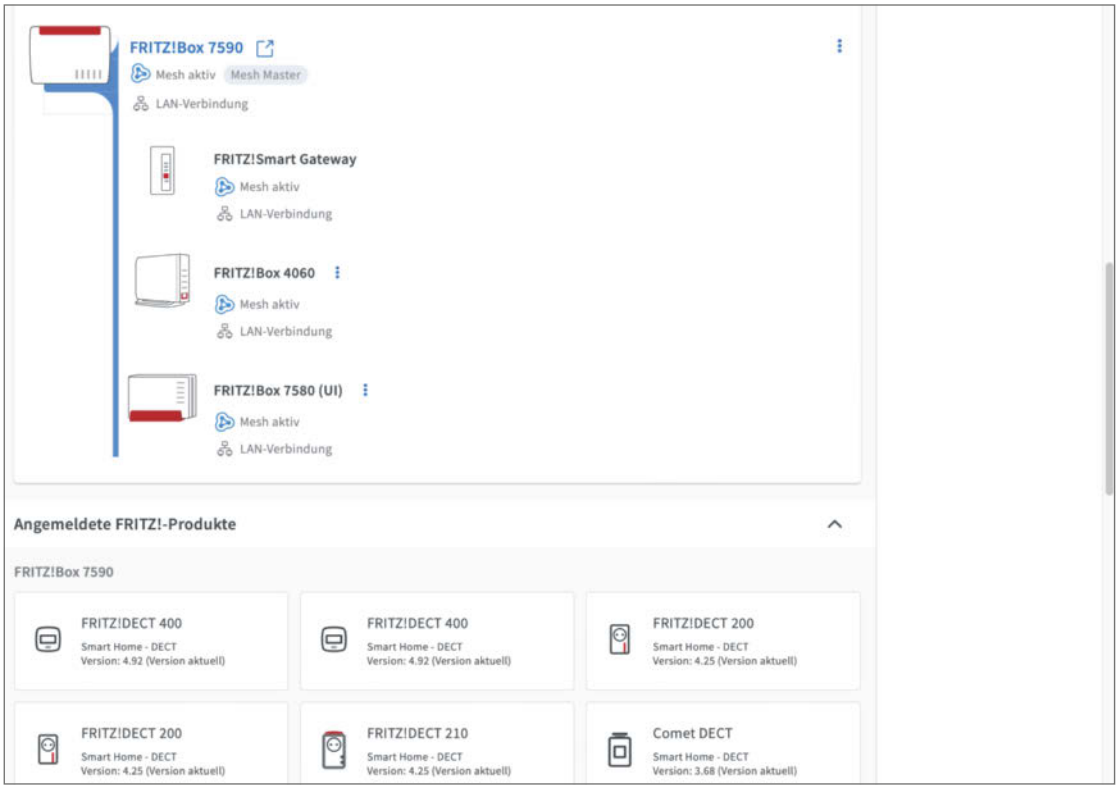
Verwirrend ist, dass im Webinterface der Box die Push-Service-Optionen für Zigbee-Geräte fehlen. Man könnte also denken, dass sie dazu keine Push-Mails verschickt. Doch diese Option findet man durchaus, aber nur im Webinterface des Gateways, dort immerhin an derselben Stelle wie in der Box. Außerdem synchronisieren Gateway und Fritzbox die Sortierreihenfolge der Geräte nicht untereinander, sodass man das immer wieder per Hand nachführen oder mit unterschiedlicher Reihenfolge leben muss.

Wer viele Geräte eingebunden hat, kann in der Ansicht „Geräte und Gruppen“ über das Klappmenü rechts oben unerwünschte Geräteklassen vorübergehend ausblenden, um die Übersicht zu verbessern. Aber nach Verlassen und Wiederkehr blendet die Fritzbox wieder sämtliche Geräte ein. Das hat AVM in seiner Smart-Home-App besser gelöst: Damit kann man in den Einstellungen die Liste der Geräte nach Bedarf sortieren und auch einzelne Geräte dauerhaft aus der Bedienansicht ausblenden. Diese Einstellungen gelten nur für das jeweilige Smartphone, sodass jeder Benutzer nur die Geräte anzeigen lassen kann, die für ihn von Belang sind.

Noch zu feilen hat AVM an der Tabelle „Geräte und Gruppen“. Dort wird immer der „Verbindungszustand




**Um auf Geräte wie Heizungsthermostaten aus der Ferne zugreifen zu können, richtet man auf dem Smartphone die FritzApp Smart Home ein. Dafür gestattet man die „Nutzung von unterwegs“.**




**Richtet man ein MyFritz-Konto für die Fritzbox ein, kann man von dort aus beispielsweise zum Webinterface der Fritzbox wechseln. Zusätzlich liefert dieser von AVM betriebene DynDNS-Dienst Informationen über angeschlossene Smart-Home-Geräte.**

zur Fritzbox“ eingeblendet, auch wenn ein Gerät über das Gateway angekoppelt ist. Nützlich wäre eine Spalte, der man entnehmen kann, ob ein DECT-Client an der Fritzbox oder am Gateway angemeldet ist oder eine eigene grafische Übersicht wie beim Mesh-WLAN. Und wir wünschen uns Export-/Import-Funktionen für einzelne Clients, damit man sie leicht zwischen Fritzbox und Gateway umziehen kann sowie Angaben zur Empfangsgüte (Link Quality) wie sie manche Zigbee-Geräte standardmäßig melden (ct.de/wdd5).

## Schlusswort

Das Smart-Home-Universum ist zwar weiterhin zersplittert, aber mit seinem Zigbee-Gateway zeigt AVM, dass sich mehrere, bisher gänzlich inkompatible Systeme gut unter einer Bedienoberfläche integrieren lassen. Die Menüführung leuchtet unmittelbar ein, auch ohne vorherige Fritzbox-Erfahrung. Das macht Hoffnung auf kommende Geräte mit dem Universalstandard Matter. Auf dem Weg dahin hat AVM den Funktionsumfang des Gateways nach dem Verkaufsstart erweitert: Seit dem Sommer lassen sich auch Zigbee-Taster und Unterputzmodule in das Smart Home der Fritzbox einbinden.

Dennoch sollte man im Sinn behalten, dass Grundfunktionen zwar gut implementiert sind, aber die eine oder andere von Zigbee-Apps gewohnte Sonderfunktion fehlt. Das erschwert Kaufinteressenten die Entscheidung für das Fritzsmart-Gateway. Nutzer, die auf möglichst alle von den Zigbee-Apps gewohnten Funktionen Wert legen, werden damit hadern. Wer die Automatisierung der Fritzbox schätzt, kann sich aber auf neue Kombinationsmöglichkeiten von Zigbee- und DECT-ULE-Geräten freuen. (dz) c't

**Zigbee-Infos, Fritzbox-Tipps, Interview**
**ct.de/wdd5**

# Erweitern Sie Ihren Horizont!

## So reizen Sie Linux voll aus


**Heft + PDF mit 28 % Rabatt**

Linux-User schätzen die vielen Möglichkeiten, das System an ihre Bedürfnisse anzupassen. **c't Linux-Praxis** zeigt Ihnen weitere Stellschrauben, die Sie noch nicht gesehen haben. Aber auch für Ein- und Umsteiger, die auf Windows nicht verzichten wollen, zeigt dieses Sonderheft detailliert, wie Sie beide Systeme sicher miteinander verheiraten. Seien Sie gespannt auf diese Themen:

- Das eigene Linux einrichten, erweitern, optimieren
- Windows und Linux als Dual-Boot
- Linux als Tonstudio
- System anpassen und administrieren
- Daten sichern und wiederherstellen
- **Auch als Bundle mit Buch "Linux – Das umfassende Handbuch" vom Rheinwerk-Verlag erhältlich!**

**Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €**

**shop.heise.de/linux-praxis23**

Bild: Andreas Martini

# Fritzsmart-Gateway in der Praxis

**In der Fritzbox-Erweiterung Fritzsmart steckt ein Doppel-Gateway für das smarte Heim. In unseren Praxistests spielten damit diverse DECT- und sogar mehr Zigbee-Geräte zusammen als erwartet. Nach ein wenig Handarbeit vergrößert das Gateway auch die Abdeckung beider Funknetze.**

Von **Dušan Živadinović**

Mit der Fritzbox-Erweiterung „FRITZ!Smart Gateway“, im Weiteren kurz Fritzsmart genannt, will AVM im Zigbee-Markt mitmischen. Es verschafft Nutzern ein weit größeres Angebot an Smart-Home-Geräten, als bisher auf DECT-Grundlage vorhanden ist. AVM führt in seiner Kompatibilitätsliste 56 Zigbee-Lampen und 10 Zigbee-Steckdosen auf und seit dem Sommer 7 Einfach- oder Mehrfachtaster sowie 6 Unterputzmodule. In unserem Test funktionierten außerdem weitere Steckdosen und Steckdosenleisten, die AVM nicht aufführt.

Jedoch: Man kann Zigbee-Geräte seit jeher mittels preisgünstiger Gateways anderer Hersteller (Philips,

Lidl, Ikea, etc.) auch an der Fritzbox betreiben. Das Fritzsmart hält dagegen und wirft in die Waagschale: ein zusätzliches DECT-Gateway (verdoppelt die maximale Anzahl der DECT-Clients), WLAN- oder LAN-Anbindung an die Fritzbox, USB-Buchse zum Laden von Smartphones sowie weitreichende Integration mit dem Webinterface der Fritzbox – das kann sich auf dem Papier sehen lassen.

Den tatsächlichen Schwächen und Stärken sind wir in einem mehrwöchigen Praxistest mit diversen Zigbee-Lampen und -Steckdosen nachgegangen. In diesem Beitrag fassen wir die damit gewonnenen Erfahrungen beim Netzaufbau und Betrieb zusammen. Im Einzelnen geht es um optimales Aufstellen, Erweitern der DECT-Abdeckung, Kombination von DECT- und Zigbee-Geräten und Erfahrungen mit Zigbee-Bluetooth-Gateways.

Als Grundlage haben wir dafür die im vorhergehenden Beitrag geschilderte Konfiguration verwendet. Damit greift man sicher und ohne Cloud auch aus der Ferne auf das Smart Home zu und lässt sich über Statusänderungen per Mail oder per Fritz-App Smart Home informieren.

## Optimal aufstellen und verbinden

Bevor man das Fritzsmart-Gateway nutzen kann, muss man es per WLAN oder Ethernet mit der Fritzbox koppeln. Das ist mit je einem Tastendruck auf Gateway und Fritzbox erledigt. Anschließend verwaltet man das Smart Home wahlweise über das Webinterface des Gateways oder der Fritzbox; die Geräte synchronisieren sämtliche Smart-Home-Inhalte automatisch. Manche Nutzer dürften zur Kopplung die WLAN-Schnittstelle bevorzugen, denn damit kann man den Aufstellungsort flexibel wählen; auch AVM empfiehlt im Webinterface des Gateways WLAN („Die empfohlene Zugangsart ist die WLAN-Brücke“, FritzOS 7.54).

Doch WLAN sollte nur zweite Wahl sein, denn wenn Zigbee- und WLAN-Geräte im 2,4-GHz-Band funken, bremsen sie sich gegenseitig ähnlich WLAN und Bluetooth. Das zeigte sich schon bei ersten Experimenten in einem Gebäude mit viel WLAN-Verkehr. Manche Schaltbefehle wurden nur mit einigen Sekunden Verzögerungen umgesetzt. Verbindungsabbrüche haben wir in der Zeit nicht beobachtet, sie können bei WLAN- oder Bluetooth-Störungen aber ebenfalls auftreten. Dem gehen Sie mit Ethernet aus dem Weg.

Auch eignet sich Ethernet um so besser, je weiter das Gateway von der Fritzbox stehen soll. In Gebäuden überbrückt WLAN unter guten Bedingungen rund 30 bis 40 Meter, ein Ethernet-Segment kann aber bei üblicher Verkabelung rund 100 Meter lang sein. Dort lässt sich das Signal per Switch auffrischen und dann über das nächste Segment weitere 100 Meter weit bringen.

Falls Ihre Entscheidung dennoch zugunsten von WLAN ausfällt, bleibt der LAN-Anschluss des Fritz-

**Mit dem von AVM gefertigten Fritzsmart-Gateway lassen sich neben Lampen (z. B. Tint E27) auch etliche schaltbare Steckdosen per Zigbee-Funk in das Smart Home der Fritzbox bringen (die Fernbedienung leider nicht): Müllerlicht Tint Smart Power Strip, Ikea Åskväder, Osram Smart+, Ledvance Smart+ Plug EU Indoor und Ikea Trådfri.**

smart-Gateway ungenutzt. Er eignet sich nicht zum Ankoppeln von Computern, Fernsehern oder anderen LAN-Geräten; das Fritzsmart ist kein WLAN-Repeater und damit auch keine WLAN-zu-LAN-Bridge.

## DECT-Abdeckung vergrößern

„Die Fritzbox hat keine Verbindung mehr zum Smart-Home-Gerät xy. Bitte überprüfen Sie, ob Störquellen die DECT-Verbindung beeinträchtigen oder der Abstand zwischen Smart-Home-Gerät und Fritzbox zu groß ist.“ Mit dieser Fehlermeldung informiert die Fritzbox per Mail, wenn die Verbindung zu einem DECT-Gerät abreißt. Damit legt der Hersteller zwar den Finger in die Wunde, hilft aber nicht wirklich. Es gibt schließlich Situationen, in denen die Fritzbox nicht versetzt werden kann, weil dann beispielsweise andere Clients nicht mehr erreichbar wären. Es gibt aber Abhilfe: Man kann entweder die DECT-Abdeckung mittels des Fritzsmart-Gateway vergrößern oder versuchen, die Aufgabe mit Zigbee-Geräten zu erledigen (siehe Abschnitt „Zigbee-Reichweite“).

Zunächst zur DECT-Lösung: Stellt man das Gateway abgesetzt von der Fritzbox auf, erweitert es auch die DECT-Abdeckung, obwohl AVM diesen Vorteil herunterspielt. Doch für Fritzbox-Nutzer ist das Smart-Gateway die bisher einzige Möglichkeit, Smart-Home-Clients außerhalb der Reichweite der Fritzbox zu betreiben und damit die Abdeckung zu vergrößern. AVM hat zwar einen DECT-Repeater im Lieferprogramm, aber der eignet sich nicht für die Smart-Home-Clients, denn ihm fehlt die HAN-FUN-Implementierung (Home Area Network FUNctional protocol). Umgekehrt eignet sich Fritzsmart nicht für DECT-Telefone, sondern nur für Smart-Home-Geräte (DECT ULE, HAN FUN).

Die DECT-Funktion von Fritzsmart kann man nutzen, um beispielsweise getrennte Gruppen von Clients in benachbarten Gebäuden aufzustellen, etwa Doppelhaushälften. Beide lassen sich dann (anders als etwa nach Einbinden in zwei Fritzboxen) trotzdem auf Gateway und Fritzbox über dasselbe Webinterface verwalten und auch automatisieren.

Das Fritzsmart ist jedoch kein DECT-Repeater, mit dem sich die Abdeckung einfach durch Aufstellen vergrößern ließe. Auch fehlt eine Funktion für den automatischen Wechsel (Hand-over) zwischen Gateway und Fritzbox. Stattdessen führt man dem Fritzsmart die DECT-Clients per Hand zu. Ein bereits an der Fritzbox angemeldetes Gerät muss man dafür zuerst vom Router abmelden. Fortan bleibt jedes Gerät der jeweiligen DECT-Basis zugeordnet, auch wenn man es so versetzt, dass es näher an der anderen steht.

Wenn Sie das Gerät in der Fritzbox in einer Automatisierungsvorlage verwendet oder einer Gruppe zugeordnet haben, fehlt es dort nach dem Auszug. Daraus folgt für den Einzug im Fritzsmart: Falls Sie das Gerät auf Fritzsmart in einem neuen Szenario benötigen, gehen Sie wie üblich vor und legen neue Gruppen, Vorlagen oder Routinen an. Wenn das Gerät in den ursprünglichen Gruppen oder Vorlagen laufen soll, müssen Sie es per Hand an den entsprechenden Stellen wieder eintragen.

Damit das bis aufs letzte Detail klappt, empfiehlt es sich, die Gruppen- und Vorlageneinstellungen in der Fritzbox vor dem Umzug zu notieren oder als Screenshots zu archivieren. Das ist mit etwas Arbeit verbunden, aber da Smart-Home-Geräte meist an einem festen Platz bleiben, zieht man sie nur einmal um. AVM würde aber sicher Freunde hinzugewinnen, wenn es Export/Import-Funktionen dafür nachreichen würde.

**Unter den schaltbaren Steckdosen sind auch Modelle, die Messwerte zur Leistungsaufnahme angeschlossener Verbraucher liefern: Tuya Power Plug-001SPB2, Aubess Smart Socket (alias Girier JR-ZPM01), Lidl SilverCrest Zwischenstecker und innr SP120.**

**Seit jeher lassen sich an der Fritzbox auch Zigbee-Gateways anderer Hersteller betreiben, beispielsweise das SilverCrest-Gateway der Supermarktkette Lidl. Mangels Integration in die Fritzbox-Welt führen sie aber ein Eigenleben.**

Im Einzelnen geht man so vor: Öffnen Sie in der Fritzbox das Menü „Smart Home/Geräte und Gruppen“ und archivieren Sie die aktuellen Einstellungen wie beschrieben. Klicken Sie dann weiter unten auf den Button „Gerät löschen“ und dann beim entsprechenden Client rechts in der Spalte auf den Papierkorb. Wenn Sie die Sicherheitsrückfrage abnicken, verschwindet es aus der Ansicht und die Fritzbox entfernt es aus etwaigen Gruppen, Vorlagen, Szenarien und Automatisierungsroutinen. Weitere Clients entfernen Sie auf dieselbe Weise. Klicken Sie zum Schluss auf Fertig. Anschließend sind die aus der Fritzbox gelöschten Geräte frei für Kopplungen mit dem Gateway.

Falls ein Gerät während des Pairings zuerst eine gescheiterte Kopplung meldet und dann eine erfolgreiche: Das passiert, wenn es noch in der Fritzbox eingetragen ist. Dann meldet es sich erneut an der Fritzbox an und nicht am Gateway. Nachdem Sie es gelöscht haben, sollte das Pairing mit dem Gateway ohne Fehlermeldung ablaufen.

Wenn es tatsächlich neu angekoppelt wurde, finden Sie es unter einem neuen, generischen Namen im Menü „Smart Home/Geräte und Gruppen“, beispielsweise „FritzDECT 301 #3“. Nun können Sie die ursprünglichen Einstellungen neu eintragen; sie funktionieren dann wieder, obwohl das Gerät am Gateway angemeldet ist. Die Fritzbox hat das gelöschte Gerät zwar aus den Vorlagen getilgt und blendet dort „Keine Geräte enthalten“ ein, aber den neuen Eintrag bringt man wie gewohnt über das zugehörige Menü wieder in die Vorlage hinein. Zum Beispiel: die Vorlage „Ilonas Zimmer heizen“ anklicken, dann im Geräteauswahlmenü den gewünschten Client auswählen und übernehmen.

Kleines Manko: Anders als bei der Fritzbox kann man die Connect-Taste am Gateway nicht deaktivieren, sodass Angreifer mit physischem Zugang eigene Geräte ins Smart Home bringen können. Angriffsszenarien sind uns bisher aber nicht bekannt und AVM schätzt das Sicherheitsrisiko als gering ein (siehe Interview unter ct.de/wzdg).

## Zigbee-Reichweite

Wenn sich die Smart-Home-Abdeckung nicht ausreichend per DECT vergrößern lässt, kann man Zigbee ausprobieren. Der Zigbee-Funk überbrückt zwar nur 10 bis 30 Meter in Gebäuden, aber mit Repeatern kann ein Zigbee-Netz weit größer sein als die Funkblase des Zigbee-Gateways.

Repeater bieten beispielsweise Ikea (Trådfri Signal-Repeater) und Tuya an (ZigBee 3.0 Signal Repeater USB Extender, siehe ct.de/wzdg). Beide ließen sich im Test mit dem Gateway koppeln, obwohl AVM diese Geräteklasse gar nicht in seiner Kompatibilitätsliste aufführt.

Praktisch daran ist, dass ein Repeater anschließend ohne Konfiguration funktioniert: Man stellt ihn zum Beispiel auf halber Strecke zu einem Zigbee-Client auf, der außerhalb der Gateway-Reichweite steht. Sofern der Repeater das Gateway und den fernen Client erreichen kann, leitet er Zigbee-Daten automatisch zwischen den beiden hin und her. Die Strecke lässt sich verlängern, indem man weitere Repeater anhängt. Wenn in einem Zigbee-Mesh mehrere Routen zu einem Gerät führen, finden die Mesh-Teilnehmer die kürzeste Route selbstständig (Ad hoc On-Demand Distance Vector Routing).

Viele Zigbee-Lampen, -Steckdosen, -Unterputzmodule und andere kontinuierlich per 230 Volt versorgte Geräte arbeiten selbst als Repeater und bilden ebenso automatisch ein Mesh. Meist kann man sich deshalb die Kosten für einen separaten Repeater sparen.

## Mesh-Test

Für Fritzbox-Nutzer sind außer Lampen schaltbare Zigbee-Steckdosen interessant, weil manche billiger sind als die beiden DECT-Geräte von AVM. Beide Modelle, FritzDECT 200 und 210, bekommt man mitunter ab rund 50 Euro, doch manche Zigbee-Dosen schon für unter 20 Euro. Sie können zusätzlich inte-

ressant sein, wenn man mehr Leistung braucht, als FritzDECT 200 und 210 schalten können (2,3 kVA/10 Ampere beziehungsweise 3,45 kVA/15 Ampere). Tuya Zigbee 3.0 Smart Socket etwa schaltet bis zu 3,68 kVA/16 Ampere.

Manche Hersteller versprechen auch 20 Ampere, aber die allermeisten Hausinstallationen geben nicht mehr als 16 Ampere her. Und selbst wenn man eine solche Dose tatsächlich verwenden kann: Vor dem Kaufklick lohnt ein genauerer Blick auf das Datenblatt, denn manche versprechen zwar 20 Ampere groß auf der Startseite, aber verraten erst in der Doku, dass das nicht für 230 Volt Netzspannung, sondern für 110 Volt gilt (ct.de/wzdg).

Wir haben einige aktuelle Zigbee-Dosen aus verschiedenen Quellen (siehe ct.de/wzdg) kommen lassen und ausprobiert, ob und wie gut sie sich für Fritzsmart eignen. Darunter sind Modelle mit Leistungs- und Spannungsmessung besonders interessant. Vom China-Basar AliExpress stammen die zwei baugleichen Modelle von Aubbess (Smart Socket) und Girier (JR-ZPM01) sowie Tuya Power Plug-001SPB2. Außerdem haben wir Ikea Åskväder und Trådfri, Ledvance Smart+ Plug EU Indoor, Müllerlicht Tint Smart Power Strip, Lidl SilverCrest Zwischenstecker sowie als Gebrauchtgeräte innr SP120 v2.0 und Osram Smart+ ausprobiert.

Darunter eignen sich die Modelle Aubess/Girier, Power Plug-001SPB2, SilverCrest und innr SP120 zur Messung der Leistungsaufnahme. Jedoch kam schnell ans Licht: Das Fritzsmart liest den Messfühler nicht aus, sodass die Leistungsmessung an AVMs Gateway brachliegt. Ob AVM diese Funktion nachrüstet, ist offen (siehe auch Interview unter ct.de/wzdg). Wenn es nur um die Leistungsmessung geht, kann man jedenfalls gegenüber dem AVM-Angebot sparen, wenn man ein separates Gateway und einen der vier Kandidaten kauft. Beispielsweise kosten ein SilverCrest-Gateway und der zugehörige Zwischenstecker bei Lidl rund 40 Euro. Die Lidl-Home-App liest auch die Werte der drei übrigen messenden Steckdosen aus.

Neben der Leistungsmessung haben wir untersucht, wie gut die Steckdosen und der Tuya-Repeater im Mesh mit Fritzsmart zusammenspielen und wie gut sie repeaten. Heraus kam: Alle haben im Test in einem Gebäude mit gemauerten Wänden funktioniert, also zusammen mit Zigbee-Lampen ein Mesh gebildet und Zigbee-Datenpakete untereinander weitergeleitet.

Zusätzlich mussten sie als Brücke zu einem Client vermitteln, den wir außerhalb der Reichweite des Gateways aufgestellt hatten. Die gesamte Strecke war rund 30 Meter lang und das Signal musste mehrere gemauerte Wände durchdringen; die Repeater haben wir in der Mitte aufgestellt.

Außer dem Tint Power Strip waren an der Brückenposition alle Teilnehmer vom Gateway aus umgehend nach Einschalten erreichbar und ließen sich per Funk schalten. Tint Power Strip brauchte mehr als eine halbe Stunde, um sich am Brückenpunkt zu orientieren. Anschließend war er dort gut erreichbar. Als Brücke funktionierte er auch, brauchte aber wiederum lange, bis er den entfernten Client fand und Pakete zu ihm routete. Die Ledvance-Steckdose war an der Brückenposition erreichbar, aber das letzte Stück zum enfernten Client konnte sie im Test nicht überbrücken.

## DECT-Taster steuert Zigbee-Lampe

Im Test ließen sich die Steckdosen wie erwartet in gemischte Automatisierungen mit DECT-Geräten einbinden. Zum Beispiel kann man sie per DECT-Taster bedienen. Auch lassen sie sich in automatischen Routinen nutzen.

Viele Modelle kann man über einen Knopf per Hand schalten. Da sie diesen Tastendruck an das Fritzsmart melden, kann man sich das für manuelle Schaltszenarien zu Nutze machen und über den Testendruck Befehlsketten auslösen; so lassen sich zum Beispiel mehrere weitere, zu einer Gruppe zusammengefasste Geräte gemeinsam schalten. Aber ob ein Zwischenstecker einen Knopf enthält oder nicht, das ist den Herstellerfotos nicht immer zu entnehmen. Beispielsweise spart Ikea bei den Trådfri-Dosen den Knopf ein. Sie lassen sich nur per Funkbefehl schalten.

Bei Gruppenschaltungen kann man derselben Vorlage zusätzliche Steckdosen hinzufügen oder durch andere Steckdosen ersetzen. So kann man eine leistungsmessende DECT-Steckdose wie die FritzDECT 210 mit wenigen Mausklicks von einem Szenario in ein anderes umbetten. Dafür genügt je eine Änderung in Vorlage, Szenario und Routine.

## Pairing-Jammertal

Viele Geräte kann man direkt nach dem Auspacken ankoppeln, indem man sie neben dem Gateway einschaltet und dessen Connect-Taste drückt. Bei Käufen aus Gebrauchtbörsen kann die Anleitung schon mal fehlen und dann ist guter Pairing-Rat

teuer, denn jeder Hersteller verwendet seine eigene Methode, um seine Geräte in den Pairing-Modus zu versetzen. In diesen Fällen lohnt ein Besuch der umfangreichen Webseite zigbee.blakadder.com. Dort hat Saša Milićevič zahlreiche Zigbee-Geräte erfasst und zu vielen am Ende des Geräteeintrags den Pairing-Modus auf Englisch beschrieben.

Hat man ein Zigbee-Gerät mit Fritzsmart gekoppelt, kann man die meisten nicht mehr über die Hersteller-eigene App steuern und muss auf Sonderfunktionen verzichten; AVM hat bisher nur Grundfunktionen implementiert. So lässt sich etwa bei Lampen von Müllerlicht mit der Tint-App eine Party-Beleuchtung mit Flackerlicht aktivieren, aber nicht über das Webinterface von Fritzsmart.

Mit etwas Glück können Sie das Manko abmildern: Wenn ein Zigbee-Gerät gleichzeitig auch per Bluetooth Low Energy funkt (Bluetooth-LE), können Sie auf Smartphone-Apps ausweichen.

Bluetooth LE überbrückt je nach Sendeleistung durchaus 10 bis 30 Meter in Gebäuden und eignet sich dann auch für Smart-Home-Anwendungen. Ob das bei Ihrem Gerät tatsächlich der Fall ist, lohnt daher auszuprobieren. Lampen und Steckdosen von Müllerlicht ließen sich bei uns im Test mit einem iPhone 12 mini ohne Weiteres aus benachbarten Zimmern schalten.

## Ein bisschen Sci-Fi

Zusätzlich können Zigbee-Geräte ein Bluetooth-Zigbee-Gateway enthalten. Wenn diese mit anderen Zigbee-Geräten in Kontakt stehen, leiten sie ein per Bluetooth erhaltenes Kommando per Zigbee zum Ziel weiter. So ließen sich mit der Tint-App Lampen per Bluetooth auch zu Gruppen zusammenfassen und gemeinsam schalten.

Aber weil gleich zwei Steuerungsebenen implementiert sind, können so auch unerwartete Dinge passieren: Wenn man in der Tint-App das Kommando „alles aus“ oder „alles ein“ tippt, dann reichen die Müller-Lampen die Befehle an das Zigbee-Netz durch und zumindest Ikeas Trådfri-Steckdose führte den Befehl im Test aus. Dabei war es aber nicht erwünscht, dass sie den angeschlossenen Verbraucher schaltet.

Für den Nutzer ist das in der Tint-App nicht sichtbar; Zigbee-Geräte führt die App nicht auf, wenn sie am Fritzsmart angekoppelt sind. Das lässt an den Science-Fiction-Klassiker Brazil denken, der neben anderem durchspielt, wie Bewohnern die Kontrolle über hochautomatisierte Gebäude entgleitet. (dz) c't

**Zigbee-Infos**

**ct.de/wzdg**

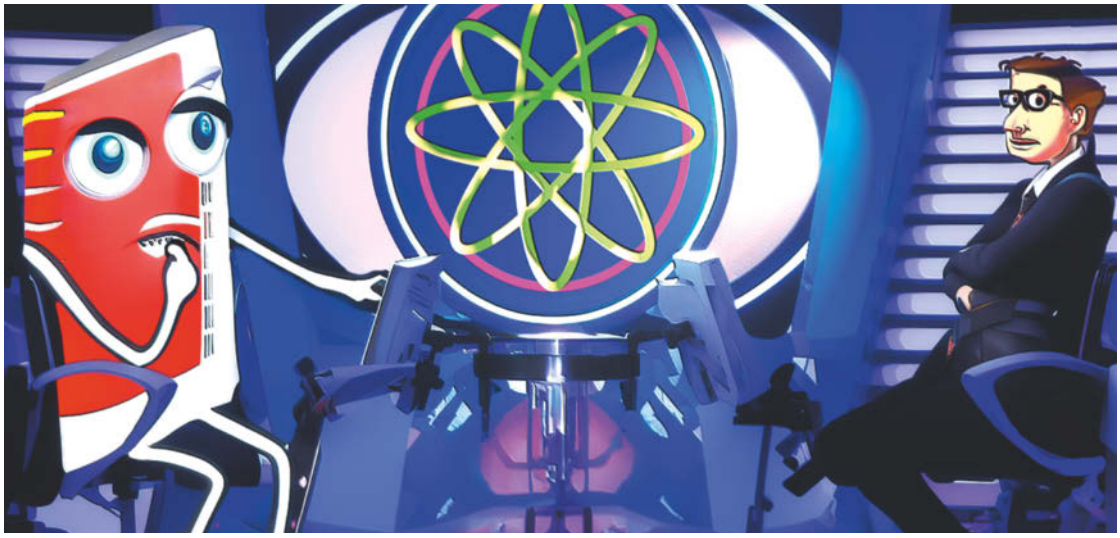


Bild: KI Stable Diffusion | Bearbeitung c't

# Fritzbox per Bash-Script abfragen

**Fritzboxen sammeln intern eine Vielzahl wissenswerter Statusdaten, die sie aber erst nach Authentifizierung rausrücken. Wir zeigen, wie man sie dem Router per Bash-Skript entlockt. Dank Hashing-Technik klappt das sogar, ohne das Passwort im Klartext zu speichern.**

Von **Mirko Dölle**

Die Fritzbox ist in Ihrem Heimnetz Doktor Allwissend: Sie verteilt per DHCP die IP-Adressen und weiß daher genau, welcher Rechner wie erreichbar ist, kennt das WLAN-Passwort, die aktuelle Leitungsauslastung und die Nummer des letzten Anrufers. Diese und viele weitere Informationen lassen sich aus der Fritzbox über die TR-064-Schnittstelle abrufen. Dafür benötigen Sie keine Programmiersprache wie Python oder NodeJS: Mit dem Wissen um die richtigen XML-Werkzeuge und die Protokoll-Details können Sie leicht selbst Informationen aus der Fritzbox in der Bash abrufen und verarbeiten.

Eine Frage, die die Fritzbox bestens beantworten kann, ist die nach der MAC-Adresse eines bestimmten Hosts in Ihrem Heimnetz. Um Strom zu sparen, sollte man Rechner, die man gerade nicht benötigt ausschalten und wieder wecken, sobald man etwa Daten von ihnen herunterkopieren möchte. Dafür bietet sich die komfortable Wake-on-LAN-Technik an, mit der man schlafende und auch heruntergefahrene Geräte per Netzwerkpaket von einem Zweitrechner aufweckt [1]. Auf diese Weckmethode reagieren praktisch alle aktuellen PCs, doch um den richtigen anzuschubsen, benötigen Sie die MAC-Adresse seiner Netzwerkschnittstelle. Diese halten Netzwerkgeräte

zwar im ARP-Cache vor, wenn sie miteinander kommuniziert haben, aber nach einer Weile räumen sie auf und die Adresse verschwindet aus dem Cache. Die Fritzbox hingegen hat ein Elefantengedächtnis und merkt sich MAC-Adressen dauerhaft.

## Fritzchen für Fritz

Viele Informationen rückt die Fritzbox nur an angemeldete Benutzer heraus, darunter die Netzwerkdetails. Dazu könnten Sie sich mit dem Passwort des automatisch angelegten Fritz-Benutzers anmelden, doch dieses Benutzerkonto ist quasi allmächtig. Deshalb empfehlen wir, unter „System/FRITZ!Box-Benutzer“ ein neues Konto mit dem Namen `fritzchen` anzulegen und ihm nur die Berechtigungen zuzuteilen, die Sie für Ihre Skripte tatsächlich benötigen.

Dazu klicken Sie unterhalb der Liste der bereits eingerichteten Benutzerkonten auf „Benutzer hinzufügen“ und geben als Benutzernamen `fritzchen` sowie ein sicheres Passwort ein.

Damit Fritzchen Auskunft zu den Netzwerkeinstellungen erhält, müssen Sie ihm mindestens die Berechtigung „Fritzbox-Einstellungen“ geben, worin automatisch auch „Sprachnachrichten, Faxnachrichten, FritzApp Fon und Anrufliste“ sowie „Smart Home“ enthalten sind. Zugang aus dem Internet sollten Sie Fritzchen jedoch nicht gestatten. Falls das erforderlich ist, richten Sie lieber eine VPN-Verbindung ein.

## Hash statt husch-husch

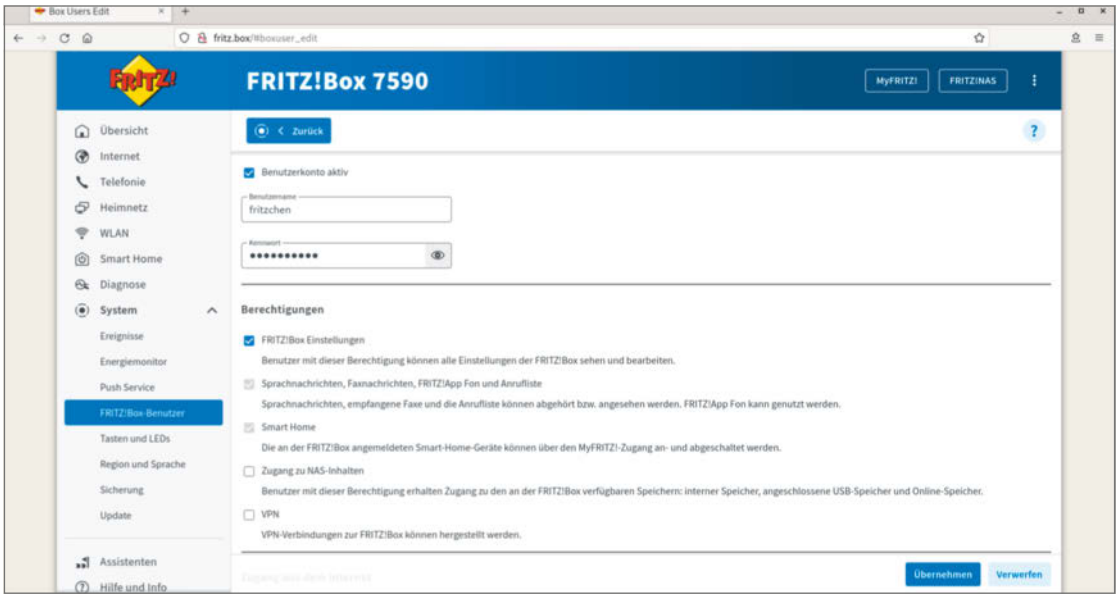
Damit das Passwort von Fritzchen nicht im Klartext im Skript steht, nutzen wir das Konzept der Fritzbox-Authentifizierung und speichern stattdessen einen vorberechneten Hash-Wert. Wie die Authentifizierung im Detail abläuft, beschreibt AVM im Handbuch „TR-064: First Steps“ (ct.de/wbp6): Fordert ein Client die Authentifizierung für eine geschützte Information per SOAP an, einem XML-basierten Netzwerkprotokoll, so liefert die Fritzbox einen Realm, der den Authentifizierungszweck angibt, sowie eine bei jedem Aufruf neue Zufallszahl im hexadezimalen Format (Nonce). Um sich also anzumelden, muss der Client den Benutzernamen, Nonce, den Realm und den Hash liefern. Das Passwort wird nicht übertragen und kann folglich nicht von Angreifern mitgelesen werden.

Eine Besonderheit der Fritzbox ist, dass der Hashwert für die Anmeldung zweistufig berechnet wird. So gibt der Pseudocode aus der Dokumentation vor, zunächst den MD5-Hash aus Benutzernamen, Realm und dem Passwort zu berechnen:

```
secret = MD5(concat(uid,":",realm,":",pwd))
```

Erst im zweiten Schritt findet dann die Nonce Eingang in den Hash:

```
response = MD5(concat(secret,":",sn))
```




**Damit Shell-Skripte sicher auf die Fritzbox zugreifen, legen Sie ein neues Benutzerkonto an und erteilen ihm nur notwendigste Rechte. Ein langes, sicheres Passwort schützt außerdem vor lokalen Angreifern.**

## Fritzchens großer Bruder

Wer in erster Linie ein Shell-Tool für den Zugriff auf die Fritzbox sucht, sollte sich das Bash-Skript fbtr64toolbox.sh von Marcus Röckrath ansehen, das auf GitHub veröffentlicht ist (siehe ct.de/wbp6). Das Skript bietet zahlreiche Funktionen, zum Beispiel die Liste der DECT-Telefone oder Nachrichten des Anrufbeantworters, Auslesen der LAN- und WLAN-Einstellungen und der MAC-Adresse von Hosts.

fbtr64toolbox.sh verwendet andere Techniken als die in diesem Artikel vorgestellten Fritzbox-Skripte. Beispielsweise verzichtet der Entwickler auf den Befehl `xmlstarlet` und verwendet eine Konfigurationsdatei im Home-Verzeichnis des Benutzers, um dort unter anderem das Fritzbox-Passwort zu speichern – auf unsere Anregung hin inzwischen ebenfalls als Hash.

Hierbei können Sie ausnutzen, dass der Realm bei der Fritzbox stets `F!Box SOAP-Auth` lautet, dies ist der Verwendungszweck. Der `secret`-Hash aus Benutzername, Realm und Passwort ist somit für alle Aufrufe des Benutzers `fritzchen` gleich. Er muss nur dann neu berechnet werden, wenn Sie den Benutzernamen oder das Passwort ändern oder die Fritzbox in einer künftigen Firmware-Version einen anderen Realm verwenden sollte.

## Übersetzungshilfe

Pseudocode wird in technischer Dokumentation häufig verwendet, um Datenformate präzise zu beschreiben. Es ist selten echter, lauffähiger Code einer bestimmten Programmiersprache, sondern beschreibt umgangssprachlich, welche Funktionen anzuwenden sind. Im Beispiel der Fritzbox-Authentifizierung steht `MD5()` für die Bildung des MD5-Hashwerts in hexadezimaler Darstellung und `concat()` fügt mehrere Teil-Strings zu einer Zeichenkette zusammen. Die Bash kennt keinen der beiden Funktionsaufrufe, man muss den Pseudocode also erst in Shell-Code übersetzen.

Für die Variable `secret` werden gemäß Pseudocode zunächst die Variablen `uid`, `realm` und `pwd` verkettet, jeweils per Doppelpunkt getrennt. Ein Funktionsaufruf wie `concat()` ist in der Bash dafür nicht erforderlich, es genügt, die Bestandteile der Zeichenkette in Anführungszeichen einzuschließen:

```
"${uid}:${realm}:${pwd}"
```

Das Berechnen des MD5-Hashes überträgt man dem Befehl `md5sum`. Er ermittelt den Hash einer Datei oder liest die Daten von der Standardeingabe ein, wenn nichts angegeben wird. Um die Zeichenkette an `md5sum` weiterzugeben, gibt es in der Bash prinzipiell zwei Möglichkeiten, per Umleitung (Here String) oder über eine Pipe:

```
secret=$(md5sum <<< \
"${uid}:${realm}:${pwd}")
secret=$(echo \
"${uid}:${realm}:${pwd}" | md5sum)
```

Das Problem: Beide Methoden hängen ein Newline-Zeichen an, sodass `md5sum` einen anderen Hashwert errechnet als die Fritzbox. Mit `echo -n` bleibt das Newline weg. Damit lautet der komplette Bash-Befehl

```
secret=$(echo -n \
"${uid}:${realm}:${pwd}" | md5sum)
```

## Aufgeräumt

Jedoch liefert `md5sum` nicht nur den Hashwert, sondern dahinter zusätzlich ein Leerzeichen, den Dateinamen, auf den sich der Hash bezieht, und ein Newline. Kommt die Eingabe aus der Pipe, lautet der Dateiname „-“. Um nur den Hashwert zu erhalten, entfernt man also die letzten drei Zeichen. Das geht beispielsweise, indem man einen Substring ab dem Anfang bis drei Zeichen vor dem Ende bildet:

```
secret=${secret:0:-3}
```

Den vollständigen Code des Skripts `fbsec`, das den Secret Hash ermittelt, finden Sie im Kasten „fbsec: Secret Hash für Fritzbox-Logins“ und als Download auf ct.de/wbp6. Es benutzt den unverschlüsselten TR-064-Zugang der Fritzbox, der standardmäßig unter http://fritz.box:49000 allen Benutzern im loka-

len Netzwerk offen steht. Besonders viel Raum nimmt der `curl`-Aufruf ein, der die Liste der Hosts per SOAP abfragt (`X_AVM-DE_GetHostListPath`). Es muss nicht die Host-Liste sein, `fbsec` muss lediglich auf eine passwortgeschützte Funktion der Fritzbox zugreifen, damit sie den Authentifizierungsvorgang auslöst und dabei unter anderem den Realm preisgibt. Den ermittelt der Befehl `xmlstarlet` in Zeile 35, das zentrale Tool zur XML-Datenverarbeitung in der Shell.

Das Passwort liest das Skript in Zeile 37 mit der Bash-internen Funktion `read` ein. Die Parameter `-r` und `-s` bewirken, dass der Backslash als reguläres Zeichen behandelt und die Eingabe nicht angezeigt wird. Der Prompt steht hinter dem Parameter `-p` und das Ergebnis landet in der Variablen `FBsec`. Da nur eine Variable angegeben ist, fungiert das Leerzeichen nicht als Trennzeichen und es funktionieren auch Passwörter, die eines enthalten.

Der Benutzername und der hexadezimale Hashwert `secret` sind alles, was Sie brauchen, um künftig geschützte Funktionen der Fritzbox zu verwenden. Das Passwort von `fritzchen` können Sie gleich wieder vergessen, weil Sie es normalerweise nicht mehr brauchen. Sollte sich der Realm jemals ändern, vergeben Sie für Fritzchen einfach ein neues Passwort.

Entscheidend für die Sicherheit ist ein langes, komplexes Passwort. Da Sie es nur ein einziges Mal in `fbsec` eingeben müssen, sollte es über 20 Zeichen lang sein und viele Sonderzeichen enthalten. Denn der Hash ist anfällig für einen Angriff etwa mit dem Passwort-Recovery-Tool `hashcat`: Da der Benutzername im Klartext im Skript steht und der Realm der Fritzbox kein Geheimnis ist, könnte ein lokaler Benutzer anhand des Hashwerts das Passwort knacken. Es ist letztlich nur eine Frage des Rechenaufwands. Deshalb sollten Sie dieses Passwort wie alle anderen nirgendwo sonst benutzen.

Der `curl`-Aufruf von Zeile 16 bis 33 bedarf einiger Erklärungen. Zunächst einmal die Parameter: `-s` entspricht `--silent` und unterdrückt die sonst übliche Ausgabe der Download-Statistik, mit `-k` genehmigen Sie selbstsignierte Zertifikate bei verschlüsselten Verbindungen und mit `-m 5` setzen Sie für die Anfrage einen Timeout von 5 Sekunden.

## fbsec: Secret Hash für Fritzbox-Logins

```
01 #!/bin/bash -x
02
03 fritzbox="http://fritz.box:49000"
04
05 if [ -z "${1}" ]; then
06   echo usage: ${0} username
07   exit 1
08 else
09   usr="${1}"
10 fi
11
12 service='urn:dslforum-org:service:Hosts:1'
13 control="/upnp/control/hosts"
14 action='X_AVM-DE_GetHostListPath'
15
16 r=$(curl -s -k -m 5 "${fritzbox}${control}" \
17 -H 'Content-Type: text/xml; charset="utf-8"' \
18 -H "SoapAction:${service}#${action}" \
19 -d "<?xml version='1.0' encoding='utf-8'?>\
20 <s:Envelope \
21   s:encodingStyle='http://schemas.xmlsoap.org/soap/
     encoding/' \
22   xmlns:s='http://schemas.xmlsoap.org/soap/envelope/'>\
23 <s:Header>\
24 <h:InitChallenge \
25   xmlns:h='http://soap-authentication.org/digest/2001/10/' \
26   s:mustUnderstand='1'>\
27 <UserID>${usr}</UserID>\
28 </h:InitChallenge>\
29 </s:Header>\
30 <s:Body>\
31 <u:${action} xmlns:u='${service}'></u:${action}>\
32 </s:Body>\
33 </s:Envelope>")
34
35 realm=$(xmlstarlet sel -t -v //Realm <<<${r})
36
37 read -r -s -p "Passwort: " pwd || exit 1
38 secret=$(echo -n "${usr}:${realm}:${pwd}" | md5sum)
39 echo -e "\nsecret = ${secret:0:-3}"
```

Das Skript `fbsec` verwendet für den Datenaustausch HTTP oder HTTPS, die Nachricht steckt in einem Envelope. Die Fritzbox verwendet verschiedene XML-Namespaces (`xmlns`, Namensräume), um die Daten zu strukturieren. Die Grundform sieht so aus:

```
<?xml version='1.0' encoding='utf-8'?>
<s:Envelope s:encodingStyle='http://↵
↳schemas.xmlsoap.org/soap/encoding/' ↵
↳xmlns:s='http://schemas.xmlsoap.org↵
↳/soap/envelope/'>
s:Header>
...
</s:Header>
<s:Body>
...
</s:Body>
</s:Envelope>
```

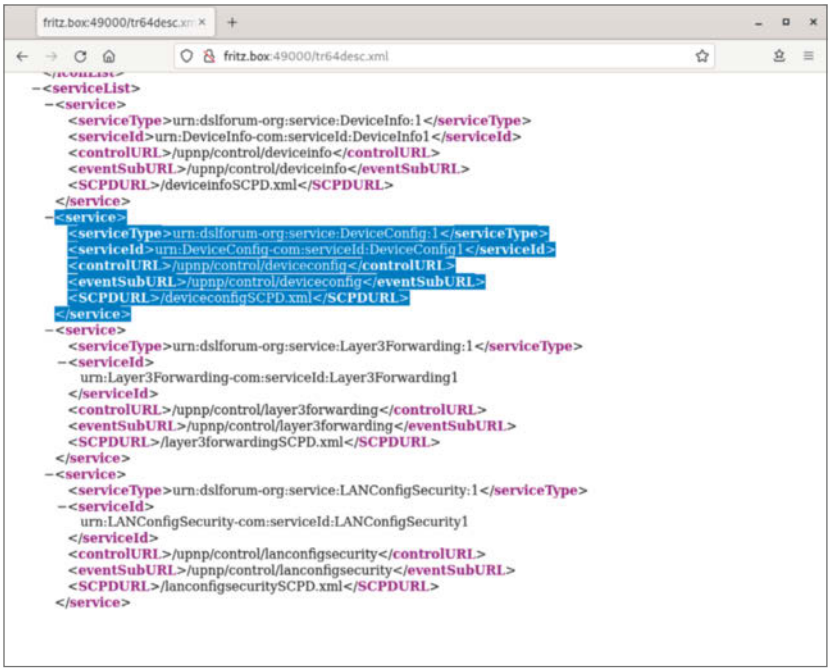
Die URLs für Kodierung und Namensraum sind keineswegs Platzhalter, sondern führen zu ebenfalls in XML verfassten Definitionen, die das Datenformat beschreiben. Eine Anfrage an die Fritzbox besteht also stets aus einem Envelope, der falls nötig ein `<Header>`-Element, in jedem Fall aber ein `<Body>`-Element enthält.

Der Body ist für alle Anfragen gleich und besteht aus dem Namen und der Namespace-URI der gewünschten Funktion als `action`:

```
<s:Body>
<u:${action} xmlns:u='${service}'>
</u:${action}>
</s:Body>
```

Welche Funktionen es gibt, ist in der Service Control Protocol Definition (SCPD) beschrieben. Davon gibt es in der Fritzbox etliche, die zentrale Anlaufstelle ist die TR-064-Definition, die Sie unter http://fritz.box:49000/tr64desc.xml abrufen können. Sie enthält Verweise auf weiterführende Definitionen. Eine davon ist die der Hosts-Dienste, hier ein Auszug:

```
<service>
<serviceType>urn:dslforum-org:↵
↳service:Hosts:1</serviceType>
<serviceId>urn:LanDeviceHosts-com:↵
↳serviceId:Hosts1</serviceId>
<controlURL>/upnp/control/hosts↵
↳</controlURL>
<eventSubURL>/upnp/control/hosts↵
```




**Welche Funktionen die Fritzbox über TR-064 anbietet, ist in den Service Control Protocol Definitionen (SCPD) beschrieben. Die erste Anlaufstelle liegt bei http://fritz.box:49000/tr64desc.xml, dort sind die SCDPs verlinkt.**

```
↳</eventSubURL>
<SCPDURL>/hostsSCPD.xml</SCPDURL>
</service>
```

Die Definition der Hosts-Dienste finden Sie unter der `SCPDURL` verlinkt. Dort ist die Funktion `X_AVM-DE_GetHostListPath` beschrieben, mit der Sie Daten über die Geräte im Netzwerk abrufen können, darunter die MAC-Adresse. Diese Funktion dürfen nur authentifizierte Benutzer verwenden, was `fbsec` ausnutzt, um den Realm zu ermitteln:

```
<action>
<name>X_AVM-DE_GetHostListPath</name>
...
</action>
```

Mit den Angaben aus den Definitionen tr64dec.xml und hostsSCPD.xml können Sie die für die SOAP-Anfrage erforderlichen Daten von `<serviceType>`, `<controlURL>` und `<action>` ermitteln:

```
service='urn:dslforum-org:service:Hosts:1'
control="/upnp/control/hosts"
action='X_AVM-DE_GetHostListPath'
```

Außerdem müssen Sie `curl` veranlassen, im HTTP-Header ebenfalls den Service und die gewünschte Funktion anzugeben. Dies geschieht mit folgendem Parameter:

```
-H "SoapAction:${service}#${action}"
```

Für die Authentifizierung verlangt die Fritzbox eine `<InitChallenge>` mit dem Benutzernamen im Header der Anfrage:

```
<s:Header>
<h:InitChallenge xmlns:h='http://soap-authentication.org/digest/2001/10/' s:mustUnderstand='1'>
<UserID>${usr}</UserID>
</h:InitChallenge>
</s:Header>
```

Auffällig ist auch hier der gesondert ausgewiesene Namespace: `<UserID>` befindet sich innerhalb von `<InitChallenge>` im Namespace `h`. Die verschiedenen Namensräume spielen auch bei der folgenden Auswertung der Antwort eine große Rolle.

In den Zeilen 19 bis 33 des Listings von `fbsec` finden Sie die vollständige SOAP-Anfrage mit dem Envelope, Header und Body. Die Fritzbox antwortet ebenfalls per XML, hier ein Auszug:

```
<?xml version="1.0"?>
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/" s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Header>
<h:Challenge xmlns:h="http://soap-authentication.org/digest/2001/10/" s:mustUnderstand="1">
<Status>Unauthenticated</Status>
<Nonce>DDDD3D22513464BC</Nonce>
<Realm>F!Box SOAP-Auth</Realm>
</h:Challenge>
</s:Header>
<s:Body>
...
</s:Body>
</s:Envelope>
```

Die Antwort enthält zwei Namespace-Definitionen: `s` bei `<Envelope>`, dessen Definition auf xmlsoap.org liegt, und `h` bei `<Challenge>` mit der Definition von soap-authentication.org. Wo welcher Namespace gilt, legen die Prefixe `s:` respektive `h:` vor den Tags fest: `s` bei `<s:Envelope>` und `<s:Header>`, `h` nur bei `<h:Challenge>`.

Für die Berechnung der Variablen `secret` benötigt `fbsec` den Realm. Zum Verarbeiten von XML-Daten in Shell-Skripten ist `xmlstarlet` erste Wahl, weil es bei Angabe des XML-Pfads einzelne Elemente aus einer XML-Struktur herausprokelt. Das folgende Beispiel liefert alle Werte (`-v`) unterhalb des Elements `<Header>` im Namespace `s`:

```
xmlstarlet sel -t \
-v "/s:Envelope/s:Header" <<<${r}
```

Auch `xmlstarlet` berücksichtigt Namespaces. Standardmäßig arbeitet es aber nur im ersten ausgewiesenen Namespace, im Beispiel des Envelope ist das `s`. Damit können Sie standardmäßig nur auf die Elemente `<Envelope>`, `<Header>` und `<Body>` zugreifen. Um an `<Challenge>` und die darunter liegenden Elemente `<Status>`, `<Nonce>` und `<Realm>` heranzukommen, müssen Sie zuvor über den Parameter `-N` den Namespace `h` definieren. Das erfordert folgende zusätzliche Parameter:

```
-N h="http://soap-authentication.org/digest/2001/10/"
```

Es gibt jedoch einen Trick: Da `<Status>`, `<Nonce>` und `<Realm>` kein expliziter Namespace zugewiesen wurde, können Sie die Elemente mittels Platzhaltern referenzieren, ohne den Namespace definieren zu müssen. So liefert

```
xmlstarlet sel -t -v //Realm <<<${r}
```

den Wert aller Elemente, die `Realm` heißen, unabhängig davon, wie ihr exakter XML-Pfad lautet. Weil in der Antwort der Fritzbox `<Realm>` nur einmal vorkommt, fällt automatisch der richtige Wert heraus.

## Abgefragt

Für öffentlich abrufbare Daten genügt ein einzelner `curl`-Aufruf. Auch der Envelope schrumpft deutlich. Als Beispiel für eine solche Datenabfrage dient hier die Funktion `GetSecurityPort`, mit der die Fritzbox verrät, wo Sie die XML-Daten verschlüsselt überträgt:

```
FBcontrol="/upnp/control/deviceinfo"
FBservice='urn:dslforum-org:
service:DeviceInfo:1'
FBaction='GetSecurityPort'
r=(curl -s -k -m 5 \
"http://fritz.box:49000${FBcontrol}" \
-H 'Content-Type: text/xml;
charset="utf-8"' \
-H "SoapAction:${FBservice}#${FBaction}" \
-d "<?xml version='1.0' encoding='utf-8'?>\
<s:Envelope s:encodingStyle='http://
schemas.xmlsoap.org/soap/encoding/'
xmlns:s='http://schemas.xmlsoap.org/
soap/envelope/'>\
<s:Body>\
<u:${FBaction} xmlns:u='${FBservice}'>
</u:${FBaction}>\
</s:Body>\
</s:Envelope>")
```

Die gesuchte Information steckt in der Antwort gemäß http://fritz.box:49000/deviceinfoSCPD.xml im Tag `<NewSecurityPort>`, hier ein Auszug:

```
<?xml version="1.0"?>
<s:Envelope ...>
<s:Body>
<u:GetSecurityPortResponse ...>
<NewSecurityPort>49443</NewSecurityPort>
</u:GetSecurityPortResponse>
</s:Body>
</s:Envelope>
```

Um die Portnummer 49443 auszulesen und in der Variablen `${FBport}` zu speichern, bemühen Sie abermals `xmlstarlet`:

```
FBport=$(xmlstarlet sel -t \
-v //NewSecurityPort <<<${r})
```

Indem Sie anschließend die URL https://fritz.box:49443 für Ihre Anfragen verwenden, können Sie verhindern, dass jemand in Ihrem Netzwerk die Kommunikation belauscht und so Daten mitliest, die eine Authentifizierung erfordern. Diese sind schließlich nicht für jedermanns Augen bestimmt – so wie die bereits in `fbsec` verwendete Funktion `X_AVM-DE_GetHostListPath`, die verschiedene Daten der Netzwerkgeräte liefert.

Auch hier ist für die Authentifizierung zunächst eine `<InitChallenge>` fällig. Der XML-Envelope ist der gleiche wie bei `GetSecurityPort`, nur dass es diesmal einen `<Header>` gibt und in den Feldern Funktionsname, Service-Typ und Control-URL andere Werte stehen. Deshalb ist es sinnvoll, den XML-Envelope ein für alle Mal als Variable `${FBenv}` zu definieren und anschließend nur noch die für jede Anfrage spezifischen Angaben zu ändern:

```
FBenv="<?xml version='1.0'
encoding='utf-8'?>\
<s:Envelope s:encodingStyle='http://
schemas.xmlsoap.org/soap/encoding/'
xmlns:s='http://schemas.xmlsoap.org/
soap/envelope/'>\
\${FBeheader}\
<s:Body>\
<u:\${FBaction} xmlns:
u='\${FBservice}'></u:\${FBaction}>\
</s:Body>\
</s:Envelope>"
```

Wenn Sie das Gleiche für den Content Type und die SOAP-Anfrage tun, macht das den Abruf des verschlüsselten Ports sehr viel übersichtlicher:

```
FBct='Content-Type: text/xml;
charset="utf-8"'
FBsoap="SoapAction:\${FBservice}#
\${FBaction}"
FBcontrol="/upnp/control/deviceinfo"
FBservice='urn:dslforum-org:service:
DeviceInfo:1'
FBaction='GetSecurityPort'
r=$(curl -s -k -m 5 \
"${FBhost}${FBcontrol}" -H "${FBct}" \
-H "${FBsoap@P}" -d "${FBenv@P}")
```

Der Clou steckt in der Parametertransformation `${parameter@operator}` der Bash: Während `${FBsoap}` lediglich die Zeichenkette ausgibt, den die Variable bei der Zuweisung gerade besaß, wendet `${FBsoap@P}` unter anderem die Variable Expansion auf den String an. Sie befüllt die Variablen `${FBservice}` und `${FBaction}` aus `${FBsoap}` mit ihren aktuellen Werten. Es genügt daher, `${FBenv}` und `${FBsoap}` am Anfang der Datei einmalig mit Variablen an den veränderlichen Stellen zu definieren und diese im Nachgang mittels `${FBenv@P}` respektive `${FBsoap@P}` zu ersetzen.

Nun ist es ein Leichtes, die `<InitChallenge>` für die Funktion `X_AVM-DE_GetHostListPath` zu formulieren:

```
FBcontrol="/upnp/control/hosts"
FBservice='urn:dslforum-org:service:
```

```
↳Hosts:1'
FBaction='X_AVM-DE_GetHostListPath'
FBeheader="\
<s:Header>\
<h:InitChallenge xmlns:h='http://soap↵
↳-authentication.org/digest/2001/10/'↵
↳ s:mustUnderstand='1'>\
<UserID>${FBuser}</UserID>\
</h:InitChallenge>\
</s:Header>"
r=$(curl -s -k -m 5 \
"${FBhost}${FBcontrol}" -H "${FBct}" \
-H "${FBsoap@P}" -d "${FBenv@P}")
```

Da in der Definition von `$FBenv` die Variable `${FBeheader}` als Platzhalter für einen Header steckt, muss man den Envelope nicht neu definieren. Aus der Antwort der Fritzbox gewinnen Sie die Nonce sowie den Realm, berechnen unter Zuhilfenahme der Secret `FBsec` den Authentifizierungs-Hash und können dann die gewünschte Liste anfordern:

```
FBnonce=$(xmlstarlet sel -t \
-v //Nonce <<<${r})
FBrealm=$(xmlstarlet sel -t \
-v //Realm <<<${r})
FBauth=$(echo -n \
"${FBsec}:${FBnonce}" | md5sum)
FBeheader="\
<s:Header>\
<h:ClientAuth xmlns:h='http://soap-↵
↳authentication.org/digest/2001/10/' ↵
↳s:mustUnderstand='1'>\
<Nonce>${FBnonce}</Nonce>\
<Auth>${FBauth:0:-3}</Auth>\
<UserID>${FBuser}</UserID>\
<Realm>${FBrealm}</Realm>\
</h:ClientAuth>\
</s:Header>"
r=$(curl -s -k -m 5 \
"${FBhost}${FBcontrol}" -H "${FBct}" \
-H "${FBsoap@P}" -d "${FBenv@P}")
```

Ob die Authentifizierung geklappt hat, verrät der Befehl

```
xmlstarlet sel -t -v //Status <<<${r}
```

mit der Antwort `Authenticated`. Daneben gibt es eine neue `<Nonce>` für weitere Abfragen.

Bei umfangreicheren Antworten wie der Netzwerkliste liefert die Fritzbox einen Pfad zurück, über den Sie das Ergebnis abrufen können. Hier ein Auszug einer solchen Antwort:

```
<s:Envelope ...>
...
<s:Body>
<u:X_AVM-DE_GetHostListPathResponse ...>
<NewX_AVM-DE_HostListPath>/devicehost↵
↳list.lua?sid=f9f18ee78924684b↵
↳</NewX_AVM-DE_HostListPath>
</u:X_AVM-DE_GetHostListPathResponse>
</s:Body>
</s:Envelope>
```

Wiederum mit `xmlstarlet` lösen Sie den Pfad heraus und laden anschließend die Antwort mittels `curl` herunter:

```
FBlua=$(xmlstarlet sel -t \
-v //NewX_AVM-DE_HostListPath <<<${r})
r=$(curl -s -k -m 5 "${FBhost}${FBlua}")
```

Eine Authentifizierung ist in diesem Fall nicht erforderlich, da der Abruf nur mit der korrekten Session-ID `sid` möglich ist. Ein weiterer Aufruf von `xmlstarlet` ermittelt aus der heruntergeladenen Liste zum Beispiel die MAC-Adresse eines Hosts:

```
xmlstarlet sel -t -m \
"List/Item[HostName='${FBsearch}']" \
-v MACAddress <<<${r}
```

Neu ist die Vorauswahl mit dem Parameter `-m`: Das Programm wählt alle `<Item>` mit dem XML-Pfad `List/Item` aus, die ein Element `<Hostname>` mit dem Wert aus `${FBsearch}` enthalten. Aus dieser Vorauswahl liefert `xmlstarlet` den Wert des Elements `<MACAddress>` und damit die MAC-Adresse des gesuchten Hosts.

## Fix und fertig

Das komplette Skript `fbgetmacaddr` haben wir auf ct.de/wbp6 zum Download bereit gestellt, Sie müssen darin nur noch den Secret Hash eintragen. Es eignet sich gut, um für das Skript `ewake` aus [1] die MAC-Adresse des zu weckenden Rechners bei der Fritzbox zu erfragen. So können Sie auch Rechner starten, deren MAC-Adresse nicht mehr im ARP-Cache liegt: Fritzchen liefert auch nach Monaten noch die korrekte Antwort. Und mit den in diesem Artikel gezeigten Techniken können Sie die TR-064-Schnittstelle der Fritzbox leicht für weitere Zwecke nutzen. (mid) c't

### Literatur

[1] Mirko Dölle, Regelrecht aufgeweckt, Mit regulären Ausdrücken in der Bash Computer aufwecken, c't 17/2023, S. 150

**Fritzbox-Skripte zum Download**

**ct.de/wbp6**

# Mesh-WLAN-Systeme richtig einsetzen

**Flottes Internet drahtlos im ganzen Haus, das versprechen Mesh-Systeme. Was ein Mesh ist und wie Sie es richtig installieren, erfahren Sie hier. Im folgenden Test haben wir sieben Kits mit dem aktuellen Wi-Fi-6-WLAN auf die Antennen gefühlt.**

Von **Andrijan Möcker**

Bild: Andreas Martini

Vor 25 Jahren machte WLAN seine ersten Schritte, heute ist die allgegenwärtige Datenfunktechnik schnell, effizient und in allerhand Geräte integriert – vom Notebook über die Smartwatch bis hin zum Toaster. Die Naturgesetze kümmert dieser Fortschritt jedoch nicht: Wenn zwischen Router und Client dämpfende Hindernisse liegen, etwa eine Steinwand oder eine Stahlbetondecke, drosseln oder stoppen diese das Netz. Dann hilft nur, weitere WLAN-Zugangspunkte aufzustellen und so das Funknetz näher an seine Nutzer zu bringen.

Früher waren das Access Points und Repeater, heute dominieren Mesh-WLAN-Systeme den Markt für kleine Netze. Alle großen Netzwerkhersteller und viele Provider bieten Produkte an, um das Heim bestmöglich mit WLAN zu fluten. Derzeit sind Sets mit zwei bis vier Geräten und von 150 bis 2000 Euro erhältlich. Mancher mag nun glauben, „Mesh“ sei lediglich ein hippes Wort für „Repeater“ und „Access-Point“. Doch es gibt einige Unterschiede, die Sie kennen sollten. Deshalb haben wir die Grundlagen aufgeschrieben und im nachfolgenden Artikel sieben Mesh-Systeme getestet.

## Was ist Mesh?

Der klassische Repeater verbindet sich drahtlos mit dem WLAN-Router, der Access-Point nutzt spektrumsschonend ein Kabel. Beide strahlen dasselbe Netz mit gleichem Funknetznamen (SSID), Verschlüsselungsmethode und Passwort aus. So können die Clients den signalstärksten Zugangspunkt herauspicken.

„Mesh“ ist im Privatkundenbereich primär ein Marketingbegriff und „WLAN-Systeme“ wäre treffender, dennoch machen die Geräte einiges besser als der erstbeste, billige Repeater aus irgendeinem Webshop: Die Zentrale jedes Mesh-Systems ist der Root-Node (Hauptknoten). Er stellt die Konfigurationsschnittstellen – Apps oder Browserseiten – des Systems und überträgt Änderungen auf die angeschlossenen Repeater-Nodes. SSID- oder Schlüsseländerungen gehen so deutlich flotter. Außerdem bieten die allermeisten Systeme ein Gastnetz, das dann idealerweise auch von den Mesh-Nodes verbreitet wird. Im nachfolgenden Testartikel zeigt sich aber, dass es Ausnahmen gibt.

Der Fritzbox-Hersteller AVM und der Internetanbieter Deutsche Telekom etwa haben die Mesh-Funktion in ihre Fritzbox- beziehungsweise Speedport-Router integriert. Da entsteht ein Mesh-System ganz einfach, indem man einen passenden Repeater dazu kauft und ihn mit dem Router koppelt – ein simpler Knopfdruck an beiden Geräten genügt und nach zwei Minuten funkt das Mesh.

Bei anderen Mesh-Kits agiert ein Gerät als Zentrale, der Root-Node (Hauptknoten). Er steckt per LAN-Kabel am Internet-Router oder Modem. Seine Kompagnons, die Repeater-Nodes, verteilt man über die abzudeckende Fläche. Sie arbeiten als Zugangspunkte für Endgeräte und leiten deren Daten weiter an den Root-Node.

Der Backbone (auch: Backhaul), also die Verbindung zwischen den Repeater-Nodes und dem Root-Node, läuft typischerweise wie bei klassischen Repeatern über Funk. Er bestimmt, wie viel Datenrate Clients erhalten, die sich mit den Mesh-Nodes verbinden. Viele Mesh-Systeme heben sich dabei durch Cross-Band-Repeating ab; sie entscheiden dynamisch, ob sie die Daten übers 2,4- oder 5-Gigahertz-WLAN-Band weiterleiten. Das verspricht mehr Durchsatz, weil die Datenpakete nicht zweimal auf demselben Funkband laufen müssen, sondern zwischendurch auf die „Parallelspur“ wechseln und deswegen die verfügbare Sendezeit (Airtime) besser nutzen.

Damit sich Clients nahtlos im abgedeckten Bereich bewegen können, gehören Roaminghelfer-Funktionen wie IEEE 802.11k (Radio Resource Management, Spektrumsmessung), 11v (BSS Transition, Basiswechsel) und 11r (Fast BSS Transition) mittlerweile zur Standardausstattung [1]. Außerdem können die Nodes schwächer werdende Clients gezielt „abwerfen“. So zwingen sie sie dazu, sich beim Wandern in der Wohnung mit einem signalstärkeren Kollegen zu verbinden.

## Im Backbone spielt die Musik

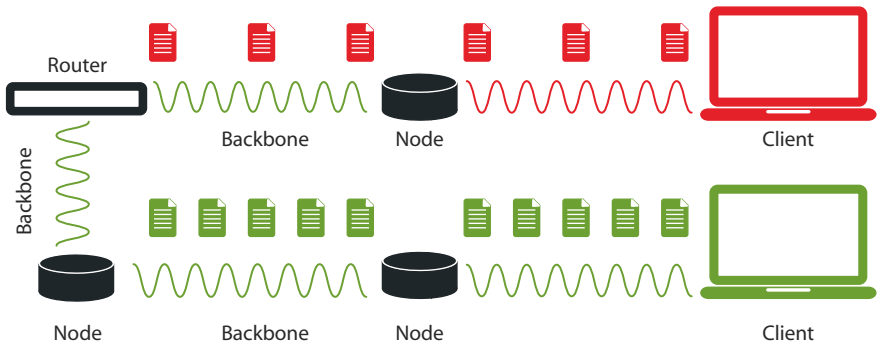
Bei hochpreisigen Sets haben die Mesh-Nodes oft ein zusätzliches Funkmodul, mit dem sie auf einem separaten 5- oder 6-GHz-Kanal den Backbone aufbauen. Mit ihnen ist man flotter unterwegs als mit Geräten, bei denen sich Backbone und Endgeräte die WLAN-Module teilen müssen.

Ketten gehören ebenso zum typischen Repertoire: Repeater-Nodes, die außerhalb der Reichweite des Root-Nodes sind, können ihre Pakete an günstiger positionierte Mitstreiter schicken, die diese zur Zentrale weiterleiten. Auch das funktioniert mit einem separaten Backbone-Modul besser.

Gewöhnliche Nodes lahmen im Kettenbetrieb aus guten Gründen: Auf einem Kanal kann immer nur ein WLAN-Gerät senden. Der Node muss die

## Backbone-Geschwindigkeit

Der Backbone oder auch „Backhaul“ ist die Verbindung zwischen den einzelnen Mesh-Nodes. Die Backbone-Datenrate bestimmt, wie schnell die mit Repeater-Nodes verbundenen Clients tatsächlich mit dem Rest des Netzwerks und damit dem Internet kommunizieren können. Die besten Ergebnisse erzielt man, wenn der Backbone per Kabel läuft und nicht per Funk.




Daten vom Client entgegennehmen, zum nächsten Repeater-Node weiterleiten und dann warten, bis alle folgenden Repeater-Nodes die Daten bis zum Root-Node übertragen haben – sozusagen Stille Post im WLAN.

Das schnellste WLAN führt deswegen immer noch über Kupfer: Wer kann, baut den Mesh-Backbone über LAN-Kabel auf. Auch Powerline oder G.hn auf alten Koaxial- oder Telefonleitungen helfen, wenn Ethernet fehlt und das Mesh nur Schneckentempo liefert [2]. Selbst eine vieradrige, zum 100-MBit-Netzwerkkabel umfunktionierte Telefonleitung kann ein besserer Backbone sein als eine tröpfelnde Funkverbindung [3].

## Wi-Fi 6 essentiell

Wi-Fi 5 alias IEEE 802.11ac ist mittlerweile veraltet und auch wenn solche Sets noch bei vielen Händlern erhältlich sind, sollten Sie bei einer Neuanschaffung nicht am falschen Ende sparen. Wi-Fi 6 ist der aktuelle WLAN-Standard.

Seine größte Neuerung ist die Übertragungstechnik OFDMA (Orthogonal Frequency Division Multiple Access). Sie erlaubt Zugangspunkten, mehrere Geräte gleichzeitig anzusprechen, indem sie den WLAN-Kanal in unterschiedlich große Unterkanäle aufteilt. In vorherigen Standards mussten Geräte immer mit der gesamten Signalbreite – also 20, 40 oder 80 Megahertz – angesprochen werden, selbst wenn sie nur wenig zu übertragen hatten. Die geringe effektive Datenrate hinterließ viel „Verschnitt“ und drosselte die Gesamtgeschwindigkeit der Funkzelle. Zusätzlich zu den vorherigen Kanalbreiten werden jetzt auch 160 MHz breite Signale unterstützt, wonach man allerdings im Datenblatt des Mesh-Sets gezielt suchen muss, denn Pflicht ist das nicht und gerade günstigere Hardware läuft oft nur mit 80 MHz.

Spatial Reuse (wortwörtlich „räumliche Wiedernutzung“) soll ebenso die Wartezeiten reduzieren, indem es Geräten erlaubt, Nachbar-WLANs zu ignorieren, sobald diese unter eine gewisse Signalstärke fallen. Geräte älterer Standards warten grundsätzlich

auf freie Lücken auf dem Kanal, bevor sie senden. Das heißt, dass selbst schwächste Signale anderer Netze für weniger Sendezeit und somit weniger Datenrate sorgen können.

In puncto Energie sparen hat sich auch etwas getan: Mittels TWT (Target Wake Time, geplante Weckzeit) können Geräte wie beispielsweise Smartphones, die besonders sparsam arbeiten wollen, einen Termin mit dem Access-Point vereinbaren. Dieser hält dann an das Gerät adressierte Pakete bis zur nächsten Weckzeit vor. Wi-Fi 6 ist also besonders gut zu akkubetriebenen Geräten und taugt auch für Smart-Home-Hardware. Access-Points älterer Standards hingegen können lediglich dem Client im Anwesenheitssignal (Beacon) mitteilen, dass ein Paket auf ihn wartet. Dafür muss der Client aber bis zu zehnmal pro Sekunde mit einem Auge auf die Beacons schauen, sich also aus dem energiesparenden Tiefschlaf reißen. Mit TWT darf er hingegen viel länger schlummern, auch mehrere Sekunden.

Doch Obacht: Wi-Fi 6 im Produktnamen oder Datenblatt ist in Sachen Datenrate nur die halbe Miete; die Anzahl der MIMO-Streams (siehe ct.de/-6033808) spielt eine entscheidende Rolle. Wer weiß, dass er sein Mesh-Set verdrahten kann und im Heimbereich mit 5 bis 15 Geräten unterwegs ist, wird wahrscheinlich schon mit zwei MIMO-Streams – meist notiert als „2 × 2 MIMO“ – glücklich werden. Läuft der Backbone hingegen per Funk, sollten es besser vier sein. High-End-Sets besitzen in der Regel Vier-Stream-Module für die Clients und ein zusätzliches Vier-Stream-Backbone-Modul.

Findet sich im 5-GHz-Bereich Ihrer dichtgefunkten Nachbarschaft kein Platz mehr für einen separaten Backbone, dann könnte ein Wi-Fi-6E-fähiges Set wie das Deco XE75 oder das Orbi RBK963 (beide als Einzeltest in diesem Heft) einen Ausweg schaffen: Im Sommer 2021 gab die EU das 6-GHz-Band zwischen 5975 und 6425 MHz frei. Da sich 6-GHz-fähige Router und Clients bislang kaum verbreitet haben, ist das neue Band vielerorts unberührtes Terrain und somit die perfekte Datenautobahn.

## Gut konfiguriert & positioniert

Die WLAN-Einstellungen moderner Mesh-Sets sind in der Regel schon optimal. Den vorgegebenen Funknetznamen und das WLAN-Passwort sollten Sie aber ändern, damit sich nicht jeder mit Zugriff aufs Typenschild in Ihr WLAN schleichen kann. Den Kanal manuell einzustellen – wozu wir früher gelegentlich noch rieten – ist indes keine gute Idee mehr. Die automatische Kanalsuche funktioniert mittlerweile gut und da Ihre Nachbar-WLANs auch gelegentlich den Kanal wechseln, ist eine manuell eingestellte Betriebsfrequenz längst kein Garant mehr für ungestörtes Funken.

Ungeachtet der technischen Ausstattung des am Ende gekauften Sets muss man immer etwas mit dem Standort der Mesh-Geräte experimentieren, um die bestmögliche Datenrate am Wunschort zu erzielen – insbesondere wenn der Backbone per Funk läuft und Sie nicht ohne Repeater-Kette auskommen. Die Konfigurations-Apps der meisten Mesh-Sets verraten, wie gut die Verbindungen zwischen den Nodes gerade stehen.

Dabei ist der kürzere Weg nicht immer der funktechnisch bessere, weil verschiedenes Material unterschiedlich dämpft. Wie stark Baumaterialien hochfrequente Strahlung dämpfen und damit die WLAN-Geschwindigkeit beeinträchtigen, lesen Sie in [4].

## Kaufen oder warten

Wie bei jedem Kauf neuer Technik sollten Sie sich vorher genau überlegen, ob das wirklich nötig ist: Genügt Ihnen die Geschwindigkeit Ihrer aktuellen WLAN-Ausstattung, können Sie Wi-Fi 6 getrost überspringen, ohne viel zu verpassen. In wenig gestörten Umgebungen hält sich der Geschwindigkeitsgewinn von Wi-Fi 5 zu Wi-Fi 6 in Grenzen.

Das sich derzeit in der Entwicklung befindliche Wi-Fi 7 alias IEEE 802.11be wird hingegen einen kräftigen Sprung hinlegen. Es bringt nicht nur 320-MHz-Kanäle und die noch flottere Kodierung 4096QAM mit, sondern auch Multi-Link-Operation (MLO). Letzteres erlaubt Clients erstmalig, mehrere Frequenzbänder und somit die Datenraten zu bündeln – das Addieren der Linkraten, das lange Zeit reines Marketing war, wird also Realität.

AVM, Netgear und TP-Link haben bereits erste Wi-Fi-7-Geräte angekündigt, weitere Hersteller werden nachziehen. Einen ersten Eindruck vermittelt der Artikel „Wi-Fi 7: Die nächste WLAN-Generation“. Können Sie sich bis zur Verabschiedung des Standards 2024 gedulden, wartet dann eine große Auswahl neuer Hardware und Ihre antiken Wi-Fi-5-Geräte dürfen guten Gewissens in Rente gehen.

Ein Blick auf die getesteten Wi-Fi-6-Mesh-Sets im folgenden Artikel lohnt sich hingegen, wenn Ihnen Ihr WLAN aufgrund der zugefunkten Nachbarschaft regelmäßig Kummer bereitet. Dann kommen die Neuerungen der sechsten WLAN-Generation so richtig zum Tragen. (amo) c't

### Literatur


[1] Alfred Arnold, WLAN-Wanderung, IEEE-Erweiterungen für besseres WLAN-Roaming, c't 23/2017, S. 84

[2] Ernst Ahlers, Freie Nebenstrecken, Alternative Wege für die Internetverteilung im Haus, c't 4/2022, S. 22

[3] Andrijan Möcker, Alles Kabel, Grundwissen Heimnetzverkabelung: Von Notlösung bis professionell, c't 26/2020, S. 132

[4] Marcus Nemes, Wellenkunde, Wie Alufolie, Metallgitter, Beton & Co. Funkwellen dämpfen, c't 9/2021, S. 138

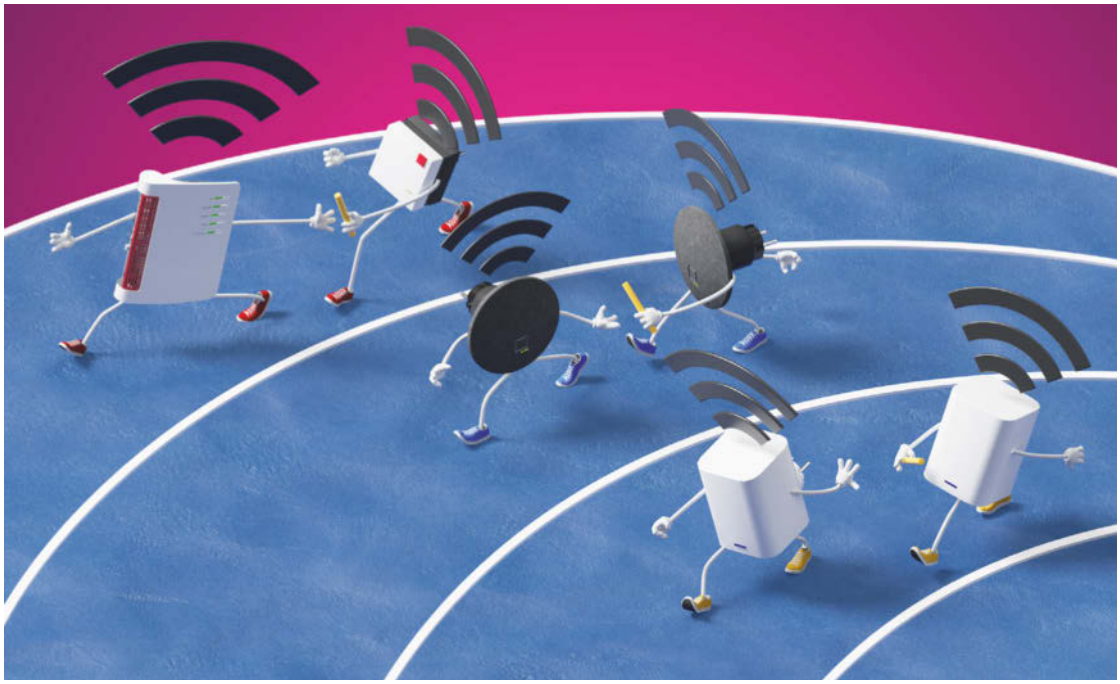


Bild: Andreas Martini

# Sieben Mesh-Systeme mit Wi-Fi 6 getestet

**Mehr Basen = mehr WLAN = mehr Internet-Speed im ganzen Haus, das ist die Kurzformel für Mesh-Systeme. Doch nicht alle leiten das Netz schnell und einfach weiter. Wir haben sieben Kits gründlich getestet.**

Von **Ernst Ahlers**

Der Gedanke hinter Mesh-WLAN leuchtet unmittelbar ein: Stopf Deine Wohnung mit WLAN-Basen voll, um überall ein starkes Signal und damit schnelles Internet zu haben. Das geht mit billigen Repeatern aus dem Elektronik-Shop als Ergänzung zum vom Provider gestellten WLAN-Router prinzipiell auch. Aber dann muss man beim Ändern etwa des WLAN-Schlüssels oder Funknetznamens zwei oder mehr Geräte einzeln anfassen, was erstens länger dauert und zweitens die Gefahr von Tippfehlern erhöht.

Mit Mesh-Systemen fällt das leicht, denn die Änderung an der Zentrale wandert automatisch auf alle Funkstationen weiter. Außerdem sind solche Kits besser aufeinander abgestimmt: Ein WLAN-Router mit dem aktuellen Wi-Fi-6-WLAN (IEEE 802.11ax, [1]) arbeitet am besten mit einem ebenfalls Wi-Fi-6-fähigen Repeater zusammen. Kommen

beide aus demselben Stall, muss man sich bei Supportfragen auch nur mit einem Hersteller herumschlagen und sitzt nicht zwischen mehreren Stühlen.

Wir haben Mesh-Kits der sieben in Deutschland bekanntesten Marken angefordert beziehungsweise zusammengestellt und im c't-Labor eingehend geprüft. Die Spanne reicht vom günstigen Dreiersatz D-Link M15 für rund 170 Euro bis zum über 600 Euro teuren Orbi-Kit RBK763 von Netgear mit ebenfalls drei Funkstationen. Fast alle haben eine Routerfunktion integriert, sodass sie die Internetverbindung über ein externes xDSL-Modem aufbauen können; die AVM- und Telekom-Router enthalten ein solches schon.

Devolos Gerätegespann hat keinen Routermodus, sondern arbeitet immer im Access-Point- (AP, WLAN-Basis am Kabel-LAN) oder Repeater-Betrieb. Wir haben es bewusst als Beispiel für ein Mesh-System hineingenommen, das das zu schwache WLAN eines älteren Routers ablösen soll. Solch einen AP-Modus unterstützen auch die meisten anderen Mesh-Kits, aber oft ohne Extras wie ein Gastnetz.

Bei AVM entschieden wir uns für das aktuelle xDSL-Topmodell Fritzbox 7590 AX als Mesh-Zentrale und stellten ihm den Fritz-Repeater 1200 AX als Mesh-Node zur Seite. Im Test der drei derzeit von AVM vertriebenen Wi-Fi-6-Repeater arbeitete der kleine besonders energiesparend und büßte dabei gegenüber den großen Brüdern verhältnismäßig wenig Performance ein [2]. Die lassen sich wie die Telekom-Repeater aber dank abgesetztem Steckernetzteil leichter für optimale Abdeckung positionieren. Falls Sie für den direkt in der Steckdose sitzenden 1200 AX keinen guten Platz finden, sind der 3000 AX und der 6000er einen Versuch wert.

Der Speedport-Router der Telekom ist als Fritzbox-Pendant eines großen Providers vertreten. Ferner spielen für etwas mehr Auswahl im unteren Preisbereich zwei Kits von Asus und TP-Link mit.

## Einrichten per App und Browser

Bei fast allen Mesh-Systemen – Ausnahme: AVM – hilft eine App beim Einrichten. Sie führt grafisch durch das Anschließen und die Inbetriebnahme. Indes muss man bei fast allen Systemen mit dem Browser nacharbeiten, denn die Apps lassen hier und da nützliche Funktionen aus, siehe Zeile „Assistent übergeht“ in der Vergleichstabelle am Ende des Artikels. Die Helfer auf den Browser-Konfigurationsseiten machen das übrigens auch kaum besser.

Das Wichtigste beim Mesh-Setup: Damit Unbefugte nicht an die Einstellungen kommen, setzen Sie ein individuelles Konfigurationspasswort. Um allzu leichtes Ins-WLAN-Schleichen zu blockieren, ändern Sie die meist aufs Typenschild gedruckten, werkseitig vorgegebenen WLAN-Einstellungen (Funknetzname und Passwort). Nachdem Sie die kompatiblen Geräte über die WPS-Taste (WLAN per Knopfdruck koppeln) ins neue Funknetz gehievt haben, schalten Sie WPS aus.

Als Prüfstein haben wir bei allen Kits das Einrichten an einem Telekom-VDSL-Anschluss ausprobiert, über den neben dem Dualstack-Internetzugang (IPv4 und IPv6) auch Live-Fernsehen per Multicast-IPTV läuft (MagentaTV).

Diese Konstellation verlangt unseren Testgeräten zwei Kniffe ab: Die Router müssen internetseitig den PPPoE-Datenverkehr in das VLAN mit der ID 7 kapseln, also VLAN-Tagging am WAN-Port beherrschen. Außerdem sollen sie als Proxy das Multicast-IPTV ins (W)LAN weiterleiten, damit man auch mit Tablet oder Notebook Live-TV schauen kann. Geräten ohne inte-

### Literatur


[1] Guido R. Hiertz, Sebastian Max, Volle Packung, Wie die Verbesserungen von Wi-Fi 6 wirken, c't 3/2020, S. 112

[2] Ernst Ahlers, WLAN-Verlängerer, Fritz-Repeater 3000 AX für Wi-Fi 6 getestet und verglichen, c't 7/2023, S. 76

[3] Ernst Ahlers, Ultrahochfunker, Test: WLAN-Router Asus GT-AXE11000 mit drei Funkmodulen, c't 7/2022, S. 84


**WLAN-FAQ**

**ct.de/wpbv**

### Mesh-WLAN-Systeme mit Wi-Fi 6 – Durchsatz und Leistungsaufnahme

| | Client 20 m 2,4 GHz (Mbit/s) | Client 20 m 5 GHz (Mbit/s) | Backbone 20 m (Mbit/s) | Client 26 m 2,4 GHz (Mbit/s) | Client 26 m 5 GHz (Mbit/s) | System-Leistungsaufnahme (W) |
|---|---|---|---|---|---|---|
| | besser ▶ | besser ▶ | besser ▶ | besser ▶ | besser ▶ | ◀ besser |
| Asus ZenWiFi XD4 Plus | 150 | 152 | 236 | 145 | 71 | 15,1 |
| AVM Fritzbox 7590 AX + 1200 AX | 155 | 260 | 446 | 140 | 135 | 23,0 |
| Devolo Repeater 5400 + 3000 | 99 | 235 | 477 | 99 | 98 | 17,4 |
| D-Link Mesh System M15 | 58 | 177 | 373 | 85 | 87 | 14,2 |
| Netgear Orbi RBK763 | —[1] | 312 | 614 | —[1] | 309 | 20,8 |
| Telekom Sp. Smart 4 + Sp. Home WLAN | 256 | 204 | 638 | 202 | 202 | 22,3 |
| TP-Link Deco X20 | 243 | 221 | 355 | 215 | 188 | 14,1 |

[1] nicht messbar, da Band Steering nicht abschaltbar und Client stets auf 5 GHz verband

### Asus ZenWifi XD4 Plus

Wer das Asus-System über ein Modem am Telekom-VDSL nutzen will, sollte es mit dem Browser-Assistenten einrichten. Die „Asus Router“-App übernahm das VLAN-Tagging nicht, sodass bei uns trotz korrekter Konfiguration keine Internetverbindung zustande kam. Ohnehin lässt sich das System per Browser viel feiner einstellen. So kann man die ab Werk inaktiven WLAN-Funktionen TWT und Airtime Fairness einschalten, die Sommerzeit-Schaltpunkte korrigieren (letzter statt vierter Sonntag) oder bei Bedarf ein Gastnetz einrichten. Während andere Systeme automatisch umschalten, muss man bei Asus’ AiMesh den Backbone-Betrieb übers LAN manuell wählen. Das gilt laut Browser-Hilfe immer für alle Nodes, man kann also nicht einzelne per LAN anbinden.

**bestes günstiges Kit im Test**
**nutzt 5-GHz-Band nicht ganz**


### AVM Fritzbox 7590 AX + Fritz-Repeater 1200 AX

Bei den meisten Mesh-Kits spielt das WLAN die Hauptrolle und die Routerfunktion ist eine notwendige Nebensache, AVMs Fritzboxen gehen es umgekehrt an: Sie sind in Sachen Routing im Vergleich exzellent ausgestattet und haben die Mesh-Funktion ins Router-Betriebssystem integriert. Selbst Profis vermissen für kleine Netze wenig, vielleicht eine dritte Netzwerkzone für Smart-Home-Geräte parallel zu Stamm- und Gastnetz. Das Einrichten klappt bei Anschlüssen der meisten Provider sehr leicht, wenn man den Empfehlungen des Browser-Assistenten folgt; eine App fehlte uns nicht. Verbesserte WLAN-Verschlüsselung und Gastnetz-Einrichtung muss man auch hier händisch nachholen. Ein Mesh-System entsteht ganz simpel per Tastendruck. Das zum Testzeitpunkt fehlende TWT hat AVM mit der 7.50er-Firmware nachgeliefert.

**sehr flexible Router-Funktionen**
**kinderleichtes Mesh-Setup**

griertes Modem schnallten wir ein Draytek Vigor167 vor. Internet gabs anschließend immer, Multicast-IPTV nur manchmal.

## WLAN-Optionen

Als Wi-Fi-6-Systeme sollen die Kits die wichtigsten WLAN-Verbesserungen des aktuellen Standards beherrschen, also Spatial Reuse mit BSS Coloring und Target Wait Time (TWT). BSS Coloring erlaubt Wi-Fi-6-Netzen zu senden, wenn der Kanal schon von einem fremden, aber nur schwach zu hörenden WLAN belegt ist. Das funktioniert quasi wie die kleinen Gesprächsgrüppchen in einem großen Festsaal und steigert den Funkzellendurchsatz. Mit TWT können Mobilgeräte länger akkuschonend in den Tiefschlaf gehen als bei früheren WLAN-Versionen.

Multi-User-MIMO, kurz MU-MIMO (ct.de/wpbv), gibt es schon seit Wi-Fi 5. Damit können WLAN-Basen Daten auf derselben Frequenz gleichzeitig an mehrere Empfänger senden, was ebenfalls den Summendurchsatz verbessert. Bei WLAN-Systemen mit weniger als vier MIMO-Streams ist MU-MIMO optional. Uplink-MU-MIMO dreht den Spieß um: Mehrere Clients können gleichzeitig an dieselbe Basis senden. Das ist ebenfalls nützlich, kommt im Alltag aber selten vor und ist damit eher Sahnehäubchen als Tortenboden.

Das Mesh-System sollte idealerweise ab Werk die aktuelle WLAN-Verschlüsselung WPA3 im Mixed-Mode (WPA2+3) beherrschen, damit auch ältere Clients, die nur WPA2 kennen, sich noch verbinden können. Der Mixed-Mode fehlte in der getesteten Netgear-Firmware. Wenn das Orbi-System auf WPA3

## Devolo WiFi 6 Repeater 5400 + 3000

Devolos Mesh-fähige Repeater sind die Exoten im Test, denn sie haben keinen Routermodus. Mindestens einer muss als Access-Point per LAN am Internetrouter hängen (im Test das 5400er-Modell), der Rest als Repeater mit WLAN-Backbone oder ebenfalls als Access-Point per LAN (3000er). Das optionale Gastnetz entsteht über Layer-2-Firewallregeln: Besucher kommen trotz gleicher IPv4- und IPv6-Adressbereiche nur ins Internet. Die Home-Network-App führt geschickt durch den kurzen Setup-Prozess für das erste Gerät, doch muss wie so oft für manche nützlichen Dinge der Browser ran. Die weiteren Nodes koppelt man einfacherweise per Knopfdruck. Diese bieten aber bei der aktuellen Firmware weder das Gastnetz noch WPA2+3 an, beides gibts zurzeit nur am Root-Node.

**einfach einzurichten**

**läuft nur hinter Internetrouter**

## D-Link Mesh System M15

Das M15-System von D-Link haben wir bewusst als „Billigheimer“ in den Test genommen und so präsentierte es sich auch: Wi-Fi 6 gibts nur auf 5 GHz. Die 2,4-GHz-Funkmodule der Nodes arbeiten nach dem veralteten Wi-Fi-4-Standard (IEEE 802.11n-300), was zu weit unterdurchschnittlichem Durchsatz in dem Band führte. Das Konfigurieren fürs Telekom-VDSL klappte erst nach manuellem Eingriff per Browser. Wir brauchten mehrere Anläufe, bis alle Nodes ins Mesh eingebunden waren. Das System nutzte im Test trotz Automatik nie die hohen 5-GHz-Kanäle; laut Hersteller soll es erst bei viel Fremdverkehr hochgehen. Die Firmware zeigte die von D-Link bekannten IPv6-Macken (siehe Artikel „25 Router auf IPv6 getestet“), mit denen der Hersteller aber beileibe nicht allein ist. Wer die Hürden genommen hat, bekommt Dualstack-Internet, wenn auch kein rasend schnelles.

**viele Nodes für wenig Geld**

**veraltetes WLAN auf 2,4 GHz**

gestellt war, bot es laut den Beacons (Anwesenheitssignal von WLAN-Basen) tatsächlich nur das an. Ein Verbindungsversuch mit einem älteren Android-8-Smartphone scheiterte prompt: Beim Erstkontakt zum WPA3-Orbi-WLAN meinte das Handy, WPA2-Enterprise mit individueller Authentifizierung gemäß IEEE 802.1x gefunden zu haben, und fragte nach Zugangsdaten. So zwingt Netgear dazu, beim veralteten, aber immerhin noch sicheren WPA2 zu bleiben.

Koppelt man Devolos Geräte als Access-Point und Repeater zu einem Mesh-WLAN, dann steht WPA2+3 nur am AP zur Verfügung. Das könnte sich mit einem kommenden Firmware-Update ändern. Devolos Konfigurationsseite warnt vor Interoperabilitätsproblemen mit manchen Clients, wenn man WPA2+3 und den Roaming-Helfer IEEE 802.11r (Fast BSS Transition, schneller Basiswechsel) gleichzeitig aktiviert. Das ist keine blanke Theorie und gilt auch bei anderen Systemen mit 11r-Option: Ein zum Test verwendetes Android-12-Smartphone konnte in dieser Konstellation tatsächlich keine stabile WLAN-Verbindung aufbauen; das Windows-11-Testnotebook (siehe „WLAN ausgemessen“) hielt sie hingegen problemlos. Wer WPA2+3 nutzen will, sollte 11r ausgeschaltet lassen.

Die anderen Roaming-Helfer 802.11k (Radio Resource Management) und 11v (BSS Transition) fanden wir erfreulicherweise bei allen Systemen, wenn auch ersteren in unterschiedlich feiner Ausprägung. Asus’ XD4 Plus etwa unterstützt laut Beacons bei 11k nur den „Neighbor Report“, während AVMs Geräte auch „Link …“, „Beacon Active …“, „Beacon Passive …“ und weitere „… Measurements“ beherrschen.

### Netgear Orbi RBK 763

Netgears Orbi-Kit bildet das teure Pendant zum Sparbrötchen M15 von D-Link. Ein Dreiersatz kostet über 600 Euro statt 170, rechtfertigt aber seinen Preis mit der besten WLAN-Performance im Test: Mit 300 Mbit/s über 5 GHz hinter dem Repeater-Node lag es im Test weit vor dem zweitschnellsten System, dank seines separaten Mesh-Backbones. Aber auch hier war nicht alles Gold: Die Orbi-App scheiterte am Setup für Telekom-VDSL, sodass wir zum Browser greifen mussten. Ferner nervte die App mit penetrantem Gedrängel zu kostenpflichtigen Abo-Diensten. Eigenartigerweise bot das Orbi-System nur WPA2 oder WPA3 als WLAN-Verschlüsselungsmethode, nicht aber den mittelfristig unverzichtbaren Mixed-Mode WPA2+3. Wer keine älteren Clients aussperren will, muss beim schwächeren WPA2 bleiben.

**rasantes WLAN**
**kein Mixed-Mode WPA2+3**

### Telekom Speedport Smart 4 + Speed Home WLAN

Einfacher kann die Internet-Einrichtung kaum sein, falls man den Zugang von der Telekom bezieht: Anschließen, einschalten und auf das Ich-bin-Online-Feuerwerk auf dem Display warten. Ein simpler Tastendruck koppelt dann die Mesh-Nodes. Im Test lieferte das System sehr guten Durchsatz, sein Backbone war sogar ein Quäntchen schneller als der des Netgear-Kits. Der Speedport-Router glänzt mit vielen Funktionen, kommt aber nicht an das Niveau der Fritzbox heran. So beschränkt er die Zahl der WireGuard-VPN-Zugänge auf fünf, und wir fanden weder IPv6 im Gastnetz noch IPv6-Dienstfreigaben für Heim-Admins, die eigene Server betreiben wollen. Die MeinMagenta-App hilft bei der Inbetriebnahme; für Konfigurationseingriffe taugt der Browser besser.

**extrem leichtes Setup am T-Netz**
**schnelles Mesh**

## WLAN ausgemessen

Wie schnell die Mesh-Nodes funken, haben wir mit einem Wi-Fi-6E-fähigen Notebook (Galaxy Book Pro von 2021 mit WLAN-Modul Intel AX210) und unserem Standard-Benchmark iperf3 gemessen und als „Client-Durchsatz am Root-Node“ verzeichnet. Die Werte gehen als typisch für Wi-Fi 6 durch. Einzig das D-Link M15 leistete sich im 2,4-GHz-Band wegen seines veralteten Wi-Fi-4-Funkmoduls einen krassen Ausrutscher nach unten.

Manche Wi-Fi-6-Basen können Daten im 5-GHz-Band über ein 160 Megahertz breites Signal senden. Das verdoppelt gegenüber dem regulären 80-MHz-Betrieb die maximale Bruttodatenrate (ct.de/wpbv) mit zwei MIMO-Streams bei einer guten Funkverbindung auf 2400 Mbit/s. Mit NBase-T-Ports (Multigigabit-Ethernet), die je nach Ausführung bis 2500, 5000 oder 10.000 Mbit/s übertragen, gehen dann bis zu 1500 Mbit/s oder 1,5 Gbit/s ins Kabel [3]. Ein regulärer Gigabit-Port (1000 Mbit/s) kappt den Nettodurchsatz aber auf 930 bis 940 Mbit/s. Das sieht man bei den „Nah“-Ergebnissen der Root-Nodes von Devolo, Netgear und Telekom.

## Stabübergabe

Beim drahtlosen Weiterleiten entscheidet der Mesh-Backbone, wie schnell die Daten beim Repeater ankommen – mehr kann er nicht an den Client weitergeben. Den „Backbone-Durchsatz“ bestimmten wir über die LAN-Ports von Root- und Repeater-Node, zwischen denen 20 Meter mit Steinwänden lagen. Wegen der unvermeidlichen Ausrichtungsabhängig-

### TP-Link Deco X20

Am Telekom-VDSL via Modem muss man beim Einrichten aufpassen und das VLAN-Tagging „benutzerdefiniert“ setzen. Nach dem Aktivieren von IPv6 mit PPPoE vergab der Deco-Router Adressen per DHCP, was für Server praktisch ist, alle anderen aber leicht verfolgbar macht. Das lässt sich über „Internetverbindungstyp“ und „Zugewiesener Typ“ auf „SLAAC + Stateless DHCP“ korrigieren. WLAN-seitig vermissten wir die Wi-Fi-6-Funktionen BSS Coloring und TWT. Der optionale Roaming-Helfer IEEE 802.11r entpuppte sich als Placebo: Nach dem Einschalten von „Fast Roaming“ fehlte in den WLAN-Beacons immer noch das kennzeichnende Information Element 54 (Mobility Domain). Wenigstens war das funktional sparsame Mesh-System auch energetisch sparsam und flink.

**gute Mesh-Performance**
**Wi-Fi 6 in Minimalausstattung**

keit haben wir wie beim Node/Client-Benchmark in vier unterschiedlichen Orientierungen der Geräte gemessen. Beim sich so ergebenden Durchsatzbereich konnten sich die WLAN-mäßig gut ausgestatteten Kits von Netgear und Telekom vom Mittelfeld absetzen: Ihr Maximum von über 600 Mbit/s war uns eine sehr gute Note wert. Zwischen 200 und 400 Mbit/s gab es ein „zufriedenstellend“.

Was am Ende der Kette drahtlos beim Notebook ankam, zeigt der „Client-Durchsatz 26 m“. Weniger als 50 Mbit/s, die Geschwindigkeit eines gewöhnlichen VDSL-Internetzugangs, hätte eine schlechte Note ergeben. Bis 100 Mbit/s finden wir „zufriedenstellend“, das Doppelte davon oder mehr „sehr gut“.

Ein LAN-Backbone zwischen Root- und Repeater-Node überträgt Daten in den meisten Fällen deutlich schneller als das WLAN-Pendant, nämlich mit 940 Mbit/s, wenn eine Gigabit-Ethernet-Verbindung zustande kommt. Dadurch klettert tendenziell auch der Client-Durchsatz am Repeater-Node, der nun zum Access-Point geworden ist. Meist steigt die Nettodatenrate im 5-GHz-Band beträchtlich an, im Test bei den Systemen von Asus, AVM, Devolo und Telekom. Die einmalige Mühe, ein LAN-Kabel zu verlegen, zahlt sich auch beim Mesh langfristig aus.

## Mesh kostet Strom

Jeder Mesh-Node nuckelt am Stromnetz, je nach WLAN-Ausstattung und Anschlussbelegung mal mehr, mal weniger. Wir haben den Leistungsbedarf an Root- und Repeater-Nodes gemessen und für ein Dreiersystem überschlagen. Bei den Root-Nodes waren zwei Ethernet-Ports belegt beziehungsweise das integrierte Modem und ein LAN-Port aktiv. Die Repeater-Nodes liefen ohne Ethernet-Hosts; pro Gigabit-Ethernet-Link muss man 0,3 bis 0,5 Watt Mehrbedarf veranschlagen.

Bei Kits ohne Modem haben wir für die Benotung drei Watt aufgeschlagen, sodass Systeme mit Modem-Router nicht benachteiligt werden. Fürs Dreiergespann setzten wir unter 20 Watt als „gut“ an, mehr als „zufriedenstellend“. Bei Repeater-Nodes lag der zufriedenstellende Bereich zwischen 4 und 6 Watt.

## Fazit

Viel Geld muss man nicht ausgeben, um ein schwaches oder veraltetes Router-WLAN durch ein Mesh-System abzulösen: Schon für 170 Euro gibts ein Dreier-Kit in Sparausführung von D-Link, doch das nutzt man lieber im kabelgebundenen Access-Point-Modus und lässt den Router weiter seine Arbeit tun. Für etwas mehr Geld bieten die anderen Wi-Fi 6 auch im 2,4-GHz-Band, was nah an der Basis extra Schub bringt.

Wer einen aktuellen Router von AVM oder der Telekom hat, braucht nur passende Repeater gleicher Herkunft als Mesh-Nodes und fährt damit am besten.

Die weiteren getesteten Kits benötigen ein separates Modem für den Internetanschluss, falls man den alten Router in Rente schicken will. Von ihnen entpuppte sich das Asus-Set im Test als Preis/Leistungs-Tipp. Der Netgear-Satz zog allen nicht nur preislich davon, sondern auch beim WLAN-Durchsatz.

# Mesh-WLAN-Systeme mit Wi-Fi 6 – Technische Daten und Messwerte

| Typ | ZenWiFi XD4 Plus | Fritzbox 7590 AX + Repeater 1200 AX | WiFi 6 Repeater 5400 + 3000 |
|---|---|---|---|
| Hersteller | Asus | AVM | Devolo |
| getestete Firmware-Version | 3.0.0.4.386_67853 | 7.39-103725 + 103436 | 5.10.3 |
| **Anschlüsse** | | | |
| Ethernet / USB (am Root-Node) | 2 × 1G / – | 5 × 1G / 2 × USB 3.2 Gen 1 | 2 × 1G + 1 × 1G / – |
| Bedienelemente | WPS, Reset | WLAN, DECT, Connect | Add, Reset |
| Statusanzeigen / abschaltbar | 1 Leuchte / ✓ | 5 Leuchten / ✓ | 1 Leuchte, dreistufiger Balken / ✓ |
| **Konfiguration** | | | |
| Per App / Browser | ✓ / ✓ | – / ✓ | ✓ / ✓ |
| HTTPS / Telnet / SSH | ✓ / ✓ / ✓ | ✓ / – / – | ✓ / – / – |
| Oberfläche auch deutsch / brauchbare Onl.-Hilfe / Assistent | ✓ / – / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ |
| Assistent übergeht | IPv6, WPA2+3, Gastnetz | WPA2+3, Gastnetz | Gerätepasswort, WPA2+3, Gastnetz |
| **Funktionen** | | | |
| WAN-Betriebsarten (außer DHCP, Static IP, PPPoE) / IPv6 | L2TP, PPTP / Passthrough, 6to4, 6RD, 6in4 | DS-Lite / DS-Lite, 6to4, 6RD, 6in4 | (kein Router-Modus) |
| T-VDSL / IPv6 / Multicast-IPTV | ✓ / ✓ / (✓)[2] | ✓ / ✓ / ✓ | (kein Router-Modus) |
| IPv6-Adresszuteilung intern ab Werk | SLAAC | SLAAC | (kein Router-Modus) |
| IPv6-Präfix-Delegation kommend / gehend | ✓ / – | ✓ / ✓ | (kein Router-Modus) |
| IPv6-Portfreigaben | per Firewall-Regel | ✓ | (kein Router-Modus) |
| Fernüberwachung per | Browser, App, SSH | E-Mail, App | – |
| Kindersicherung: Webfilter (Dienstleister) / Online-Zeitbeschränkung | ✓ (Trend Micro) / ✓ | ✓ (BPjM) / ✓ | – / ✓ |
| Besonderes | eigener DynDNS-Dienst, Lets-Encrypt-Anbindung | Supervectoring-Modem, DECT/VoIP-Tk-Anlage, lokale Smarthome-Steuerung, eigener DynDNS-Dienst, Lets-Encrypt-Anbindung | Zonentrennung auf Layer 2 (MAC-Schicht) |
| **WLAN** | | | |
| WLAN-Bestückung (MIMO-Streams) | 2 × Wi-Fi 6 (2) | 2 × Wi-Fi 6 (4) / 2 × Wi-Fi 6 (2) | Wi-Fi 6 (2) + Wi-Fi 6 (4) / 2 × Wi-Fi 6 (2) |
| alias IEEE 802.11... | ax-600 + ax-1200 | ax-1200 + ax-2400 / ax-600 + ax-2400 | ax-600 + ax-4800 / ax-600 + ax-2400 |
| nutzt alle 5-GHz-Kanäle / 160 MHz Signalbreite | – / – | ✓ / ✓ | ✓ / ✓ |
| Separater Backbone / MU-MIMO | – / ✓ | – / ✓ (nur Router) | – / ✓ (5 GHz) |
| System hat AP-Modus / Node-Kette | ✓ / k. A. | ✓ / ✓ | ✓ / ✓ |
| Gastnetz / mit IPv6 | ✓ / – | ✓ / ✓ | (kein Router-Modus) |
| Gastnetz im AP-Modus / mit IPv6 | –[4] / –[4] | ✓[5] / ✓[5] | ✓ / ✓ (nur am Root-Node) |
| WPA3 (Mixed-Mode) / im Gastnetz | ✓ / ✓ | ✓ / ✓ | ✓ / ✓ |
| Roaming-Unterstützung: 802.11k / v / r | ✓ / ✓ / – | ✓ / ✓ / – | ✓ / ✓ / ✓ |
| Wi-Fi 6: BSS Coloring / TWT / Uplink-MU-MIMO | ✓ / ✓ (nur 2,4 GHz) / ✓ (nur 5 GHz) | ✓ / ✓ (nur Node) / ✓ (nur Node) | ✓ / ✓ / ✓ (5 GHz) |
| **Durchsatz und Leistungsaufnahme** | | | |
| Router: NAT-Performance PPPoE / IPoE (Downstream) | 936 / 942 Mbit/s | 937 / 941 Mbit/s | (kein Router-Modus) |
| Client-Durchsatz am Root-Node 2,4 GHz nah / 20m | 373 / 114–150 Mbit/s | 259 / 106–155 Mbit/s | 305 / 66–99 Mbit/s |
| Client-Durchsatz am Root-Node 5 GHz nah / 20m | 556 / 32–152 Mbit/s | 742 / 236–260 Mbit/s | 941 / 154–235 Mbit/s |
| Backbone-Durchsatz 20 m | 207–236 Mbit/s | 399–446 Mbit/s | 407–477 Mbit/s |
| Client-Durchsatz 26 m 2,4 / 5 GHz | 145 / 71 Mbit/s | 140 / 135 Mbit/s | 99 / 98 Mbit/s |
| Client-Durchsatz 26 m mit LAN-Backbone | 64 / 190 Mbit/s | 149 / 299 Mbit/s | 127 / 173 Mbit/s |
| Switching-Leistung über Node-LAN-Ports | 937 / 940 Mbit/s | – | 942 / 943 Mbit/s (5400) |
| Leistungsaufnahme Root / Node / 3er-System | 5,7 / 4,7 / 15,1 W | 16,2 / 3,4 / 23,0 W | 7,8 / 4,8 / 17,4 W |
| jährliche Stromkosten 3er-System (Dauerbetrieb, 40 Cent/kWh) | 53 € | 81 € | 61 € |
| **Bewertung** | | | |
| Funktionen: Router-Mode / WLAN | ⊕ / ⊕ | ⊕⊕ / ⊕ | – / ⊕ |
| Backbone-Durchsatz | ○ | ⊕ | ⊕ |
| Client-Durchsatz 26 m 2,4 / 5 GHz | ⊕ / ○ | ⊕ / ⊕ | ⊕ / ⊕ |
| Energie-Effizienz 3er-System / Nodes | ⊕ / ○ | ○ / ⊕ | ○ / ○ |
| Preis 3er-System | 237 € | 315 € | 257 € |

✓ vorhanden/funktioniert – nicht vorhanden/funktioniert nicht k. A. keine Angabe ⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖⊖ sehr schlecht

[1] eingebettete Browser-Seite in der App für Detaileinstellungen [2] Funktionen vorhanden und manuell aktiviert, MagentaTV funktionierte im Test dennoch nicht [3] fein konfigurierbare Zeiten/Filter nur mit kostenpflichtigem Abo
[7] nicht messbar, da Band Steering nicht abschaltbar und Client deswegen immer auf 5 GHz verband [8] 5-GHz-Durchsatz war mit LAN-Backbone nicht messbar, da der Client sich in der Situation nur auf 2,4 GHz verband

| | Mesh System M15 | Orbi RBK763 | Speedport Smart 4 + Sp. Home WLAN | Deco X20 |
|---|---|---|---|---|
| | D-Link | Netgear | Telekom | TP-Link |
| | 1.07.01 | 6.3.6.4_1.2.68 | 010139.3.1.001.0 + 010143.3.0.002.1 | 1.0.6 B. 20220909 Rel. 59388 |
| | | | | |
| | 2 × 1G / – | 4 × 1G + 2 × 1G / – | 1 × 2,5G, 3 × 1G / 1 × USB 2.0 | 2 × 1G / – |
| | WPS, Reset | Sync, Reset | WLAN, Menü, Plus, Neustart, Reset | Reset |
| | 1 Leuchte / ✓ | 2 Leuchten / ✓ (autom.) | Display, 3 Leuchten / ✓ | 1 Leuchte / ✓ |
| | | | | |
| | ✓ / ✓ | ✓ / ✓ | ✓[1] / ✓ | ✓ / – |
| | ✓ / – / – | ✓ / – / – | ✓ / – / – | ✓ / – / – |
| | ✓ / – / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ |
| | WPA2+3, Gastnetz | IPv6, WPA2+3, Gastnetz | Gastnetz | IPv6, WPA2+3, Gastnetz |
| | | | | |
| | L2TP, PPTP, DS-Lite / 6rd, Auto | L2TP, PPTP / 6to4, 6rd, Passthrough, Courier | – / – | L2TP, PPTP, DS-Lite / Bridge, 6to4 |
| | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / ✓ | ✓ / ✓ / – |
| | SLAAC | SLAAC | SLAAC | DHCP (umschaltbar) |
| | ✓ / – | ✓ / – | ✓ / – | ✓ / – |
| | – | – | – | per Firewall-Regel |
| | E-Mail, App | E-Mail, App | E-Mail, (App)E | App |
| | ✓ (lokale Liste) / ✓ | ✓ (Bitdefender) / ✓ | – / ✓ | ✓[3] (Avira) / ✓[3] |
| | Zonentrennung auf Layer 2 (MAC-Schicht) | – | Supervectoring-Modem, DECT/VoIP-Tk-Anlage, Smart-home-Steuerung per Cloud, priorisierte WLAN-Zelle | – |
| | | | | |
| | Wi-Fi 4 (2) + Wi-Fi 6 (2) | 3 × Wi-Fi 6 (2) | 2 × Wi-Fi 6 (4) / Wi-Fi 6 (2) + Wi-Fi 6 (4) | 2 × Wi-Fi 6 (2) |
| | n-300 + ax-1200 | ax-600 + ax-2400 + ax-2400 | ax-1200 + ax-4800 / ax-600 + ax-4800 | ax-600 + ax-1200 |
| | – / – | ✓ / ✓ | ✓ / ✓ | – / – |
| | – / – | ✓ / – | – / ✓ | – / – |
| | ✓ / k. A. | ✓ / ✓ | ✓ / ✓ | ✓ / ✓ |
| | ✓ / ✓ | ✓ / – | ✓ / – | ✓ / ✓ |
| | – / – | ✓ / – | kein AP-Modus | ✓ / ✓ |
| | ✓ / ✓ | –[6] / –[6] | ✓ / ✓ | ✓ / ✓ |
| | ✓ / ✓ / – | ✓ / ✓ / – | ✓ / ✓ / – | ✓ / ✓ / – |
| | ✓ / – / – | ✓ / ✓ / – | ✓ / ✓ / – | – / – / – |
| | | | | |
| | 937 / 943 Mbit/s | 936 / 942 Mbit/s | 938 / 938 Mbit/s | 936 / 943 Mbit/s |
| | 103 / 41–58 Mbit/s | –[7] / –[7] | 389 / 157–256 Mbit/s | 332 / 184–243 Mbit/s |
| | 640 / 106–177 Mbit/s | 927 / 125–312 Mbit/s | 931 / 125–204 Mbit/s | 689 / 136–221 Mbit/s |
| | 301–373 Mbit/s | 514–614 Mbit/s | 467–638 Mbit/s | 295–355 Mbit/s |
| | 85 / 87 Mbit/s | –[7] / 309 Mbit/s | 202 / 202 Mbit/s | 215 / 188 Mbit/s |
| | 68 / –[8] Mbit/s | –[7] / 384 Mbit/s | 183 / 431 Mbit/s | 195 / 219 Mbit/s |
| | 452 / 459 Mbit/s | 942 / 792 Mbit/s | 941 / 806 Mbit/s | 941 / 943 Mbit/s |
| | 5,2 / 4,5 / 14,2 W | 7,6 / 6,6 / 20,8 W | 11,7 / 5,3 / 22,3 W | 5,1 / 4,5 / 14,1 W |
| | 50 € | 73 € | 78 € | 49 € |
| | | | | |
| | ⊕ / ○ | ⊕ / ○ | ⊕ / ⊕ | ○ / ⊖ |
| | ○ | ⊕⊕ | ⊕⊕ | ○ |
| | ○ / ○ | –[7] / ⊕⊕ | ⊕⊕ / ⊕⊕ | ⊕⊕ / ⊕ |
| | ⊕ / ○ | ○ / ⊖ | ○ / ○ | ⊕ / ○ |
| | 168 € | 650 € | 370 € (T-Shop) | 195 € |

[4] im AP-Modus keine Netztrennung, Gast-WLAN führt ins interne Netz [5] Gastnetz der vorgeschalteten Fritzbox [6] nur WPA2 oder WPA3, kein Mixed-Mode WPA2+3

(ea) c't

# „Revolutionärer WLAN-Booster“ entzaubert


**Der „Club der Verbraucher“ meint, die Internetanbieter drosseln die Surfgeschwindigkeit. Sein WLAN-Repeater UltraXtend soll die Bremse lösen. Wir haben das ausprobiert und dem Gerät unter die Haube geschaut.**

Von **Ernst Ahlers**

Für die Ungeduldigen und Frustrierten: Nein, auch UltraXtend alias RangeXTD kann keine 350 Mbit/s in die Wohnung senden, wenn der Provider nur 100 Mbit/s anliefert. Solch eine Beschleunigung behauptet eine angebliche Kundenbewertung von „Hugo T.“ auf club-der-verbraucher.com (vollständiger Link über ct.de/wvpg).

Bei dieser Site passt so einiges nicht zusammen: Betreiber des „Clubs“, der mit seinem Namen wohl wie eine Verbraucherschutzorganisation wirken will, ist laut Impressum eine südafrikanische Werbeagentur. Die gibt es zumindest im Web tatsächlich, doch die beim Club-Impressum genannte Geschäftsführerin ist im Agenturteam nicht zu finden. Laut whois-Information ist die Club-Domain auch nicht in Südafrika, sondern in Nassau auf den Bahamas registriert.

Je nachdem, wann man auf die UltraXtend-Seite stößt, zeigt sie ein anderes Gerät: Im Mai 2022 war es das hier getestete Modell, vier Wochen später schon ein anderes. Mit Glück kann man an einem Aufdruck des gezeigten Produkts erkennen, dass der Wunder-Repeater nach dem veralteten WLAN-Standard IEEE 802.11n alias Wi-Fi 4 arbeitet, und den Reinfall vermeiden. Denn aktuell ist Wi-Fi 6 alias IEEE 802.11ax (ct.de/wvpg), akzeptabel wäre noch Wi-Fi 5 (802.11ac).

Hanebüchen wird es bei dieser Behauptung: „Dank der verbauten Glasfaser-Technologie […] schafft es der WLAN-Verstärker, die verloren gegangene Geschwindigkeit aufzufangen und ebenfalls an Ihr Endgerät zu senden.“ Spätestens bei solchem Humbug sollte jede(r) misstrauisch werden. Wenn der Repeater eine schwache WLAN-Verbindung zum Router hat, kann auch eine noch so tolle Glasfaser nichts mehr ausrichten. Sie kann nur das weiterleiten, was da ist. Und warum die Geschwindigkeitsrückgewinnung innerhalb des Gerätes geschehen

**UltraXtend alias RangeXTD verbessert zwar tatsächlich die Funkabdeckung, übertrug im Test aber selbst im Bestfall nicht einmal 100 Mbit/s. Für 50 Euro bekommt man anderswo mehr WLAN.**

## Repeater-Durchsatz im Vergleich

| | AP-Modus | | | | Backbone | Repeater-Modus | | Leistungsaufnahme |
|---|---|---|---|---|---|---|---|---|
| | 2,4 GHz | 2,4 GHz | 5 GHz | 5 GHz | | 2,4 GHz | 5 GHz | |
| | nah | 20 Meter | nah | 20 Meter | 20 Meter | 20+6 Meter | 20+6 Meter | |
| | besser ▶ | besser ▶ | besser ▶ | besser ▶ | besser ▶ | besser ▶ | besser ▶ | ◀ besser |
| Pix-Link WR22 | 92 | 88 | – | – | 83 | 50 | – | 1,3 |
| AVM Fritz-Repeater 1200 | 205 | 205 | 510 | 122 | 363 | 204 | 96 | 3,0 |

Durchsatz in Mbit/s, gemessen mit Intel AX200 und Asus GT-AXE11000, Leistungsaufnahme in Watt

sollte, bleibt im Dunkeln. Unter der Haube haben wir auch nicht das kleinste Fitzelchen Glasfaser gefunden.

In der Praxis erreicht das von uns online georderte Kästchen selbst unter optimalen Bedingungen nicht mal die genannten 100 Mbit/s, weil es ein technisch längst überholter WLAN-Repeater billigster Machart ist. Was hier für 50 Euro angeboten wird, kostet in der chinesischen Online-Ladenzeile in größerer Menge keine 7 US-Dollar (plus Versand). Suchen Sie mal nach „Pix-Link WR22 300M Alibaba“.

Ein Repeater ist im Alltag besser als keiner, was sich in anekdotischen Erfahrungen wie „mit Repeater hab ich aber wenigstens 20 Mbit/s statt gar nix“ niederschlägt. Ein guter Repeater ist aber noch besser. Deshalb haben wir als Praxistest UltraXtend ein nur wenig teureres, aber gleich kompaktes und etwas moderneres Gerät gegenübergestellt (Fritz-Repeater 1200 für Wi-Fi 5, Test in c’t 19/2019, S. 90) und beide auf der c’t-WLAN-Teststrecke vermessen. Was herauskam, verwundert wenig: Das Markengerät liefert mehr Durchsatz, meist sogar viel mehr (siehe Balkendiagramm), zieht dafür aber mit 3,0 statt 1,3 Watt auch mehr Leistung aus der Steckdose.

Zugegeben, der Vergleich ist unfair, kann doch der 1200er-Repeater die beiden WLAN-Bänder 2,4 und 5 GHz gleichzeitig nutzen, wogegen UltraXtend ausschließlich im unteren Band funkt. Da der Fritz-Repeater 1200 aber gebraucht schon für weniger zu finden ist, als UltraXtend neu kostet, erscheint uns die Gegenüberstellung legitim.

## Ausstattung und Performance

Das im September 2014 von Mediatek vorgestellte System-on-Chip (SoC) MT7628 bildet den Kern von UltraXtend. Der Baustein (Beschreibung über ct.de/wvpg) steckt auch in Einfachst-Routern wie beispielsweise dem TP-Link TL-WR840Nv4 für 15 Euro. Das SoC funkt über zwei MIMO-Streams gemäß IEEE 802.11n und erreicht damit auf dem 2,4-GHz-Band maximal 300 Mbit/s brutto.

Beim UltraXTend ist ein Fast-Ethernet-Port herausgeführt, der 100 Mbit/s transportiert, womit das Gerät auch als Access-Point (AP) arbeiten kann, der als autonome WLAN-Basis per LAN-Kabel mit dem Router verbunden wird.

Als AP übertrug der Repeater zu unserem Wi-Fi-6-Client Intel AX200 in einem Asus-Notebook in der Nähe bestenfalls 92 Mbit/s, über 20 Meter mit Wänden noch 88 Mbit/s. Mit einem Asus-Wi-Fi-6E-Router als Basis reichte UltraXtend an der 20-Meter-Position gerade mal 50 Mbit/s ans weitere 6 Meter entfernte Notebook durch.

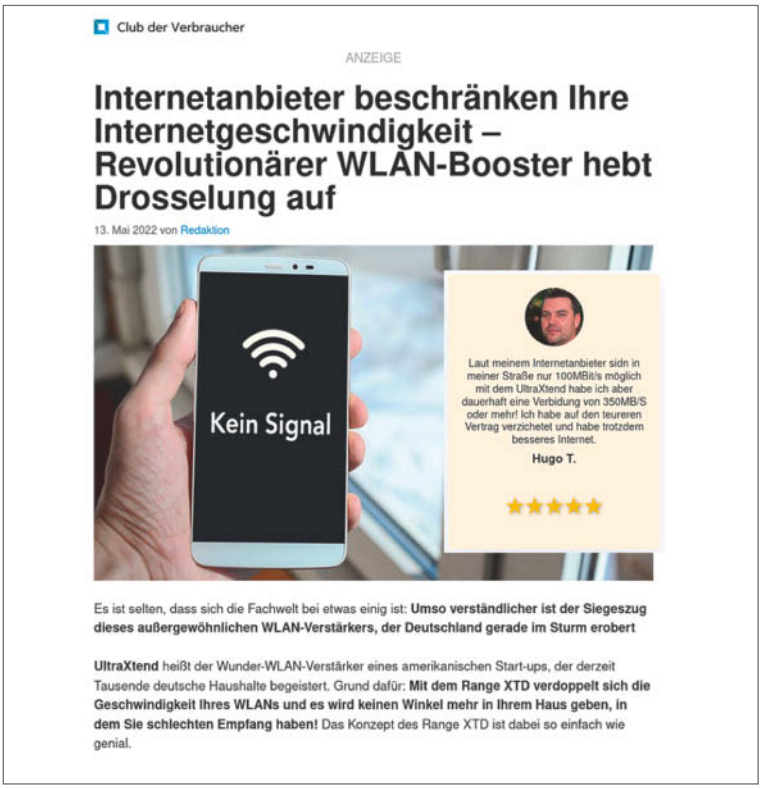
Hier wirkt sich der Repeater-Effekt von Single-Band-Geräten aus: Erst Paket empfangen, dann auf demselben Funkkanal nochmal versenden kostet zusätzliche Sendezeit, was den Durchsatz ungefähr halbiert. Koppelten wir UltraXtend am 20-Meter-Punkt per LAN-Kabel, kamen beim Notebook wieder fast 90 Mbit/s an.

Dieser Effekt fällt beim Fritz-Repeater 1200 weg, denn der kann ja in beiden Bändern gleichzeitig funken: Daten auf 5 GHz vom Router annehmen und quasi verzugsfrei auf 2,4 GHz weitergeben. So bekam das Notebook den vierfachen Durchsatz im 2,4-GHz-Band und auf 5 GHz immerhin noch das Doppelte.

## Mehr Mängel

Unsere Testmuster kamen von „Eshipping“ über die Hermes-Niederlassung am Frankfurter Frachtflughafen. Wie die Repeater den Zoll passiert haben, ist uns schleierhaft: Der hält gern Importe zurück, wenn wie beim UltraXtend keine deutschsprachige Kurz-


**Auf der UltraXtend-Platine sitzt ein Systemchip MT7628 von 2014, der nach dem alten WLAN-Standard IEEE 802.11n alias Wi-Fi 4 funkt. Aktuell ist Wi-Fi 6, akzeptabel noch Wi-Fi 5. Von einer angeblich verwendeten „Glasfaser-Technologie“ ist nichts zu sehen. Sie wäre im Repeater auch sinnlos.**




**WLAN-Schlangenöl par excellence: Die bösen Provider drosseln das Internet, ein Repeater soll die Bremse lösen. Doch der kann nicht wiederherstellen, was am Router Internetseitig gar nicht erst ankommt. (Screenshot-Collage Stand Mai 2022)**

anleitung beiliegt, sondern nur eine englische. Zwar prangt auf dem Karton ein CE-Zeichen, nicht aber auf dem Gerät selbst.

Die Mängel setzten sich im Netzwerk fort: UltraXtend leitete im Test keine Multicast-Pakete weiter. So bekommen Clients am Repeater kein IPv6, auch wenn es in der WLAN-Zelle des Routers funktioniert. Multicast-IPTV-Streams wie das MagentaTV der Deutschen Telekom liefen auch nicht an.

Im Access-Point-Modus brachte UltraXtend unser Testnetz durcheinander: Wir setzten per Browser eine zum LAN passende IPv4-Adresse und schalteten seine DHCP-Funktion ab. Trotzdem antwortete UltraXtend nach dem fälligen Neustart auf DHCP-Anfragen anderer Hosts im LAN und gab sich dabei als Internet-Gateway für seinen Standard-Adressbereich 192.168.7.0/24 aus. In der Folge brach für diese Geräte die Internetverbindung weg. Bei mehreren Versuchen speicherte das Gerät das Abschalten der DHCP-Funktion nie. Auf unsere Anfrage reagierte der Anbieter bis Redaktionsschluss nur mit vorgestanzten Mails, dass man froh sei, weiterhelfen zu können und dass man unser Anliegen intern weitergegeben habe. Zum schwachen WLAN-Durchsatz und den Netzwerk-Mängeln gab es keine Antwort.

Bleibt zu hoffen, dass Kunden, die UltraXtend auf den Leim gegangen sind, das Gerät genauso problemlos zurückgeben können wie das Stromspar-Neppkästchen Voltbox (c't 25/2021, S. 32). Dazu berichtete uns ein Käufer im Nachgang, dass die Erstattung geklappt hatte.

## Fazit

Finger weg: Die Versprechungen für UltraXtend alias RangeXTD sind heillos überzogen. Das Kästchen funktioniert zwar als Repeater, aber für das, was es praktisch kann, ist sein Preis viel zu hoch.

Gönnen Sie sich statt dieses Elektroschrotts lieber für ein paar Euro mehr ein aktuelles Markengerät, das zu Ihrem Router passt und dessen Mesh-WLAN unterstützt, flinker funkt und keine der unter „Mehr Mängel“ beschriebenen Macken hat. (ea) *c't*

**UltraXtend-Website, WLAN-FAQ**

**ct.de/wvpg**

# TAUCHE EIN IN DIGITALE WELTEN – MIT DEM c't DIGITALABO

**40 % Rabatt!**




## c't MINIABO DIGITAL AUF EINEN BLICK:

- 6 Ausgaben digital in der App, im Browser und als PDF
- Inklusive Geschenk nach Wahl
- Mit dem Digitalabo Geld und Papier sparen
- Zugriff auf das Artikel-Archiv

Jetzt bestellen:

**ct.de/angebotdigital**



**ct.de/angebotdigital** | **+49 541/80 009 120** | **leserservice@heise.de**

# Wi-Fi 7: Die nächste WLAN-Generation

**Wi-Fi 7 soll endlich echtes Multigigabit-WLAN ermöglichen, damit auch ein auf 2 Gbit/s beschleunigtes Glasfaser-Internet von morgen verlustfrei im ganzen Haus ankommt. Unsere ersten Messungen an einem Routerpärchen zeigen, dass das kein leeres Versprechen ist.**

Von **Ernst Ahlers**


**TP-Links Wi-Fi-7-Router Deco BE85 ist mit zwei 10-Gigabit-Ethernet-Ports auf extraschnelles Internet ausgerichtet.**

Gigabit-Internet liefert 1000 Megabit pro Sekunde und ist vielerorts per TV-Kabel oder manchmal auch schon per Glasfaser verfügbar. Doch der aktuelle WLAN-Standard Wi-Fi 6 alias IEEE 802.11ax trägt die hohe Geschwindigkeit in der Praxis nur auf kurze Distanzen verlustfrei weiter. Das dürfte der jetzt in ersten Geräten erscheinende Nachfolger Wi-Fi 7 (IEEE 802.11be) ändern.

Wi-Fi 7 soll die Funkdatenrate noch mal vervielfachen [1, 2]: Nach gegenwärtigem Stand kann es im neuen 6-GHz-Frequenzband mit einem extrabreiten Signal von 320 statt 160 MHz und über die maximal acht MIMO-Streams bei guten Funkbedingungen satte 23 Gigabit pro Sekunde brutto schicken; bei Wi-Fi 6 sind es maximal 9,6 Gbit/s.

Bisher haben die Hersteller nur Wi-Fi-7-Router angekündigt, deren drei Funkmodule jeweils mit höchstens vier MIMO-Streams funken, also auf bis zu 11,5 Gbit/s kommen. Darauf beschränkt sich auch der erste in der c't-Redaktion eingetroffene Wi-Fi-7-Router Deco BE85 von TP-Link: Seine WLAN-Module transportieren in den drei Bändern bis zu 1376 Mbit/s (40-MHz-Signal auf 2,4 GHz), 5760 Mbit/s (160 MHz bei 5 GHz) und 11.520 Mbit/s (6 GHz).

Der große Zuwachs im 6-GHz-Band kommt zum überwiegenden Teil durch das breitere Signal zustande: Die höchste bei guter Funkverbindung mögliche Kodierung von Wi-Fi 7 (4096QAM mit 12 Bit/Symbol) bringt gerade mal 20 Prozent mehr als 1024QAM bei Wi-Fi 6 (10 Bit/Symbol, mit vier MIMO-Streams 1150 und 4800 Mbit/s auf 2,4 und 5 GHz).

## Parallelfunk

Mit Multi-Link Operation (MLO) führt Wi-Fi 7 eine nützliche neue Funktion ein: Geräte können Daten in mehreren Frequenzbändern gleichzeitig übertragen. Das steigert entweder den Durchsatz, indem unterschiedliche Datenpakete über verschiedene Bänder laufen. Oder es verbessert die Zuverlässigkeit, wenn dasselbe Datenpaket über mehrere Bänder fließt. Auch die gefürchteten Verbindungsabrisse, wenn mobile Clients die Funkzelle wechseln, dürften so seltener werden.

Noch ist der nächste WLAN-Standard nicht fertig, doch Chiphersteller und Routerfabrikanten haben längst erste Produkte angekündigt und auch schon im Markt. Wir hatten Gelegenheit, ein Paar der im Herbst 2022 angekündigten BE85 auszuprobieren.

Dabei gibt es einen Haken: Clients für Wi-Fi 7 sind noch rar. Einzig ein paar Smartphones wie etwa das Xiaomi 13 Pro haben schon den neuen Schnellfunk. Intel bereitet zwar Wi-Fi-7-Module für Notebooks und PCs unter den Typenbezeichnungen BE200 (für PCI-Express-Anschluss) und BE201 (CNVi, proprietäre Prozessorschnittstelle) vor. Aber auf der Computex-

Messe Anfang Juni hieß es, sie würden frühestens Ende 2023 auf den Markt kommen [3]. So konnten wir die Rasanz des kommenden Standards nur auf dem Mesh-Backbone zweier Router testen (Bridge-Modus). Dazu koppelten wir die BE85 als Mesh-Nodes und schickten die Daten über ihre 10-Gigabit-Ethernet-Ports.

Zwar ließ sich mit einem Handheld-Spektrumanalyzer physikalisch auf Layer 1 klären, dass MLO schon funktioniert und die BE85 tatsächlich in mehreren Funkbändern parallel Daten übertragen. Leider wirkt der MLO-Schalter in TP-Links Mesh-Konfigurations-App nur auf Client-Verbindungen und nicht auf jene zwischen den Mesh-Nodes. So konnten wir noch nicht testen, ob und wie stark MLO praktisch auf Speed und Latenz wirkt.

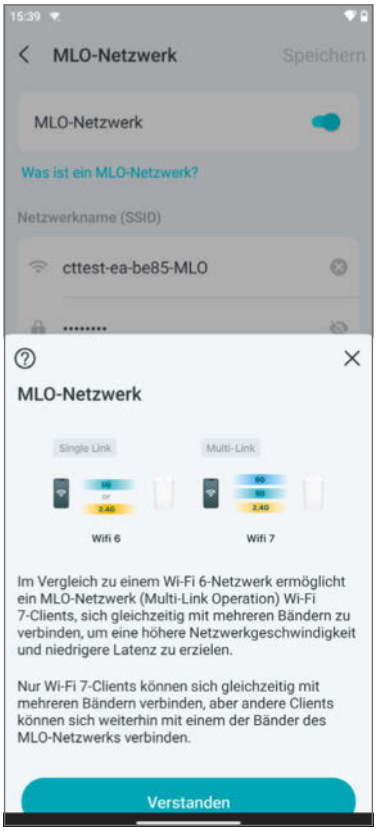
Mit einem Wi-Fi-6E-fähigen Notebook überprüften wir, dass die Wi-Fi-7-Basen auch ältere Clients bedienen, also abwärtskompatibel sind. Die gemessenen Durchsätze fielen erwartungsgemäß aus (siehe Tabelle). Man muss also nicht gleich alle WLAN-Clients ersetzen, wenn Wi-Fi 7 einzieht. Umgekehrt bringt es aber auch nichts, jetzt schon in einen Wi-Fi-7-Router zu investieren, solange es im Haushalt noch keine Wi-Fi-7-Clients gibt.

## Ausprobiert

Schon der Vorabtest im Redaktionsbüro deutete an, dass dieses Wi-Fi-7-Gespann schnell ist. Einzelne Spitzen des Nettodurchsatzes auf Anwendungsebene erreichten rasante 7,8 Gbit/s. Der Eindruck bestätigte sich bei der systematischen Messung im Verlagskeller, wo keine anderen WLANs im 2,4- und 5-GHz-Band stören.

Mit einem TCP-Stream, also einem Down- oder Upload, transportierte der BE85-Mesh-Backbone im Mittel beider Richtungen bei guter Funkverbindung auf kurze Distanz rund 3 Gbit/s. Mit mehreren parallelen Übertragungen wurden es sogar 7,1 Gbit/s. Ein hypothetischer Wi-Fi-7-Laptop mit zwei Antennen (Zwei-Stream-WLAN) würde als Client die Hälfte bekommen.

Über 20 Meter durch Wände schaffte das Wi-Fi-7-Deco-Pärchen ebenfalls einen deutlich höheren Durchsatz als wir bisher sahen: 925 Mbit/s bei günstiger Ausrichtung genügen, um einen Gigabit-Internetanschluss fast auszuschöpfen, denn mehr als rund 940 Mbit/s gibt er derzeit ohnehin nicht her. Die besten in diesem Sonderheft vorgestellten Wi-Fi-6-Mesh-Systeme kamen in dieser Konstellation nur auf etwas über 600 Mbit/s.




**Die mit Wi-Fi 7 kommende neue WLAN-Funktion Multi-Link Operation (MLO) muss man erst einschalten. Dann sendet der Router Daten an seine Clients über mehrere WLAN-Bänder (2,4, 5 und 6 GHz) gleichzeitig.**

Mit mehreren parallelen Übertragungen schoss die Datenrate des BE85-Backbones über Distanz sogar auf bis zu 2,5 Gbit/s hoch, ein bislang im c't-Labor unerreichter Wert. Davon profitieren besonders Mesh-Systeme, deren Repeater-Nodes mehrere Clients bedienen müssen.

## Angepingt

Für Gamer ist nicht die absolute Geschwindigkeit, sondern die Latenz entscheidend: Datenpakete sollen mit möglichst wenig Verzug laufen.

## TP-Link Deco BE85

| WLAN-Router mit Wi-Fi 7 | | |
|---|---|---|
| Hersteller, URL | TP-Link, tp-link.com/de | |
| Anschlüsse | 4 × RJ45 (2 × 10GBase-T, 2 × 2,5G NBase-T), SFP+ (Komboport), 1 × USB 3.2 Gen 1 (5 Gbit/s) | |
| WLAN (MIMO-Streams) | 3 × Wi-Fi 7 (4) alias IEEE 802.11be-1376/5760/11520 (2,4 / 5 / 6 GHz), WPA3, MLO | |
| **Wi-Fi-6/6E-Kompatibilität**[1] | | |
| Client 2,4 GHz nah / 20 m | 351 / 159–223 Mbit/s | |
| 5 GHz nah / 20 m | 1386 / 191–241 Mbit/s | |
| 6 GHz nah / 20 m | 974 / 226–292 Mbit/s | |
| **Wi-Fi 7 (Mesh-Backbone)** | **1 TCP-Stream** | **6 TCP-Streams** |
| nah / 20 m | 3076 / 731–928 Mbit/s | 7143 / 2264–2457 Mbit/s |
| NAT-Performance PPPoE | 9,4 / 9,4 Gbit/s (Down-/Upstream) | |
| NAT-Performance IP/IP | 9,5 / 9,5 Gbit/s | |
| Idle-Leistung Gigabit-Links[2] | 17,5 / 18,6 W (33,7 / 35,7 VA) | |
| Idle-Leistung 10 Gigabit[2] | 20,8 / 20,3 W (38,6 / 38,1 VA) | |
| jährliche Stromkosten[3] | 57 bis 73 € | |
| Preis | 700 € (Amazon) | |

[1] gegen Intel AX210 in Galaxy Book Pro [2] BE85 als Mesh-Router, 2 × Kupfer / Kupfer+optisch; BE85 als Mesh-Node: 16,3 Watt (31,5 VA) ohne Ethernet, 17,0 Watt (32,4 VA) mit einem Gigabit-Link, 18,5 Watt (35,5 VA) mit einem 10GBase-T-Link [3] bei 40 Cent/kWh

Beim BE85-Pärchen maßen wir in der Nähe einen mittleren Ping von 2,9 bis 3,2 Millisekunden (Round Trip Time, RTT). Über Distanz war es mit 3,0 bis 9,1 ms etwas mehr. Interessanterweise transportierte ein zum Vergleich mit gemessenes Wi-Fi-6E-Pärchen des Typs Deco XE75 in beiden Fällen die Pakete flotter (1,2 bis 1,6 ms in der Nähe, 1,6 bis 1,8 ms auf Distanz). Doch diese Unterschiede sind im Alltag bedeutungslos, da sie weit unter der menschlichen Reaktionsgeschwindigkeit liegen.

Beim Vermitteln der Daten zwischen Internet und internem Netz (LAN und WLAN) hat der Deco BE85 genug Dampf selbst für einst kommende 10-Gigabit-Internetanschlüsse: Wir maßen mit den verbreiteten WAN-Protokollen PPPoE und IP/IP (DHCP) 9,4 und 9,5 Gbit/s in beide Richtungen. Dafür sorgt das potente System-on-Chip, ein Qualcomm IPQ9570, der vier mit bis zu 2,2 GHz Takt angetriebene ARM-Cortex-A73-Kerne hat.

## Wi-Fi 7 saugt

Die hohe Netz- und WLAN-Performance hat ihren Preis: Der Deco BE85 gönnt sich mindestens 16 Watt aus dem Stromnetz, mit schnellen Ethernet-Links sogar bis über 20. Das treibt die jährliche Stromrechnung pro Gerät bei gängigen 40 Cent/kWh im Schnitt um 60 Euro nach oben.

Seine Verlustwärme wird der BE85 mit seiner Kaminkonstruktion durch natürliche Konvektion los. Man sollte also nichts auf dem Gerät ablegen, das den Luftfluss blockiert. Wenn es dem Router dennoch zu warm wird, läuft vorübergehend ein Lüfter, der im c't-Büro kaum auffiel. Im heimischen Wohnzimmer dürfte das intermittierende Rauschen lästiger wirken.

## Fazit

Wi-Fi 7 ist ganz frisch, kaum den Windeln entwachsen und noch nicht mal richtig standardisiert. Schon deshalb sind unsere Ergebnisse am Wi-Fi-7-Erstling TP-Link Deco BE85 nur als vorläufig anzusehen. Gleichwohl bestätigen sie, dass Wi-Fi 7 wie versprochen mehr WLAN-Geschwindigkeit bringt, besonders wenn mehrere Übertragungen gleichzeitig laufen. Wer ab 2024 den heimischen Internetanschluss auf Gigabit hochstuft und dann schon mit einem einzelnen Notebook ausschöpfen will, sollte die neue WLAN-Technik in Erwägung ziehen.

Dass die neue Multiband-Übertragung MLO schon funktioniert, ließ sich zwar bestätigen, leider aber noch nicht, ob sie ihre Vorteile – unter anderem mehr Speed und weniger Latenz – in der Praxis auch umsetzen kann. Die weitere Entwicklung wird spannend, besonders wenn die ersten Wi-Fi-7-fähigen Notebooks erscheinen. Wir werden weiter testen. (ea) **c't**

### Literatur


[1] Jennifer Li, Ernst Ahlers, Warum Wi-Fi 6 besser funkt und was seine Nachfolger bringen, ct.de/-7352007

[2] Jennifer Li, WLAN-Wandel, Wi-Fi 8 wirft seinen Schatten voraus, c't 23/2022, S. 40 (auch online: ct.de/-7311245)

[3] Florian Müssig, Vor Wi-Fi 7 liegt noch eine Durststrecke, ct.de/-9154611

[4] Ernst Ahlers, FAQ: WLAN – Standards, Fachbegriffe, Schutzmechanismen, ct.de/-6033808

# IMPRESSUM


## Redaktion

**Postfach 61 04 07, 30604 Hannover**
**Karl-Wiechert-Allee 10, 30625 Hannover**
**Telefon: 05 11/53 52-300**
**Telefax: 05 11/53 52-417**
**Internet: www.heise.de**

**Leserbriefe und Fragen zum Heft:**
sonderhefte@ct.de

Die E-Mail-Adressen der Redakteure haben die Form xx@ct.de oder xxx@ct.de. Setzen Sie statt „xx" oder „xxx" bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

**Chefredakteur:** Torsten Beeck (tbe)
(verantwortlich für den Textteil)

**Konzeption:** Dušan Živadinović (dz)

**Koordination:** Jobst Kehrhahn (Leitung, keh), Pia Ehrhardt (piae), Angela Meyer (anm)

**Redaktion:** Ernst Ahlers (ea), Mirko Dölle (mid), Sven Hansen (sha), Christian Hirsch (chh), Angela Meyer (anm), Andrijan Möcker (amo), Dušan Živadinović (dz)

**Mitarbeiter dieser Ausgabe:** Benjamin Pfister, Sebastian Piecha, Alexander Traud

**Assistenz:** Susanne Cölle (suc), Tim Rittmeier (tir), Christopher Tränkmann (cht), Martin Triadan (mat)

**DTP-Produktion:** Dörte Bluhm, Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Kapell, Steffi Martens, Marei Stade, Matthias Timm, Christiane Tümmler, Ninett Wagner

**Digitale Produktion:** Christine Kreye (Ltg.), Kevin Harte, Thomas Kaltschmidt, Martin Kreft, Pascal Wissner

**Fotografie:** Andreas Wodrich, Melissa Ramson

**Illustration:** Albert Hulm, Berlin; Andreas Martini, Wettin; Michael Vogt, Berlin

**Titel:** Steffi Martens, www.freepik.com

## Verlag

**Heise Medien GmbH & Co. KG**
**Postfach 61 04 07, 30604 Hannover**
**Karl-Wiechert-Allee 10, 30625 Hannover**
**Telefon: 05 11/53 52-0**
**Telefax: 05 11/53 52-129**
**Internet: www.heise.de**

**Herausgeber:** Christian Heise, Ansgar Heise, Christian Persson

**Geschäftsführer:** Ansgar Heise, Beate Gerold

**Mitglieder der Geschäftsleitung:** Jörg Mühle, Falko Ossmann

**Anzeigenleitung:** Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

**Anzeigenverkauf:** Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

**Leiter Vertrieb und Marketing:** André Lux (-299)

**Service Sonderdrucke:** Julia Conrades (-156)

**Druck:** Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

**Vertrieb Einzelverkauf:**
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

**Einzelpreis:** € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

**Erstverkaufstag: 20.10.2023**





Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

# Wi-Fi-6-Router RT6600ax getestet


**Mesh-fähige Wi-Fi-6-WLAN-Router wie Synologys RT6600ax gibt es schon einige. Der Neuling funkt flott, das Spannende ist aber seine Firmware: Darin finden sich auch Nebenbei-Admins sofort zurecht und richten mit wenigen Klicks bis zu fünf Netzwerkzonen ein.**

Von **Ernst Ahlers**

Synologys jüngster WLAN-Router RT6600ax ist mit drei Wi-Fi-6-Funkmodulen (einmal 2,4 GHz, zweimal 5 GHz) gut für Mesh-WLAN-Systeme gerüstet; Synology hat dafür zurzeit nur den Wi-Fi-5-Meshrepeater MR2200ac im Programm.

Der Systeminfo zufolge sorgt im RT6600ax ein Qualcomm-System-on-Chip IPQ6018 mit vier 1,8 GHz flotten ARM-A53-Kernen für den Datentransport. Das schlug sich im Test mit hohem NAT- (siehe Tabelle, PPPoE begrenzt durch Testserver) und sehr gutem NAS-Durchsatz nieder (optimal mit einem ext4-Dateisystem, etwas niedriger mit NTFS). An der guten bis exzellenten WLAN-Leistung im Test mit einem Intel-AX200-bestückten Notebook gibt es nichts zu meckern; der Router unterstützt alle wichtigen Roaming-Funktionen (IEEE 802.11k, 11v, optional 11r) und die verbesserte WPA3-Verschlüsselung.

**Synology RT6600ax**

| WLAN-Router | |
|---|---|
| Hersteller, URL | Synology, synology.de |
| WLAN | 3 × Wi-Fi 6 (2+2+4) = IEEE 802.11ax-600 / 1200 / 4800, simultan dualband, WPA3, WPS, DFS |
| Anschlüsse | 5 × RJ45 (4 × Gigabit-Ethernet, 1 × Multigig-Eth. bis 2,5 Gbit/s) |
| Bedienelemente | Ein, Reset, WPS, WLAN, 7 Statusleuchten |
| Getestete Firmware | SRM 1.3-9193 |
| NAT-Perf. PPPoE (DS / US) | 797 / 814 Mbit/s |
| IP-zu-IP (DS / US) | 950 / 949 Mbit/s |
| WLAN 2,4 GHz nah / 20 m[1] | 269 / 128–197 Mbit/s |
| 5 GHz I nah / 20 m[1] | 808 / 138–176 Mbit/s |
| 5 GHz II nah / 20 m[1] | 1611 / 398–672 Mbit/s |
| NAS-Durchsatz große Dateien | 86 / 240 MByte/s (Schreiben / Lesen) |
| Leistungsaufnahme[2] | 11,5 Watt / 24,8 VA |
| Jährliche Stromkosten[2] | 40 € |
| Preis | 305 € |

[1] gegen Intel AX200 [2] idle, bei Dauerbetrieb, 40 Cent/kWh, gerundet

## Firmware-Sprung

Mit dem RT6600ax führt der Hersteller auch eine neue Firmware-Generation ein: Der Synology Router Manager (SRM) 1.3 bringt als wichtigste Neuheit die Unterstützung für VLANs (Netzwerkzonen, c't 8/2017, S. 80) im LAN und WLAN mit. Zwei – das interne Netz und das Gastnetz – sind vordefiniert. Bis zu drei weitere, etwa je eines für Kinder-PCs, IoT und Smart Home, kann man selbst anlegen.

Die Zonen bekommen auch eigene IPv6-Subnetze (Präfixe), was man aber nach der assistentenunterstützten Router-Einrichtung noch manuell aktivieren muss: DHCP-PD fürs WAN setzen, IPv6 in den Zonen aktivieren, Präfixe wählen, Stateless-DHCPv6 setzen. Die VLANs kann man an den LAN-Ports getaggt ausleiten (Trunk-Ports), um sie per Ethernet weiterzugeben. Leider ist das die Vorgabe und bringt Windows-PCs im LAN manchmal durcheinander; wenn nicht nötig, schalten Sie sie ab.

Wer schon mal ein Synology-NAS in Betrieb genommen hat, kommt mit den Konfigurationsseiten des RT6600ax schnell klar. Der Router ließ sich mit dem Browser-Assistenten über ein xDSL-Modem vergleichsweise leicht am Telekom-VDSL-Netz in Betrieb nehmen (in den ISP-Einstellungen VLAN-Tagging aktivieren, VID 7 für Internet eintragen). Er leitete

aber im Test trotz Aktivieren des IGMP-Proxys das Multicast-IPTV (Magenta TV) nicht in sein internes Netz weiter.

## Ausfallüberbrückung

Mit „Smart WAN“ kann man einen LAN-Port zum zweiten WAN-Port für eine Internet-Ersatzleitung umwidmen (Failover). So lenkte der Router den Verkehr bei Ausfall der Hauptleitung binnen 10 Sekunden auf den zweiten Anschluss um – leider aber nur für IPv4.

SRM 1.3 ist wie die Vorgängerversionen mit Add-ons erweiterbar, doch beim RT6600ax gab es zum Testzeitpunkt nur eine: „Safe Access“ setzt als Kindersicherung einen Webfilter und Zeitkontingente ein. Es kann mit Rückgriff auf Google Safe Browsing und eine Threat-Intelligence-Datenbank auch Zugriffe auf Malware-verseuchte Webseiten blockieren. Weitere von SRM 1.2 gewohnte Add-ons, beispielsweise der VPN-Server und der Medienserver, sind schon in Vorbereitung.

Die NAS-Herkunft des Herstellers macht sich bei der „Datenflusssteuerung“ bemerkbar, dem Quality of Service etwa für unterschiedliche Prioritäten verschiedener Verkehrstypen oder Geschwindigkeitsschranken. In deren Einstellungen kann man an manchen Stellen wie in Netzwerken üblich die Werte auch in bit/s vorgeben, an anderen aber nur in Byte/s. Da wäre Vereinheitlichung hilfreich.

An anderen Stellen hat Synology den entscheidenden Schritt weiter gedacht: Sein Gastnetz bot der RT6600ax auch im Access-Point-Betrieb an, sogar inklusive separatem IPv6-Präfix. Weitere VLANs kann man als WLAN-Zonen (Multi-SSID) anlegen, für ihre IP-Versorgung per VLAN-Tagging ist aber der vorgeschaltete Router zuständig.

## Fazit

Mit dem RT6600ax liefert Synology einen soliden Breitband-WLAN-Router mit Wi-Fi 6. Über die Nickeligkeiten der neuen Firmware-Generation kann man hinwegsehen, sie werden wohl bald durch Updates beseitigt. Schon die neue Hauptfunktion von SRM 1.3 – Netzwerkzonen per VLANs – wertet den Router deutlich auf. (ea) c't

# Fritz-Repeater 3000 AX

**Mit dem Modell 3000 AX hat AVM das Loch zwischen dem „kleinen“ Wi-Fi-6-Repeater 1200 AX und dem teuren 6000er geschlossen. Wir haben den Neuling durchgemessen und ordnen ihn ein.**

Von **Ernst Ahlers**

Wer sein Fritzbox-WLAN mit einem Wi-Fi-6-Repeater bis in die letzte Wohnungsecke ausdehnen wollte, hatte bei AVM bis vor Kurzem nur die Wahl zwischen dem günstigen Fritz-Repeater 1200 AX mit zwei 2-Stream-Funkmodulen und dem teuren 6000er-Modell, das mit drei 4-Stream-MIMO-Funkmodulen protzt. Dazwischen hat AVM den Fritz-Repeater 3000 AX platziert. Er soll jene locken, denen der 1200 AX für ihre 4-Stream-Fritzbox zu wenig Leistung verspricht, aber das große Schwestermodell zu teuer ist.

Der wesentliche Unterschied zwischen 6000er und 3000 AX: Letzterer hat für die Clientanbindung 2-Stream-Funkmodule, was in den allermeisten Fällen genügt. Zum Router hin nimmt der 3000 AX über ein 4-Stream-Modul Kontakt auf. Anders als der Fritz-Repeater 6000 kann er über seine 5-GHz-Module auch mit einem extrabreiten 160-MHz-Signal funken, was den Durchsatz gegenüber dem regulären 80-MHz-Betrieb verdoppelt – falls die Clients das auch können. Wir haben die drei Wi-Fi-6-Repeater mit aktueller Firmware in drei Situationen getestet (Access-Point, Mesh-Repeater mit einer Fritzbox 7590 AX und Mesh-Repeater mit LAN-Verbindung).

Wie seine Geschwister lässt sich der 3000 AX per simplem Connect-Knopfdruck ins Fritz-Mesh einbin-

## Fritz-Repeater für Wi-Fi-6-WLAN

| Typ | 1200 AX | 3000 AX | 6000 |
|---|---|---|---|
| Hersteller, URL | AVM, www.avm.de | | |
| WLAN | 2 × Wi-Fi 6 (2), 600 / 2400 Mbit/s, 160 MHz, WPA3, DFS | 3 × Wi-Fi 6 (2/2/4), 600 / 2400 / 4800 Mbit/s, 160 MHz, WPA3, DFS | 3 × Wi-Fi 6 (4), 1200 / 2400 / 2400 Mbit/s, WPA3, DFS |
| Bedienelemente | Connect, 1 Statusleuchte | Connect, 2 Statusleuchten | Connect, 2 Statusleuchten |
| Anschlüsse | 1 × LAN (Gigabit-Ethernet) | 2 × LAN (Gigabit-Ethernet) | 2 × LAN (2,5 und 1 Gbit/s) |
| getestete Firmware | 7.30 | 7.41 | 7.30 |
| WLAN 2,4 GHz nah / 20 m[1] | 350 / 105–215 Mbit/s | 416 / 97–244 Mbit/s | 404 / 213–291 Mbit/s |
| 5 GHz I nah / 20 m[1] | 946 / 126–156 Mbit/s | 941 / 71–121 Mbit/s | 940 / 133–184 Mbit/s |
| 5 GHz II nah / 20 m[1] | –[2] | 410 / 184–222 Mbit/s | 910 / 233–312 Mbit/s |
| Backbone-Durchsatz 20 m | 450–532 Mbit/s | 319–413 Mbit/s | 279–402 Mbit/s |
| Repeater-Durchsatz 26 m 2,4 / 5 GHz[1] | 229 / 132 Mbit/s | 181 / 137 Mbit/s | 265 / 209 Mbit/s |
| mit LAN-Backbone[1] | 180 / 293 Mbit/s | 160 / 333 Mbit/s | 254 / 333 Mbit/s |
| Leistungsaufnahme / Stromkosten[3] | 3,6 W (6,7 VA) / 13 € | 7,2 W (12,5 VA) / 25 € | 8,7 W (18,0 VA) / 31 € |
| Preis | 75 € | 148 € | 213 € |

[1] mit Intel AX200 (Treiber 22.190) und Fritzbox 7590 AX (FritzOS 7.31) [2] Fritz-Repeater 1200AX hat nur ein 5-GHz-Funkmodul [3] kein Traffic, kein Ethernet-Port belegt, Stromkosten jährlich bei Dauerbetrieb und 40 Cent/kWh

den und übernimmt alle relevanten Einstellungen von der Fritzbox. Die Fritz-Repeater funktionieren auch an anderen Routern, aber dann muss man nach der Tastenkopplung eventuell weitere Einstellungen per Browser anpassen, etwa unterschiedliche Funknetznamen für die WLAN-Bänder.

Mit unserem üblichen Wi-Fi-6-Client (Intel AX200 im Asus Vivobook 14) lagen die drei Repeater als Access-Points performancemäßig ungefähr gleichauf (siehe Tabelle). Über 20 Meter durch Wände erreichte der 6000er ein etwas höheres Niveau und zeigte sich tendenziell weniger ausrichtungsabhängig.

Als Mesh-Repeater am 20-Meter-Punkt zum sechs Meter weiter entfernten Notebook ließ sich der 3000 AX in unserer Testumgebung im 2,4-GHz-Band von beiden überholen. Auf 5 GHz lag er mit dem 1200 AX gleichauf und musste dem 6000er hinterherschauen.

Der größte Unterschied zwischen den drei Fritz-Repeatern für Wi-Fi 6 offenbarte sich beim Energiehunger: Der 1200 AX war mit 3,6 Watt Leistungsaufnahme geradezu bescheiden. Der 3000 AX gönnte sich schon das Doppelte und der WLAN-mäßig opulent ausgestattete 6000er noch einen Schluck mehr, was sich in den Stromkosten niederschlägt.

## Fazit

Fürs grüne Gewissen ist der 1200 AX der Fritz-Repeater der Wahl. Doch seine großen Geschwister kann man mit ihrem abgesetzten Steckernetzteil viel leichter für optimales Funken positionieren. Der 6000er hat dem 3000 AX mehr MIMO-Streams voraus, weswegen er in unserer Testsituation auch mehr Datenrate herausholte. So bleibt der 3000 AX ein kostspieliger Kompromiss zwischen maximalem Durchsatz und geringen Energiekosten. (ea) c't

# Draußen-WLAN

**Zyxels Outdoor-WLAN-Basis NWA55AXE versorgt den Garten oder das Firmengelände mit schnellem WLAN.**

Von **Ernst Ahlers**


Der Outdoor-AP NWA55AXE ist fürs Einbinden in Zyxels Cloud-Management Nebula vorgesehen, läuft per Browser-Konfiguration aber auch autonom. Admins finden sich dort zurecht, Einsteigern hilft der automatisch anlaufende Setup-Wizard. Ärgerlich: Auch mit Nacharbeiten an den DFS-Einstellungen und viel Probieren schafften wir es nicht, den AP regulierungskonform stabil nur auf 5-GHz-Kanälen ab 100 zu betreiben. Da sollte Zyxel nachbessern.

Dafür entschädigt der NWA55AXE mit guter WLAN-Performance und Multi-SSID-Betrieb mit VLAN-Tagging für mehrere Netzwerkzonen (Familie/Mitarbeiter, Gäste/Kunden, Smarthome/IoT). Im Mesh-Modus kann man mit mehreren Geräten die Abdeckung auch ohne LAN-Infrastruktur vergrößern. Betreiber kleiner Netze bekommen beim NWA55AXE einen guten Gegenwert fürs Geld. (ea) c't

### Zyxel NWA55AXE

| WLAN-Access-Point | |
|---|---|
| Hersteller, URL | Zyxel, zyxel.de |
| WLAN | 2 × Wi-Fi 6 (2) alias IEEE 802.11ax-600/1200, WPA3, DFS, Multi-SSID (8 pro Band, VLAN-Tagging) |
| Anschlüsse | 1 × RJ45 (Gigabit-Ethernet, PoE-PD, IEEE 802.3at) |
| getestete Firmware | 6.25(ABZL.5)C0 |
| WLAN 2,4 GHz nah / 20 m[1] | 146 / 55–137 Mbit/s |
| 5 GHz nah / 20 m[1] | 527 / 127–212 Mbit/s |
| Leistungsaufnahme[2] | 5,4 W (10,8 VA) |
| jährliche Stromkosten[2] | 19 € |
| Preis | 95 € |

[1] gegen Intel AX200 [2] idle, primär am beiliegendem PoE-Injektor, Dauerbetrieb, 40 Cent/kWh

# Mesh-Kit TP-Link Deco XE75 untersucht

**Das Mesh-System Deco XE75 von TP-Link deckt größere Wohnungen mit schnellem WLAN ab, auch im neuen 6-GHz-Funkband. Es kostet nicht mal ein Viertel des Erstlings vom Mitbewerber, hält aber bei der Performance gut mit.**

Von **Ernst Ahlers**

Netgear war Erster: Sein Mesh-WLAN-Kit Orbi RBK963 mit drei Basen zum Abdecken größerer Wohnungen und Häuser bedient Clients zusätzlich im neuen 6-GHz-Funkband (Wi-Fi 6E, siehe ct.de/wvxq). Es ist exzessiv ausgestattet, performant und teuer (siehe nachfolgenden Test).

| TP-Link Deco XE75 | |
|---|---|
| **Mesh-WLAN-System** | |
| Hersteller, URL | TP-Link, tp-link.de |
| WLAN | 3 × Wi-Fi 6 (2) = IEEE 802.11ax-600 / 2400 / 2400, simultan triband, WPA3, WPS, DFS |
| Anschlüsse | 3 × RJ45 (Gigabit-Ethernet) |
| Bedienelemente | Reset, 1 Statusleuchte |
| Getestete Firmware | 1.0.0 Rel. 40135 (10.3.2022) |
| NAT-Perf. PPPoE (DS / US) | 776 / 887 Mbit/s |
| IP-zu-IP (DS / US) | 940 / 938 Mbit/s |
| WLAN 2,4 GHz nah / 20 m[1] | 363 / 214–244 Mbit/s |
| 5 GHz nah / 20 m[1] | 922 / 302–387 Mbit/s |
| 6 GHz nah / 20 m[1] | 938 / 219–305 Mbit/s |
| Backbone-Durchsatz 20 m | 346–481 Mbit/s |
| Client-Durchsatz 26 m 2,4 / 5 / 6 GHz[1] | 189 / 292 / 312 Mbit/s |
| AP-Modus 26 m 2,4 / 5 / 6 GHz[1] | 223 / 321 / 337 Mbit/s |
| Leistungsaufnahme[2] | 21 W / 40 VA |
| jährliche Stromkosten[2] | 75 € |
| Preis | 380 € (Dreierset) |

[1] gegen Intel AX210 [2] Dreierset, idle, bei Dauerbetrieb, 40 Cent/kWh, gerundet

TP-Link hat dem WLAN-Porsche sein Deco XE75 als Mesh-Volkswagen entgegengestellt: Drei Nodes kosten zusammen knapp unter 400 Euro. Sie funken mit drei 2-Stream- statt vier 4-Stream-WLAN-Modulen und haben „nur“ Gigabit-Ethernet statt bis zu 10 Gbit/s an den Kabel-Ports. Doch das genügt für die heute gängigen Internetangebote. Mit üblichen Clients – Notebooks, Tablets, Smartphones – merkt man den Unterschied in der Praxis allenfalls, wenn viele Geräte über einen sehr schnellen Anschluss gleichzeitig große Downloads machen.

Mit unserem Test-Client (Intel AX210 in einem aufgerüsteten Asus-Notebook) maßen wir über 20 Meter durch Wände bei beiden Systemen näherungsweise denselben WLAN-Durchsatz (siehe Tabelle). Auch über einen Repeater-Node hinweg (26-m-Werte) gab es keine gravierenden Unterschiede. Einzig beim Backbone-Durchsatz (LAN-WLAN-LAN) landete Netgear in unserer Testsituation viel weiter vorne (750 bis 830 Mbit/s versus 350 bis 480 Mbit/s).

Fürs Client-Roaming unterstützt Deco die üblichen Funktionen (IEEE 802.11k: Radio Resource Measurement, 11v: BSS Transition). „Fast Roaming“ (11r) kann man aktivieren, aber das zugehörige Information Element 54 (Mobility Domain) fanden wir in den WLAN-Beacons (Steuerpakete als Anwesenheitssignal) nicht.

TP-Links sparsamere Hardware-Ausstattung macht sich schließlich auch positiv auf der Stromrechnung bemerkbar: Während sich ein Netgear-

Node rund 14 Watt gönnt, bescheidet sich das XE75-Pendant mit der Hälfte.

## Routing-Verhalten

Das Deco-System lässt sich per App leicht in Betrieb nehmen, aber ein TP-Link-Cloud-Konto ist unumgänglich. Nach dem Assistenten-geführten Setup sollte man noch ein paar Dinge nachholen: IPv6 aktivieren, auf die verbesserte Verschlüsselung „WPA3-Personal + WPA2-PSK“ umschalten und das Gastnetz einrichten. Damit Wi-Fi-6E-kompatible Geräte auch im noch weitgehend freien hohen WLAN-Funkband verbinden können, stellt man die 6-GHz-Funkzelle auf „WLAN-Netzwerk & Backhaul“ um.

Zum Einrichten eines Telekom-VDSL-Zugangs über ein xDSL-Modem betrieben wir den ersten Deco-Node zuerst an einem anderen Router, setzten in den Deco-Interneteinstellungen die IPTV/VLAN-Einstellung passend (VID 7, Prio. 0, mit 802.1Q-Tag) und steckten das Gerät danach ans Modem um. Multicast-IPTV (MagentaTV) funktionierte nur im Access-Point-Modus hinter dem anderen Router; in TP-Links Labor soll ein Magenta-Receiver problemlos funktioniert haben.

Deco trennt sein Gastnetz per Firewall-Regeln vom internen Netz, beide Zonen teilen sich die IPv4- und IPv6-Adressbereiche. So steht das Gastnetz auch im AP-Modus zur Verfügung.

Das System hat grundlegende Funktionen zur Kindersicherheit (Profile mit Geräten, URL-Filter, Inhaltsfilter mit neun Kategorien, Onlinezeitbegrenzung) sowie gerätebasierte Priorisierung. Für feinere Steuermöglichkeiten braucht man den nach 30 Tagen kostenpflichtigen Dienst HomeShield Pro für 6 Euro pro Monat.

## Fazit

Mit Deco XE75 macht TP-Link die 6-GHz-WLAN-Erweiterung Wi-Fi 6E massentauglich: 127 Euro pro Basis sind beim Haushaltsvorstand viel eher vertretbar als Netgears fünfmal so teure Orbi-Nodes. Das geht für die meisten Nutzer auch ohne Kompromisse in Sachen Performance. Und wer mehr Leistung will, darf auf kommende Geschwister gespannt sein. (ea) c't

**WLAN-FAQ**

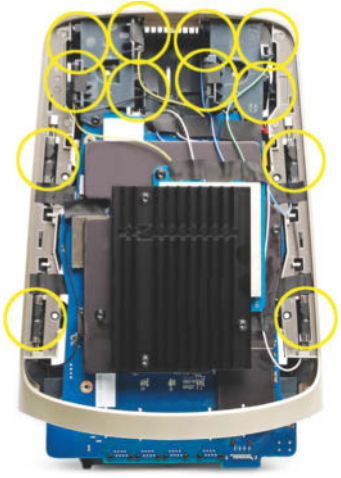
ct.de/wvxq

# Orbi RBKE963: Mesh-Kit mit Wi-Fi 6E


**Da kann der Netzwerk-Nerd das Sabbern nicht unterdrücken: Vier WLAN-Module für drei Funkbänder, zwölf Antennen, Multigigabit-Ethernet – in Netgears Mesh-Nodes Orbi 960 steckt alles, was gut und teuer ist. Die Hardware hält, was die Spezifikation verspricht, aber der Preis ist heftig und im Test zeigten sich ein paar Merkwürdigkeiten.**

Von **Ernst Ahlers**

Netgear gehört zu den Vorreitern beim Mesh-WLAN. Sein 2016 eingeführtes Orbi-System soll das schnelle Internet ohne neue Kabel und bei vollem Durchsatz noch in die letzte Ecke des Hauses bringen. Seitdem hat Orbi jede WLAN-Verbesserung mitgenommen.



**Die 16 Hochfrequenzports der vier 4-Stream-WLAN-Module hat Netgear auf zwölf Antennen verteilt. Weil diese etwas Abstand zueinander haben müssen, damit MIMO gut funktioniert, brauchen die Orbi-Nodes mit fast 30 Zentimetern Höhe vergleichsweise große Gehäuse.**

Nun kommt erstmals Wi-Fi 6E [1] ins Mesh: Zusätzlich zu den angestammten WLAN-Bändern 2,4 und 5 Gigahertz nutzt das Systemkit RBKE963 das neue und allerorten noch freie 6-GHz-Band, um kompatible Clients schnell mit Daten zu versorgen. Im Karton liegen ein Router als Mesh-Zentrale für die Internetanbindung und zwei Mesh-Repeater, „Satelliten“ in Netgears Vokabular. So viel sei vorweggenommen: Dieses Kit erwies sich im c’t-Labor als das bisher schnellste Mesh-System, aber mit fast 2000 Euro Straßenpreis auch mit Abstand als das teuerste – auch bei den Stromkosten (siehe Tabelle).

Für das viele Geld bekommt man viel: Der Internetanschluss des Routers (WAN-Port) überträgt gemäß NBase-T Multigigabit-Ethernet bis 10 Gigabit/s. Fürs interne Netz gibt es immerhin einen bis zu 2,5 Gbit/s schnellen LAN-Port sowie drei Gigabit-Ports. An den Repeatern entfällt der 10G-Anschluss.

In allen Nodes stecken gleich vier Wi-Fi-6-fähige WLAN-Schnittstellen, die über jeweils vier MIMO-Streams funken. Drei bedienen die Clients in unterschiedlichen Frequenzbereichen mit maximal 1200, 2400 beziehungsweise 4800 Megabit/s brutto (bei maximal 40, 80 und 160 MHz Kanalbreite), eine ist für die drahtlose Verbindung der Geräte untereinander im hohen Block des 5-GHz-Bandes reserviert (Mesh-Backbone, 2400 Mbit/s, 80 MHz).

Als CPU dürfte ein System-on-Chip Qualcomm IPQ8074A mit vier 2,2 GHz flotten ARM-Cortex-A53-Kernen fungieren. Das mechanisch fünflagige Hard-

## Literatur

[1] Jennifer Li, Von 540 auf 1040, Wie Wi-Fi 6E das WLAN-Spektrum verdoppelt, c’t 1/2021, S. 48

[2] Ernst Ahlers, 6er-Implantat, Notebooks auf den neuen WLAN-Standard aufrüsten, c’t 19/2019, S. 106

[3] Ernst Ahlers, Gute Zäune, gute Nachbarn, Getrennte Zonen im (W)LAN einrichten, c’t 8/2017, S. 80

[4] Ernst Ahlers, Ultrahochfunker, Test: WLAN-Router Asus GT-AXE11000 mit drei Funkmodulen, c’t 7/2022, S. 84

## Netgear Orbi RBKE963

| Mesh-WLAN-System | |
|---|---|
| Hersteller | Netgear, www.netgear.de |
| WLAN | 3 × Wi-Fi 6 (4) + Wi-Fi 6E (4) = IEEE 802.11ax-1200 / 2400 / 2400 / 4800, simultan triband, WPA3, WPS, DFS nur beim Mesh-Backbone |
| Bedienelemente | Sync, Reset, 2 Statusleuchten |
| Anschlüsse | Router: 5 × RJ45 (1 × 10 Gbit/s, 1 × 2,5 Gbit/s, 3 × Gigabit-Ethernet), Repeater: 4 × RJ45 (1 × 2,5 Gbit/s, 3 × Gigabit-Ethernet) |
| getestete Firmware | 6.0.3.85 |
| NAT-Perf. PPPoE (DS / US) | 793 / 908 Mbit/s |
| IP-zu-IP (DS / US) | 2370 / 2350 Mbit/s |
| WLAN 2,4 GHz nah / 20 m[1] | 299 / 214–238 Mbit/s |
| 5 GHz nah / 20 m[1] | 835 / 254–363 Mbit/s |
| 6 GHz nah / 20 m[1] | 1448 / 243–322 Mbit/s |
| Backbone-Durchsatz 20 m | 753–828 Mbit/s |
| Client-Durchsatz 26 m 2,4 / 5 / 6 GHz[1] | 190 / 347 / 231 Mbit/s |
| AP-Modus 26 m 2,4 / 5 / 6 GHz[1] | 188 / 375 / 266 Mbit/s |
| Leistungsaufnahme System[2] | 43 W / 89 VA (idle) |
| jährliche Stromkosten[2] | 151 € |
| Preis | 1900 € (3er-Set) |

[1] gegen Intel AX210, vorläufig [2] 3er-Set, idle, bei Dauerbetrieb, 40 Cent/kWh, gerundet

waregebilde im Routergehäuse trauten wir uns nicht komplett zu zerlegen, sodass der weit oben gefundene WLAN-Chip QCN9024 – der kleine Bruder des 9074 – fürs 6-GHz-Band als sehr sicheres Indiz herhalten muss.

## WLAN-Performance

Mit dem Intel-WLAN-Modul AX210 unseres selbst aufgerüsteten Testnotebooks [2] verstand sich der Orbi-Router bestens. Der Nettodurchsatz in der Nähe lag je nach Band zwischen 300 und knapp 1500 Mbit/s. Über eine größere Strecke durch Wände sackte die Datenrate erwartungsgemäß ab, war aber immer noch sehr gut. Im 6-GHz-Band könnte die Geschwindigkeit mit dafür tauglichen Antennen im Client noch etwas klettern, denn unser Notebook ist im Originalzustand nur für Dualband-Betrieb ausgelegt.

Die Verbindung zwischen Router und Repeater war über die 20-Meter-Strecke mit 750 bis 830 Mbit/s sehr flott, sodass das Notebook im Mesh-Betrieb am 26-Meter-Punkt je nach Band immer noch 190

bis 350 Mbit/s bekam. Mittelschnelle Internetanschlüsse der 250-Mbit/s-Klasse sollte man mit dem Mesh also meistens ausschöpfen können.

Das Client-Roaming zwischen den Basen unterstützt das Orbi-System mit den üblichen WLAN-Funktionen (IEEE 802.11k, Radio Resource Measurement, 11v, BSS Transition). Eine Dreierkette aus Router, Repeater und Repeater in den c't-Fluren lieferte vom T-VDSL250-Anschluss über 65 Meter auch noch rund 240 Mbit/s. Beim Wechsel zwischen den Basen zeigten Audiostreams nur selten Aussetzer und die können auch am Client liegen.

Mit dem Weiterleiten schneller Anschlüsse ins LAN hatte der Router kein Problem: Die gemessenen 900 Mbit/s beim PPPoE-WAN-Protokoll dürften die Grenze unseres Testsetups darstellen. Der Router kann sehr wahrscheinlich einiges mehr, denn mit DHCP kamen wir immerhin auf knapp 2,4 Gbit/s.

In Sachen VPN sieht es hingegen trübe aus: Orbi bietet nur OpenVPN an, weder IPsec noch das moderne WireGuard. Zu einem Host im LAN ließen sich aus dem simulierten Internet heraus damit nur rund 80 Mbit/s übertragen.

## Einrichtung

Das Mesh-System richtet man bequem per Smartphone-App ein, doch diese zeigte sich ignorant: Weder bot die App an, das heute unverzichtbare IPv6-Protokoll zu aktivieren, noch wies sie auf das ab Werk ausgeschaltete Gast-WLAN hin. Das muss leider auch nach Aktivieren von IPv6 im Hauptnetz ohne das moderne Protokoll auskommen, die verbesserte WLAN-Verschlüsselung WPA2+3 (Mixed-Mode) kann man für Gäste nur per Browser aktivieren. Auf 6 GHz fehlte das Gastnetz.

Als Besonderheit bietet Orbi zwei weitere WLAN-SSIDs (virtuelle Funkzellen) an, eine für IoT- und Smart-Home-Geräte, die andere nur auf dem neuen Funkband, wenn man einen Client ausschließlich über 6 GHz anbinden will. Doch anders, als man hoffen könnte, führen diese zusätzlichen Funkzellen gleichfalls ins Hauptnetz und nicht in separate Netzwerkzonen (VLANs, [3]), was mindestens fürs IoT nützlich wäre.

Wer Orbi über ein Modem an einem VDSL-Anschluss der Deutschen Telekom betreiben will, kommt mit der App nicht weiter, sondern muss per Browser tief in den Einstellungen wühlen, um das erforderliche VLAN-Tag (VID 7 für PPPoE) zu setzen. Immerhin funktioniert dann neben IPv6 auch das Live-TV per Multicast (MagentaTV) klötzchenfrei in LAN und WLAN. In einer Kaskade nachgeschaltete Router bekommen aber kein IPv6.

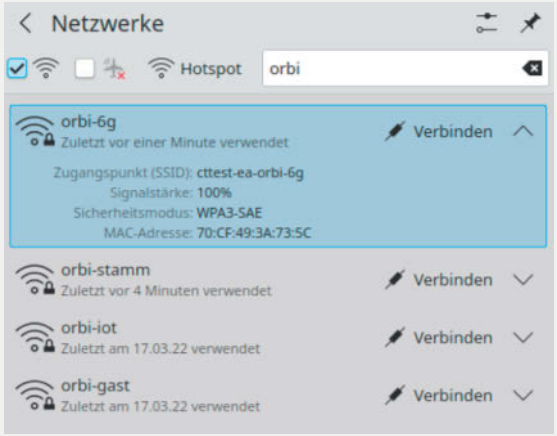
Ärgerlich: Ohne AGB-Abnicken geht es heute nirgendwo mehr weiter. Netgear setzt einem dafür geschlagene 119 KByte Text vor – das lesen womöglich sogar Juristen nicht komplett. Ferner versucht Netgear hartnäckig, kostenpflichtige Abodienste für Malwareschutz (Netgear Armor alias Bitdefender) und Kindersicherung an die Frau und den Mann zu bringen.

## Fazit

Das Wi-Fi-6E-fähige Orbi-Kit RBKE zeigt, was heute WLAN-technisch geht: opulente Hardware, exzellente Performance, dezentes Gerätedesign. Das darf man bei dem exorbitanten Preis auch erwarten – aber ebenso, dass Netgear die oben beschriebenen Macken noch abstellt. (ea) c't

## Wi-Fi 6E unter Linux

Nach unseren ersten vergeblichen Versuchen mit Wi-Fi 6E auf einem dafür ausgelegten Samsung Galaxy Book Pro unter Windows 11 [4] probierten wir es auch mit Linux. Eine parallele Kubuntu-21.10-Installation mochte die 6-GHz-Funkzellen noch nicht erkennen. Nach dem Upgrade auf die Beta-Ausgabe der Version 22.04 (`sudo do-release-upgrade -d`) erschienen sie auch auf diesem Gerät und ließen sich mit dem Network Manager wie gewohnt verbinden. Die Hardware ist also tatsächlich Wi-Fi-6E-fähig.




**Kubuntu 22.04 baut mit dem WLAN-Modul Intel AX210 Verbindungen über den Network Manager im 6-GHz-Band auf.**

**WLAN-FAQ**

**ct.de/wgku**

Minds Mastering Machines

# MLOps 2023

## ML-Anwendungen implementieren und optimieren

**9. November – Online Deep Dive**

### Lernen Sie, wie Sie Modelle effizient in Produktion bringen und zuverlässig betreiben

- Vom Proof of Concept zum produktiven Einsatz
- CI/CD für Machine Learning
- Trainingsdaten effizient verwalten
- Hyperparameter optimieren mit AutoML
- Modelle mit Kubernetes deployen
- MLOps-Prozesse absichern

Jetzt Tickets sichern!

**m3-konferenz.de/mlops.php**

**Workshop am 13. November: Schritt für Schritt zur erklärbaren KI**

Veranstalter

iX MAGAZIN FÜR PROFESSIONELLE IT

dpunkt.verlag

# Netzwerkkabel günstig nachgerüstet

**Stockende Videos und hakende Videokonferenzen aufgrund von lahmem WLAN und Powerline können den Geduldsfaden auf Spannung ziehen. Aber nur für wenige Jahre in der Mietwohnung teuer Netzwerkkabel in die Wand legen und renovieren? Muss nicht sein, so geht Gigabit-Ethernet günstig!**

Von **Andrijan Möcker**

Egal wohin man schaut: Überall gibt es kleine oder größere Netzwehwehchen; lahmes WLAN oder Powerline, schlechter Empfang und so weiter. Die Situation ist tatsächlich prekär, denn viele Menschen leben in Mietobjekten, wovon der Großteil seit Jahrzehnten nicht kernsaniert wurde. Selbst wenn, spart sich fast jeder Vermieter die Netzwerkinstallation; es gibt ja schließlich WLAN, so oft die Auffassung, und man muss ja nicht selbst drin wohnen.

Die alternativ aufgebaute kabellose Internetversorgung über WLAN-Mesh-Sets oder Powerline-Adapter (Ethernet übers Hausstromnetz) kommt jedoch vergleichsweise teuer und bleibt in puncto Geschwindigkeit oft hinter der Herstellerwerbung zurück; insbesondere, wenn massive Wände oder lange Stromleitungen die WLAN- beziehungsweise Powerline-Signale abschwächen. Groß ist die Enttäuschung, wenn von den 500 Mbit/s des neuen Glasfaseranschlusses drei Räume weiter nur 50 bis 100 Mbit/s übrig sind. Kurzum: Nur Twisted-Pair-Netzwerkkabel schaffen die Daten wirklich flott und günstig durchs Heim zum Router. Führen zusätzliche WLAN-Basen die Daten per Kabel statt durch die Luft zum Router, ist man auch an Mobilgeräten schneller unterwegs.

In einer Mietwohnung möchte man aber nicht tausende Euro für eine Netzwerkinstallation vom Elektriker und die dann erforderliche Renovierung ausgeben. Deshalb haben wir den Bauvorschlag fürs günstige Gigabit-Heimnetz zusammengestellt: Mit steckerlosem Netzwerkkabel, einfachen RJ45-Dosen, Plastik-Patchpaneln und Kabelkanal-Sockelleisten können Sie das Problem lösen. Dabei ist egal, ob Sie die ganze Wohnung verkabeln wollen oder nur zwei Anschlüsse benötigen. Die Installationskosten beginnen bei etwa 140 Euro für zwei Räume und vier Dosen.

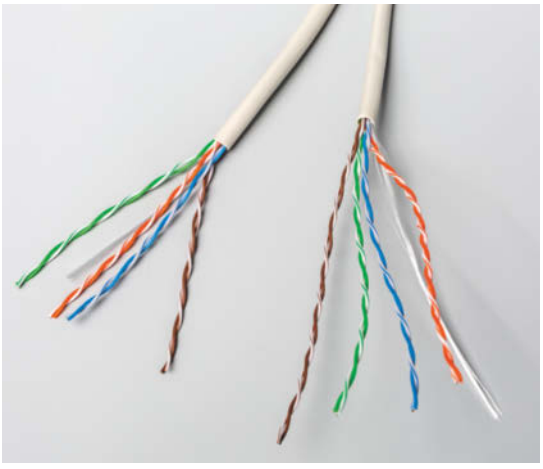
Kern der Idee ist, Sockelleisten mit Kabeln zu versehen oder gegen solche mit Kabelkanal auszutauschen und so eine Netzwerkverteilung minimalinvasiv aufzubauen. Zwar bleibt Ihnen das Verrücken der Möbel und das Bohren nicht erspart, wohl aber das Aufstemmen der Wände und die Putz- und Tapezierarbeiten. Nachfolgend schildern wir, was Sie brauchen und wie Sie vorgehen.

## Gigabit-Kompromiss

Wer professionell Netzwerke installiert, wird sicher an der einen oder anderen Stelle Tränen in den Augen haben und das zu Recht: Unser Vorschlag entspricht nicht den aktuellen Standards für feste Installationen, er ist weder professionell noch Jahrzehnte zukunftstauglich. Er ist ein Kompromiss.

Falls Sie Wohneigentum besitzen, für das Sie zeitnah eine Renovierung planen, ist unser Vorschlag nichts für Sie. Investieren Sie in diesem Fall besser in eine professionelle Netzwerkverteilung mit Twisted-Pair-Installationskabel der Kategorie 8. Zwar kostet allein das Kabel rund einen Euro pro Meter, es eignet sich aber für 10 GBit/s und auf kürzeren Strecken sogar für 25 Gbit/s. Wir verwenden dieses Kabel in diesem Artikel nicht, weil es aufgrund von Dicke und Starrheit kaum für die engen Kabelkanäle geeignet ist und auch zu teuer für eine Interimslösung.

Die im Weiteren empfohlenen Cat-5e-Kabel liefern bis 90 Meter Länge mindestens Gigabit-Ethernet-Geschwindigkeit und auf Strecken unter 50 Metern je nach Signalgüte 2,5, 5 oder sogar 10 Gigabit pro Sekunde. Wir haben ein Vierer-Bündel aus ungeschirmtem Kategorie-5e-Patchkabel über 25 Meter getestet: Zwei 5-Gigabit- und zwei Gigabit-Verbindungen liefern anstandslos gleichzeitig, ohne sich gegenseitig zu stören. Verlassen Sie sich dennoch nicht darauf, denn äußere Störeinflüsse können einen Strich durch die Multigigabit-Rechnung machen.



**Es muss nicht immer das teure und starre Verlegekabel sein. Auch dünne Patchkabel eignen sich für Gigabit-Ethernet und Festinstallationen. Sie sind günstig und flexibel und die Montage erfordert nur wenig Werkzeug.**

## Planung

Um Einkauf und Installation optimal zu planen, sollten Sie zunächst den Montageort der Netzwerkzentrale festlegen – also den Ort, wo die Kabel aller Dosen zusammenlaufen und Sie einen Netzwerkverteiler (Switch) montieren. Dort, wo die Installation startet, muss nicht zwangsläufig auch der Router stehen, mindestens aber eine Steckdose für den Switch in Reichweite sein.

Bei der Dosenplanung gilt: so viele wie nötig, so wenig wie möglich; einen weiteren, notfalls in einem fernen Zimmer abgesetzten Switch können Sie jederzeit nachrüsten. Auch wenn das Kabel aufgrund fehlender Schirmung und dünner Leiter nur leicht aufträgt, ist der Platz in Kabelkanal-Sockelleisten begrenzt und je länger viele ungeschirmte Kabel nebeneinander laufen, desto wahrscheinlicher wird, dass sie sich gegenseitig stören. In unseren Versuchen passten etwa sechs bis acht Kabel nebeneinander. Beachten Sie, dass die maximale Leitungslänge für Twisted-Pair-Kabel etwa 100 Meter beträgt. Wir haben das günstige Kabel allerdings nur bis etwa 60 Meter Länge geprüft; das sollte selbst für die größte Wohnung ausreichen.

Sind die Installationsorte festgelegt, ermitteln Sie die erforderliche Länge der Sockelleisten und die Anzahl der Außen- und Innenecken sowie der Kabelauslässe. Dann bestimmen Sie die Längen der Netzwerkkabel vom Anfang der Verteilung zu den einzelnen Dosen. Rechnen Sie die Wände ein, die per Bohrung durchquert werden müssen. Runden Sie für Reservezwecke großzügig auf ganze Meter auf.

Müssen Sie für die Verkabelung Löcher in Wände bohren, die nicht Ihnen gehören, etwa in Mietwohnungen, sprechen Sie vorab mit Ihrem Vermieter. Solange Sie keinen neuen Türdurchbruch machen und es vertraglich nicht anders vereinbart ist, dürfen Sie Löcher zwar ohne gesonderte Erlaubnis fachgerecht bohren. Allerdings kann der Vermieter oft wichtige Informationen beitragen und so verhindern, dass Ihr Schlagbohrer Bekanntschaft mit einem Stahlträger, einem Kabel oder einer Wasserleitung macht.

Eine Planungsvorlage im Markdown-Format für alle Schritte finden Sie über ct.de/wq9s. Markdown-Tipps für Einsteiger sind auch dabei.

**Mit Gehäusen für Keystone-Einsätze bauen Sie kleine Netzwerkverteilungen dezent und unkompliziert auf. Im Gehäuse werden die Kabel in RJ45-Einsätzen aufgelegt und von dort über kurze Patchkabel mit einem Netzwerkverteiler (Switch) verbunden.**

## Werkzeuge

Neben einer Schlagbohrmaschine mit zur Wandstärke und dem Kabeldurchmesser passenden Bohrern sollten Sie auch ein Ortungsgerät zur Hand haben, um etwaige vergessene oder nicht dokumentierte Elektroleitungen und metallische Hindernisse aufzufinden.

Mit einem Gliedermaßstab alias Zollstock stellen Sie sicher, dass Sie in passender Höhe durch die Wand bohren.

Um Sockelleisten auf Länge zu bringen, genügt eine kleine Handsäge. Ein Akkuschrauber hilft, die Leisten handgelenkschonend an die Wand zu schrauben.

Einen Permanentmarker (Filzstift) benötigen Sie, um die einzelnen Kabel an beiden Enden mit Ringen zu kennzeichnen, damit Sie später beim Auflegen nicht raten müssen, welche Leitung auf welcher Dose endet.

Werkzeuge auszuleihen beziehungsweise zu mieten, spart gegenüber dem Kauf viel Geld. Nicht nur Familie und Freunde sind dafür praktisch, auch viele Baumärkte und private Anbieter auf Kleinanzeigenportalen helfen kostengünstig.

Ein Netzwerk-Werkzeugset und einen kleinen Seitenschneider sollten Sie hingegen besitzen; einfache Sets gibt es ab etwa 25 Euro. Damit lässt sich auch ein defekter Anschluss reparieren. Typischen Netzwerksets liegt außerdem ein RJ45-Durchgangsprüfer bei, der schnell verrät, ob die Kabel richtig aufgelegt sind. Da beidseitig Buchsen installiert

sind, benötigen Sie zum Prüfen auch zwei kurze Patchkabel.

Über ct.de/wq9s finden Sie für bereits genannte und alle folgenden Komponenten Quellenvorschläge.

## Einkauf

Bevor Sie den Austausch planen, sollten Sie die bereits installierten Sockelleisten auf Eignung prüfen. Für neue Sockelleisten mit Kabelkanal müssen Sie je nach Qualität und Material 3 bis 10 Euro pro Meter veranschlagen. Innen- und Außenecken, Verbinder, Endstücke und Kabelauslässe kosten etwa 2 bis 6 Euro pro Stück.

Ungeschirmtes Netzwerkkabel der Kategorie 5e bekommen Sie etwa von Logilink oder Goobay für 15 bis 20 Cent pro Meter. Die Kabelvariante heißt U/UTP (Unshielded/Unshielded Twisted Pair). Um Störungen durch Übersprechen zwischen mehreren Kabeln zu vermeiden, ist der Typ „Screened Foiled Unshielded Twisted Pair“ (SF/UTP) empfehlenswert, also Kabel ohne Aderpaarschirme, aber mit äußerem Geflecht- und Folienschirm. Das kostet dann 20 bis 30 Cent pro Meter.

Achten Sie darauf, nur Patchleitung ohne Stecker zu kaufen, also kein Verlegekabel mit starren Adern. Letztere erschweren das Verlegen im engen Kabelkanal erheblich und sind teurer. Manch einer mag behaupten, dass Patchkabel sich nicht für Dosen eignen, doch das geht – wie, erklären wir weiter unten. Nehmen Sie aber keinesfalls Flachbandkabel, um fürs Verlegen die Stecker abzutrennen: Deren Adern sind für die Dosen schlicht zu dünn.

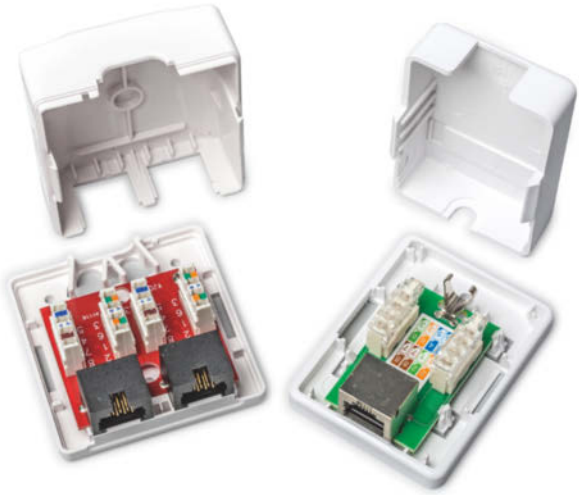
Netzwerkverteilungen beginnen typischerweise in einem 10- oder 19-Zoll-Patchfeld, einem passiven Bauteil mit vielen RJ45-Buchsen und Klemmstellen für die Kabel. Weil Modelle für Firmennetze vergleichsweise teuer und unschön sind, nutzen wir stattdessen Keystone-Gehäuse aus weißem Kunststoff, die man mit vier bis zwölf Ports für 5 bis 15 Euro bekommt. Keystone ist ein standardisiertes Steckplatzformat für allerhand Einsätze, alias Jacks, darunter auch RJ45 für Netzwerkverkabelungen. Damit die Installation günstig bleibt, nutzen wir Jacks aus Plastik für 1 bis 2 Euro pro Stück; robustere Ausführungen mit Metallgehäuse kosten 4 bis 10 Euro.

Netzwerkdosen gibt es in unterschiedlichen Qualitäts- und Preisklassen: Besonders günstig kann man sich etwa bei deleyCon und Delock bedienen, die Aufputzdosen mit einem oder zwei Ports ab etwa 4 beziehungsweise 7 Euro bieten. Allerdings zeigt die Buchse bei diesen Dosen nach oben, was unhandlich und optisch unbefriedigend sein kann. Typische Netzwerkdosen mit kabelschonend nach unten herausgeführten Buchsen kosten 8 bis 15 Euro. Unter ct.de/wq9s finden Sie Links zu passenden Angeboten.

Je nach Lieferumfang benötigen Sie zusätzlich Schrauben und Dübel aus dem Baumarkt, um Netzwerkdosen, Sockelleisten und Keystone-Gehäuse an der Wand zu montieren. Aus leidiger Erfahrung raten wir davon ab, die Dosen mit Klebepads an der Tapete zu fixieren: Sie fallen entweder nach kurzer Zeit ab oder nehmen bei der Demontage die halbe Wand mit.

Um die Netzwerkkabel gebündelt durch Löcher in der Wand zu führen beziehungsweise am Bohrer hindurchzuziehen, behelfen Sie sich mit etwas Isolierband. Außerdem benötigen Sie kleine Kabelbinder zur Zugentlastung der Netzwerkleitungen im Keystone-Gehäuse. Beides gibts im Baumarkt.

Außerdem brauchen Sie einen Gigabit-Ethernet-Switch sowie kurze Patchkabel für die Verbindung vom Keystone-Gehäuse zum Switch.



**Netzwerkdosen bekommt man für wenige Euro pro Stück. Sie nutzen die gleichen Klemmstellen wie RJ45-Jacks oder Patchfelder, sodass das Auflegen des Kabels unkompliziert ist.**

## Aufgelegt und eingepresst

Haben Sie noch nie Netzwerkkabel aufgelegt, also das Kabel mit Dosen, Jacks oder Patchfeldern verbunden, mag die Sache auf den ersten Blick kompliziert erscheinen, ist sie aber nicht. Moderne Netzwerkbuchsen – und alles, was Sie in der Liste unter ct.de/wq9s finden – nutzen Schneidklemmen, um

die acht Adern eines Netzwerkkabels mit der Buchse zu verbinden. Eine Schneidklemme besteht aus zwei gegenüberstehenden Messern, die die Isolation der Ader beim Einpressen anschneiden und so den elektrischen Kontakt herstellen. Sie müssen also nur den äußeren Mantel und die Schirmung des Kabels entfernen, um es verbinden zu können (LSA, löt-, schraub- und abisolierfreie Technik).

Besitzt das Bauteil keine integrierte Presshilfe, braucht es Werkzeug. In einem Netzwerkerset gibt es typischerweise zwei Optionen: Eine LSA-Zange, die die Ader in einem Rutsch einpresst und den Überstand abschneidet oder ein kleines gelbes oder blaues Auflegewerkzeug (siehe Bild) mit integriertem Kabelmesser zum Entfernen der Isolierung. Das Auflegewerkzeug ist die richtige Wahl, um Patchkabel in Jacks und Dosen aufzulegen, denn die hintere Anpressfläche der LSA-Zange beschädigt oder zerstört die feinen Kabel meistens. Mit dem Auflegewerkzeug kann man sie hingegen mit Fingerspitzengefühl zwischen die Messer drücken. Den Überstand entfernen Sie mit einem Seitenschneider.

**Mit dem Auflegewerkzeug drückt man die Adern mit Fingerspitzengefühl in die Schneidklemmen. Der Jack links besitzt dafür eine eigene Presse. Farbkennungen an Netzwerkbauteilen erleichtern die korrekte Belegung.**

Damit die Daten flutschen, müssen Sie die Schneidklemmen beidseitig mit den richtigen Adern belegen und dafür gibts zwei Standards: TIA-568A und TIA-568B. Diese legen farblich fest, welche Ader auf welchem Pin im RJ45-Anschluss landet. Das klappt, weil auch die Farben der vier Adernpaare im Netzwerkkabel genormt sind: Grün, Orange, Blau und Braun sowie deren weiß-gestreifte Partner. In manchen Kabeln sind die Partneradern einfach weiß, sodass man darauf achten muss, mit welcher gefärbten Ader sie verdrillt sind, um sie richtig aufzulegen.

Die leicht unterschiedlichen 568er-Standards haben weder Vor- noch Nachteile, sie sind schlicht historisch gewachsen. Auf aktuellen Netzwerkbauteilen finden Sie die Belegungen für beide Varianten. Sie suchen sich also Version A oder B aus und tun sich und möglichen Folgenutzern den Gefallen, das mit einem Permanentmarker auf die Innenseite des Keystone-Gehäuses zu schreiben. Das macht klar, dass der Erbauer nicht von Dose zu Dose neu gewürfelt hat und erleichtert das Warten und Ersetzen einzelner Komponenten.

## Durchgestromt

Haben Sie Gehäuse und Dosen an die Wand geschraubt und die Kabel verlegt, beginnen Sie mit dem Verbinden. Das Einstecken der Keystone-Jacks ist etwas fummelig: Die Klemmstellen gehören nach oben. Zuerst haken Sie die obere kleine Nase oben im Rahmen unter, dann drücken Sie die untere über die Schwelle bis zum Rastpunkt.

Um das Kabel abzuisolieren, nehmen Sie das kleine Auflegewerkzeug, spannen die Leitung in die erste Mulde am Kabelmesser ein und drehen eine Runde. Das genügt in der Regel, damit Sie die Hülle leicht abziehen können.

Die Installation der Jacks und Dosen variiert von Modell zu Modell etwas. Die Anleitung hilft im Zweifelsfall weiter. Wichtig ist nur, dass Sie für jedes Kabel beidseitig etwas Reserve im Kabelkanal verstauen und nicht gleich alles verschließen, wenn die Adern farblich korrekt eingepresst sind. Außerdem sollten Sie beim Einpressen nur wenig mehr Druck benötigen als zum Öffnen eines Kugelschreibers. Wehrt sich die Schneidklemme, haben Sie wahrscheinlich die Nut des Werkzeugs nicht genau darüber positioniert. Obacht, auch wenn Sie nur eine Klemme beschädigen,

müssen Sie das Bauteil komplett ersetzen; Gigabit-Ethernet benötigt alle acht Adern.

Nutzen Sie nach jedem neu aufgelegten Kabel den Durchgangsprüfer, um zu testen, ob alles korrekt verknüpft ist. In den meisten Fällen schneiden die Schneidklemmen die Adern richtig an, aber falls das mal nicht klappt, erkennen Sie es an der dunkel bleibenden Leuchte am Prüfgerät.

Blinkt alles akkurat, entfernen Sie das Prüfgerät und verbinden den frischen Port am Keystone-Gehäuse mit einem Switch. An der Dose testen Sie zum Beispiel mit einem Laptop, ob eine Gigabit-Verbindung zustande kommt. Wenn nicht, schauen Sie sich beidseitig die Schneidklemmen an und drücken erneut mit dem Auflegewerkzeug hinein. Hilft das nicht, ziehen Sie alle Adern aus den Schneidklemmen und beginnen von vorne.

Steht die Gigabit-Verbindung, schneiden Sie den Überstand mit dem Seitenschneider ab und installieren die Zugentlastung, also den Kabelbinder oder die mechanische Klemme, die das Kabel vor dem Herausgezogenwerden schützt.


**Nahezu allen günstigen Netzwerksets liegt ein einfacher Durchgangsprüfer bei. Der aktive Teil (links) wird auf der einen Seite einer Kabelverbindung angeschlossen, der passive auf der anderen Seite. Blinkt Letzterer ununterbrochen und der Reihe nach von 1 bis 8 lückenlos durch, ist das Kabel korrekt aufgelegt.**

## Repeater, werd' Access Point!

Mit Ihrer neuen Gigabit-Netzwerkverkabelung beschleunigen Sie nun das Funknetz: Besitzen Ihre WLAN-Repeater oder Mesh-Knoten eine Netzwerkbuchse, verbinden Sie die Geräte mit einer Dose und bringen Sie in den Access-Point-Modus; die jeweilige Anleitung verrät, wie das geht. Im Access-Point-Modus schickt das WLAN-Modul die Daten der Mobilgeräte nach Ankunft aus der Luft per Kabel durchs Heimnetz, und umgekehrt. Dadurch steigt auch die Gesamtbandbreite an allen WLAN-Zugangspunkten, weil diese sich nicht mehr einen Kanal teilen müssen.

Langfristig dürfen Sie sich auch bei neueren WLAN-Standards günstigerer Angebote bedienen, denn auf teure Mesh-Sets mit zusätzlichen, energiefressenden Backbone-Funkmodulen können Sie dank Ihrer Verkabelung verzichten. Trotz der günstigen Komponenten wird sie noch einige Zeit das robustere und schnellere Medium bleiben. (amo) c't

**Planungspad und Einkaufsempfehlungen**
ct.de/wq9s

# Koax-Switch

**Der Datenverteiler G4204C bindet bis zu vier Geräte per TV-Kabel gigabitschnell ins Netz ein.**

Von **Ernst Ahlers**


Wer sein Netz mit einem G.hn-Wave-2-Adapter beim Router ins TV-Kabel speist, kann den Internetzugang darüber an bis zu 15 andere Adapter im Haus weiterleiten (c't 2/2022, S. 98). Der G4204C mit integriertem Ethernet-Switch holt die Daten aus dem Koaxkabel und gibt sie über vier Gigabit-Ports weiter, beispielsweise im Wohnzimmer an Smart-TV, Set-Top-Box oder Surround-System.

Das Gerät lieferte im Test bis zu mittleren Dämpfungsgraden vollen Gigabit-Ethernet-Durchsatz übers Koax (siehe Tabelle). IPv6 und Multicast-IPTV (beispielsweise Telekom MagentaTV) funktionierten problemlos, getaggte VLANs für Mehrzonennetze gab der Adapter unverfälscht weiter, das alles bei niedrigem Energiebedarf. Wer mehrere Geräte an einem Ort übers Koax ans Netz binden muss, tut mit dem G4204C keinen Fehlgriff. (ea) c't

## Giga Copper G4204C

| Ethernet-over-Coax-Switch | |
|---|---|
| Hersteller, URL | GIGA Copper Networks, www.gigacopper.net |
| Bedienelemente | Ein, Reset, 6 Statusleuchten |
| Anschlüsse | F-Buchse (EoC nach G.hn Wave 2), 4 × RJ45 (Gigabit-Ethernet) |
| Getestete Firmware | 7_10_r713+4 |
| Durchsatz über 50 m Koax plus 30 / 40 / 50 / 60 dB | 942 / 936 / 846 / 474 Mbit/s |
| VLANs / IPv6 / Multicast | ✓ / ✓ / ✓ |
| Leistungsaufnahme[1] | 2,6 / 3,7 Watt (5,1 / 6,9 VA) |
| Jährliche Stromkosten[1] | 9 / 13 € |
| Preis | 150 € |

[1] idle, mit 1 / 4 GE-Links, bei Dauerbetrieb und 40 Cent/kWh

# Koax-Express

**Der Ethernet-over-Coax-Adapter MA2500D soll Daten besonders flink durchs TV-Kabel schleusen. Manchmal holpert es aber.**

Von **Ernst Ahlers**


Die mit der MoCA-2.5-Technik arbeitenden Adapter MA2500D transportierten im Kurztest mehr als 2 Gbit/s übers TV-Koaxkabel. Bei langen Koaxstrecken mit hoher Dämpfung bricht die Geschwindigkeit wie erwartet ein.

Die Adapter übertragen Daten ab Werk chiffriert; ein eigener Schlüssel lässt sich per Browser setzen. Mit Sat-TV über DVB-S im selben Kabel vertragen sich die Adapter nicht. VLANs für Multizonen-Netze reichten sie unverfälscht weiter, IPv6 funktionierte auch. Nur bei Multicast-IPTV (beispielsweise Magenta TV der Telekom) sahen wir immer wieder Ruckler. Wer das nicht nutzt, bekommt schnelle EoC-Adapter zu einem günstigen Preis. (ea) c't

## goCoax MA2500D

| Ethernet-over-Coax-Adapter | |
|---|---|
| Hersteller, URL | goCoax, gocoax.com |
| Bedienelemente | Koppeltaster, Reset, 4 Statusleuchten |
| Anschlüsse | F-Buchse, 1 × RJ45 (Multigigabit-Ethernet bis 2,5 Gbit/s) |
| getestete Firmware | 2.0.8.0 |
| Durchsatz über 50 m Koax plus 30 / 40 / 50 / 60 dB | 2,3 / 1,9 / 0,9 / – Gbit/s |
| VLANs / IPv6 / Multicast | ✓ / ✓ / (✓)[2] |
| Leistungsaufnahme Idle | 2,8 Watt (5,2 VA) |
| jährliche Stromkosten[1] | 10 € (pro Stück) |
| Preis | 80 € (pro Stück) |

[1] idle, mit 2,5-Gbit/s-Link, bei Dauerbetrieb und 40 Cent/kWh [2] deutliche Ruckler in Multicast-IPTV-Streams

# Heimnetz per Telefondraht


**G.hn-Adapter schicken gigabitschnell Daten über Telefon- oder Koaxleitungen, wenn man kein LAN-Kabel legen will. Das geht über eine Telefonleitung auch mit mehr als zwei Geräten.**

Von **Ernst Ahlers**

Gigacopper Networks bietet Adapter an, die nach dem G.hn-Standard (ITU-T G.9960) Daten über Telefon- oder TV-Koaxkabel transportieren. Darüber kann man das Internet in weit vom Router entfernt liegende Räume bringen, ohne LAN-Kabel ziehen zu müssen.

Mit der „InHome"-Firmware des Chipherstellers MaxLinear – auch in Devolos Giga Bridge – können nun bis zu 16 Geräte an einem Kabel ein Netz aufbauen (Bus-Topologie).

Das haben wir mit drei Gigacopper-Adaptern an unterschiedlich langen, zusammengesteckten Telefonkabelstücken ausprobiert. Dank beiliegender Adapterstecker kann man sie an den meisten Haustelefonleitungen direkt einsetzen. Die G.hn-Adapter funktionierten bei uns aus dem Karton – anschließen, einschalten, Daten fließen.

Das Modell G4201TM (im Bild oben) hat nur einen Gigabit-Ethernet-Port, kann ihn aber als VLAN-Trunk-Port nutzen. Die Variante G4202T bedient über zwei GE-Ports mehrere Clients. Sie kann zwar selbst kein VLAN-Tagging, reicht VLAN-gekennzeichnete Pakete aber durch und kann das Telefonleitungssignal durchschleifen.

Multicast-Verkehr (IPv6-Steuerpakete, Live-IPTV wie Telekom MagentaTV) leiteten die Geräte fehlerfrei weiter. Wer an QoS-Einstellungen – ab Werk DSCP – feilen möchte, kommt per Browser auf die Konfigurationsseiten.

Im Paarbetrieb schafften die Adapter bis 80 Meter Leitungslänge vollen Gigabit-Ethernet-Durchsatz (940 Mbit/s). Darüber ging die Nettogeschwindigkeit etwas zurück (siehe Tabelle).

Mit drei Adaptern, die gleichzeitig Daten übertrugen, hing die Summengeschwindigkeit davon ab, wie sie angeordnet waren: Mit der Quelle (simulierter Router) in der Mitte gingen bei 60 und 100 Meter Gesamtlänge 940 Mbit/s durch.

Lag die Quelle am Leitungsanfang, dann transportierte das System bei 60 Metern ebenfalls 940 Mbit/s in Summe, über 100 Meter Gesamtlänge mit 704 Mbit/s aber etwas weniger. Dabei bekam die Senke bei 50 Metern erwartungsgemäß mit etwas über 500 Mbit/s den Löwenanteil und die weiter entfernte mit knapp 200 Mbit/s deutlich weniger Durchsatz ab.

Die Bequemlichkeit, keine LAN-Kabel legen zu müssen, bezahlt man über die Stromrechnung: Die Adapter zogen im Idle-Betrieb (kein Traffic, ein GE-Port belegt) 2,5 und 2,9 Watt aus der Steckdose. Das ist für ihre Leistung angemessen, aber auch kein Pappenstiel. Wer schnelles Internet über seine hausinternen Telefonkabel weiterleiten will, darf 130 beziehungsweise 135 Euro pro Adapter reuelos investieren. (ea) c't

## Gigacopper G4201TM+G4202T

| Adapter für Ethernet über Telefonleitungen | |
|---|---|
| Hersteller, URL | Gigacopper Networks, gigacopper.net |
| Bedienelemente | G4201TM: Reset, 3 Leuchten; G4202TM: Reset, 3+2×2 Leuchten |
| Anschlüsse | G4201TM: 1 × RJ12 (Tel.ltg.), 1 × RJ45 (Gigabit-Ethernet); G4202T: 2 × RJ45 (Tel.ltg.), 2 × RJ45 (Gigabit-Ethernet) |
| getestete Firmware | Spirit v7_8_r619+33_cvs |
| Durchsatz über 80 / 100 / 120 m Telefonleitung | 940 / 850 / 740 Mbit/s |
| VLANs / IPv6 /Multicast | ✓ / ✓ / ✓ |
| Leistungsaufnahme (idle) | G4201TM: 2,9 Watt (5,7 VA); G4202T: 2,5 Watt (5,0 VA) |
| jährliche Stromkosten | 28 € (3er-Set, Dauerbetrieb, 40 ct/kWh) |
| Preis | 400 € (3er-Set wie gezeigt) |

# Tipps & Tricks

**Wo stellt man Fritzboxen am besten auf, um mehrstöckige Gebäude abzudecken, wieviele entfernte Fritzboxen kann man per VPN miteinander koppeln, wie verhindert man Aussetzer bei Videokonferenzen? In dieser Übersicht finden Sie die Lösungen zu diesen und anderen Vernetzungsfragen.**

Von **Dušan Živadinović**

## Zwei Fritzboxen für Keller und Büro?

**? Ich habe eine Fritzbox 7590 und eine 7590AX. Die eine soll im Keller den VDSL100-Anschluss herstellen, die andere das Homeoffice auf dem Dachboden mit WLAN versorgen. Eine LAN-Verbindung zwischen beiden Orten gibt es, aber welche Box sollte wo stehen? Ich tendiere dazu, die 7590AX als schnelleres Modell direkt an den Internetanschluss zu setzen.**

! Welche Box Sie als DSL-Router und Mesh-Master einsetzen und welche zum Mesh-Repeater wird, ist prinzipiell einerlei. Wenn Sie im Dachgeschoss auf die DECT-Schnurlostelefonie der Fritzbox verzichten können, scheint Folgendes sinnvoll: Die 7590AX kommt in den Keller. Fürs Dachgeschoss beschaffen Sie sich einen Fritz-Repeater 1200AX. Der zieht mit 4,1 Watt idle (14,40 Euro/Jahr bei 40 Cent/kWh) um einiges weniger Leistung aus der Steckdose als die 7590 im Mesh-Repeater-Betrieb (7,8 Watt, 27,30 Euro/Jahr). Die 7590 verkaufen Sie und sollten damit die Ausgabe für den Repeater zumindest zum Teil wieder drin haben. Die jährlich gesparten 13 Euro Stromkosten zahlen den Rest ab. (ea@ct.de)

## Fritzbox im 19-Zoll-Rack

**? Meine Fritzbox steht im Keller, wo sich auch die übrigen Netzwerkkomponenten in einem Standard-Netzwerkschrank befinden. WLAN ist ausgeschaltet, das läuft über Access-Points in den Stockwerken. Leider bekomme ich das stylische Plastikgehäuse der Fritzbox nicht sinnvoll in den Schrank integriert – eine 19-Zoll-Fritzbox gibt es ja nicht. Kennen Sie eine Lösung?**

! Es werden durchaus diverse Rackgehäuse für den Einbau einer Fritzbox angeboten, wenngleich auch nicht gerade günstig. Eine Auswahl finden Sie über ct.de/w38c.

Günstiger, wenn auch nicht so hübsch, wäre ein schlichter 19-Zoll-Boden, auf den Sie den Router einfach draufstellen. (ea@ct.de)

## FTTB: Koaxkabel ab Verteiler nutzen

**? Ich habe einen Glasfaseranschluss im Keller (Fiber to the Building). Kann ich die Koaxleitung vom Kabelnetzwerk trennen und dieses dann für die Weiterleitung des Glasfaseranschlusses über einen Konverter nutzen?**

! Technisch funktioniert das, falls vom Sternpunkt im Keller eine Koaxleitung direkt in Ihre Wohnung läuft. Etagenverteiler und dergleichen darf es dazwischen jedoch nicht geben. Dann können Sie prinzipiell Ihre Leitung unten vom Einspeiseverstärker lösen lassen.

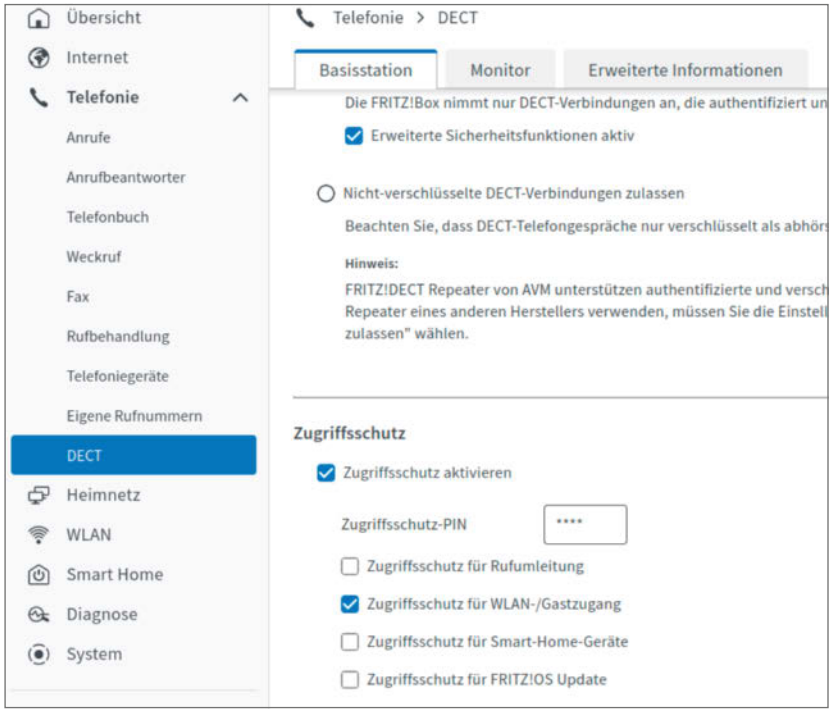
Der sitzt üblicherweise in einem abgeschlossenen und verplombten Schaltkasten, weswegen das vom Provider beauftragtes Fachpersonal erledigen muss. Sie müssen ferner klären, wem die Leitung gehört: In älteren Bauten hat typischerweise ein vom Provider beauftragter Dienstleister nachträglich das Koax-Verteilsystem installiert, womit es dem Provider gehört. Der müsste Ihnen die ander-

weitige Verwendung gestatten. Das würde entfallen, falls die TV-Koaxverteilung zum Gebäude gehört, weil sie schon bei dessen Bau errichtet wurde. (ea@ct.de)

## WLAN-Anzeige in Fritz-Fons unterbinden

**Nachdem ich meine Fritzbox 7590 auf FritzOS 7.50 upgedatet habe, hat das Schnurlostelefon Fritz-Fon C6 die Firmware-Version 4.89 bekommen. Seitdem zeigt es die WLAN-Zugangsdaten im Klartext und als QR-Code an, was für mich eine extreme Sicherheitslücke darstellt: Bei solchen „Komfortfunktionen" sind sichere Passwörter zwecklos. Wie kann ich die WLAN-Anzeige ausschalten?**

Die WLAN-Anzeige in den Fritz-Fons lässt sich zwar nicht abschalten, aber immerhin mit einer PIN schützen. Gehen Sie per Browser ins Fritzbox-Menü und rufen dort den Punkt Telefonie/DECT auf.




**Die Anzeige der WLAN-Zugangsdaten am Fritz-Fon lässt sich im Menü der Fritzbox unterbinden.**

Im ersten Reiter „Basisstation" steckt weiter unten der „Zugriffsschutz". Aktivieren Sie ihn, tragen Sie eine PIN ein und setzen Sie ein Häkchen vor „Zugriffsschutz für WLAN-/Gastzugang". Anschließend ist die Anzeige der WLAN-Daten auf allen verbundenen Fritz-Fons mit der PIN verriegelt. (ea@ct.de)

## Neue WLAN-Kanäle

**Mir ist aufgefallen, dass mir mein WLAN-Access-Point für das 5-GHz-Band auch die Kanäle von 149 bis 161 und von 165 bis 173 anbietet. Ich hatte vor einiger Zeit noch gelesen, dass diese Kanäle in Deutschland nicht genutzt werden dürfen. Hat sich daran etwas geändert?**

Ja, diese Kanäle sind tatsächlich für WLAN nutzbar. Dabei muss man jedoch einiges beachten: Der Bereich ist nicht Teil der Allgemeinzuteilung der WLAN-Frequenzen im 5-GHz-Band, die bis 5,725 GHz geht. Die Kanäle werden über die Allgemeinzuteilung für Funkanwendungen mit geringer Reichweite freigegeben, die von 5,725 GHz bis 5,875 GHz reicht und – wie die meisten in der EU harmonisierten Frequenzzuteilungen – technologieneutral ausgelegt ist. Der große Nachteil: Die Sendeleistung darf maximal 25 Milliwatt (das sind 14 dBm) an der Antenne (EIRP) betragen. Das ist in diesem Frequenzbereich nicht viel; die WLAN-Allgemeinzuteilung sieht 200 (23 dBm) beziehungsweise 1000 mW (30 dBm) vor.

Diese Leistung kann genügen, um dünnere Wände ohne Metallbauteile zu durchdringen oder einen Garten auf Sicht mit flottem WLAN zu versorgen. Der Bereich hat dabei auch große Vorteile: Die Wetterradarerkennung, die von Kanal 50 bis 144 regelmäßig für nervige Abschaltungen sorgen kann, ist in der SRD-Allgemeinzuteilung (Short Range Device) nicht vorgeschrieben. Auch sonst gibt es abgesehen von der Sendeleistung keine Einschränkungen für den WLAN-Betrieb. Zudem nutzen viele WLAN-Router und Access Points die Kanäle nicht bei ihrer Autokanalsuche, sodass der Bereich auch in dicht besiedelter Nachbarschaft oft noch frei ist – ein Segen für alle, die aufgrund voller WLAN-Kanäle im Schneckentempo surfen.

Um den Frequenzbereich rechtssicher nutzen zu können, müssen Sie Ihrer WLAN-Basis das Betriebsland in den Einstellungen mitteilen. Meist heißt diese Einstellung einfach „Land", gelegentlich aber auch „Regulatory Domain". Das ist wichtig, da diese Kanäle in anderen Ländern mit mehr Sendeleistung genutzt werden dürfen. Anbieterrouter und auch

viele freie Modelle erledigen diese Konfiguration oft automatisch. Konfigurieren Sie Ihren Router falsch, haften Sie auch dafür. Wenn das der Hersteller tut, ist er dafür verantwortlich, dass die Grenzwerte eingehalten werden – außer Sie haben den Router aus dem Ausland in die EU importiert, dafür übernehmen wiederum Sie die Verantwortung (siehe auch ct.de/w38c). (amo@ct.de)

## Fritzbox: WireGuard-VPN Site-to-Site-Verbindungen

**? Ich überlege, WireGuard auf Fritzboxen für Site-to-Site-Verbindungen einzusetzen. Aber wie viele gleichzeitige Site-to-Site-Verbindungen sind dabei möglich?**

! AVM hat dazu bisher keine öffentliche Angabe gemacht, weshalb wir direkt beim Hersteller nachgefragt haben. Die gute Nachricht: Laut AVM gibt es keine feste Begrenzung bei der Anzahl der WireGuard-VPN-Tunnel.

Die maximale Anzahl hängt von dem eingesetzten Fritzbox-Modell, den Gegenstellen, den verwendeten Algorithmen, Einsatzszenarien, Verkehrsvolumen und weiteren gleichzeitigen Aktivitäten der jeweiligen Fritzbox ab. AVM empfiehlt, nicht mehr als 20 Tunnel gleichzeitig aufzubauen.

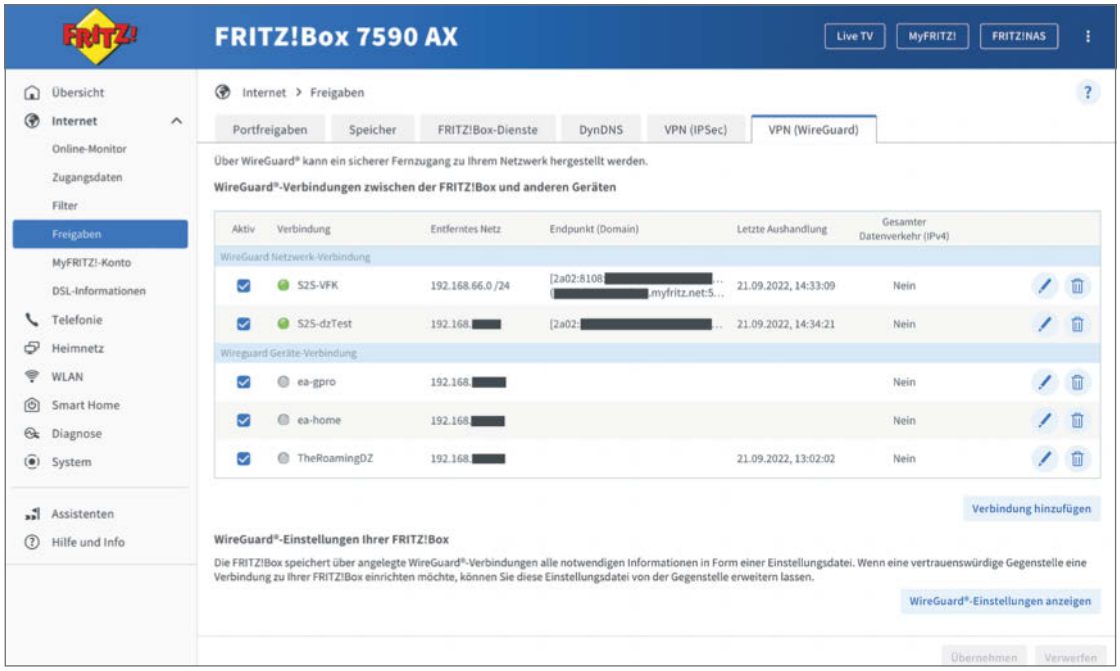
Wenn Sie also bis zu 20 Außenstellen an aktuellen Fritzboxen bedienen möchten, die aber jeweils die Datenrate nicht ausreizen, wäre WireGuard auf Fritzboxen mit aktuellem FritzOS mindestens einen Versuch wert. (dz@ct.de)

## WireGuard mit IPv4 und IPv6

**? Ich versuche zwei Fritzboxen per LAN-Kopplung über WireGuard zu verbinden. Eine Box nutzt einen IPv4-Zugang, die andere IPv6 mit DS-Lite. Beide sind an MyFritz angemeldet, aber die Kopplung funktioniert nicht.**

! Das ist normal, weil kein direkter Verbindungsweg zwischen IPv4-only und IPv6-via-DS-Lite existiert. Am besten wäre, wenn Ihr Provider für den Anschluss auch IPv6 aktivieren würde. Dann sollte es gehen, sobald Sie IPv6 in der Fritzbox aktivieren.

Alternativ kann man sich mit IPv6-Nachrüstungen in Eigenregie behelfen. Beispielsweise könnten Sie wie in c't 20/22 auf Seite 172 geschildert, einen Raspi verwenden, um einen IPv6-Tunnel an Ihrer




**Fritzboxen können ab FritzOS 7.50 VPN-Tunnel mittels der WireGuard-Technik aufbauen. Die konkrete Anzahl hängt vom Modell und von der Auslastung ab.**

IPv4-Fritzbox vorbei aufzubauen. Den IPv6-Tunnel könnten Sie dann nutzen, um mit einem Client an die entfernte Fritzbox anzukoppeln (Road-Warrior-Szenario). (ea@ct.de)

## WireGuard als Datenverschwender?

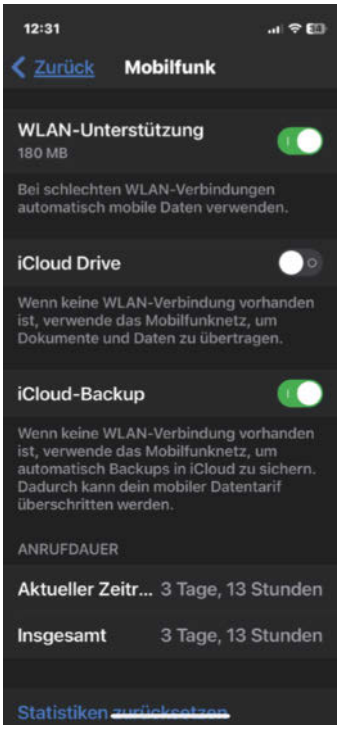
**? Ich habe einen Raspi als WireGuard-Server aufgesetzt und mein iPhone so konfiguriert, dass es automatisch auf VPN umstellt, sobald ich das Heimnetz verlasse. Prinzipiell funktioniert das. Allerdings steigt dadurch mein mobiles Datenvolumen massiv an. Allein die Hälfte des Traffics schreibt das iPhone der WireGuard App zu. Das verstehe ich nicht. Wenn es daran liegt, dass alles über WireGuard getunnelt wird, dann müssten es 100 Prozent sein. Wird nur ein Teil getunnelt? Dann funktioniert es nicht richtig. Oder verbraucht WireGuard das Volumen selbst? Das wäre heftig: Dann käme auf jedes getunnelte Bit ein Bit Overhead.**

! Das liegt vermutlich daran, dass im iPhone MultiPath-TCP für „alle möglichen Dienste“ aktiviert ist (standardmäßig nur für Siri): Wenn das iPhone im WLAN steckt, dort aber nur schwache Versorgung hat, nutzt es hilfsweise die Mobilfunkverbindung und wechselt je nach Bedarf fließend hin und her. Dann geht der Verkehr mal über den Tunnel, mal nicht. Weil auch WireGuard für nahtlosen Wechsel zwischen den Internet-Interfaces ausgelegt ist, merkt man unterm Strich nichts von den Vorgängen.

Das ist eigentlich nützlich, weil so beispielsweise Streamingdienste unterbrechungsfrei laufen. 50 Prozent Volumenverbrauch durch WireGuard ist dann nicht weiter verwunderlich, wenn das iPhone in der Hälfte der WLAN-Zeit Mobilfunk zu Hilfe nimmt.

Ob das tatsächlich durch MultiPath-TCP kommt, kann man leicht prüfen: Einstellungen/Mobilfunk öffnen und dann ganz nach unten scrollen, unter die Zeile der letzten iOS-App. Dort kann die Mobilfunknutzung als „WLAN-Unterstützung“, für „iCloud Drive“ und für „iCloud-Backup“ aktiviert sein. Um zu prüfen, ob der hohe Verbrauch an diesen Einstellungen liegt, einfach alle drei abschalten und am Ende des Abrechnungszeitraums vergleichen, ob der Verbrauch gesunken ist.

Das sollte normalerweise der Fall sein. Anschließend kann man die Optionen je nach Bedarf einschalten. Beispielsweise ist auf unseren Testgeräten in der Regel nur die WLAN-Unterstützung aktiv. (dz@ct.de)




**„WLAN-Unterstützung“ klingt harmlos, kann aber das verbrauchte Datenvolumen im Mobilfunknetz massiv erhöhen.**

## Fritzbox-Reset beschleunigt Zugriffe aufs Firmen-VPN

**? Sobald ich via VPN auf Büroanwendungen im Firmennetz zugreife, beträgt die Datenrate meines sonst normal funktionierenden DSL-50-Anschlusses nur noch maximal 12 MBit/s. Ein vergleichbarer Anschluss im Nachbarhaus funktioniert hingegen problemlos, am Firmennetz liegt es also nicht. Können Sie mir einen Tipp geben?**

! Solche Probleme treten manchmal bei unpassender Konfiguration des Routers auf, beispielsweise einer gegenüber der VPN-MTU (Maximum Transmission Unit, maximale Paketgröße im Virtual Private Network) zu klein eingestellten WAN-MTU (Wide Area Network, MTU am Internet-Port). Dann kommt es zu durchsatzsenkendem „Verschnitt“, weil

große VPN-Pakete in kleinere WAN-Pakete aufgeteilt werden müssen. Beim Test des Paketverlustes (Loss) mit wenigen Dutzend Byte kleinen ICMP-Paketen (Pings) fällt das naturgemäß nicht auf.

Fragen Sie Ihre Firmen-IT nach der dort konfigurierten VPN-MTU und setzen Sie diese probehalber in Ihrem VPN-Client etwas niedriger, beispielsweise 1420 statt 1450 Byte. Falls das schon Besserung bringt, lassen Sie die VPN-Client-Einstellungen so. Alternativ sichern Sie die Konfiguration Ihrer Fritzbox in eine Datei auf dem PC. Dann setzen Sie den Router versuchsweise auf Werkseinstellungen zurück und schauen Sie, wie sich das VPN dann verhält. Falls es jetzt den erwarteten Durchsatz liefert, holen Sie Ihre weiteren Fritzbox-Einstellungen wie den internen IPv4-Adressbereich, den Funknetznamen oder die Verschlüsselung von Hand nach. (ea@ct.de)

## Videokonferenzen ruckelfrei

**? Bei Videokonferenzen per Skype oder Zoom nerven immer wieder Ruckler und Tonausfälle. Woran liegt das und was könnte ich tun, um die Ursache zu beseitigen?**

! Übertragungsaussetzer sind immer Symptome für Stausituationen im Internet, wobei zeitkritische Anwendungen wie Videokonferenzen mehr Daten senden als Bandbreite zur Verfügung steht. Der Flaschenhals ist in der Regel die Senderichtung des Internetzugangs. Zum Beispiel können VDSL-Vectoring-Anschlüsse bis zu 250 Mbit/s empfangen (Downstream), aber nur bis zu 40 Mbit/s senden (Upstream). Dabei genügen 40 Mbit/s im besten Fall selbst für hochauflösendes Video. Doch wenn andere Anwendungen gleichzeitig senden (z. B. Mails oder Messengernachrichten mit großen Anhängen oder Cloudsynchronisierungen), bremsen sie sich gegenseitig.

Bessere Router enthalten Funktionen, um bestimmten Anwendungen oder auch Geräten Vorrang gegenüber anderen einzuräumen. Auf Fritzboxen gibt es grundsätzlich zwei Methoden: Einzelne Geräte gegenüber anderen bevorzugen, oder einzelne Anwendungen gegenüber anderen bevorzugen. Grundsätzlich muss die Fritzbox dafür entweder der alleinige Router in Ihrem Netz sein, oder als Mesh Master konfiguriert sein. Die Funktionen stehen nur für das Heimnetz, nicht aber für das Gastnetz zur Verfügung.

Um sie zu nutzen, öffnen Sie im Browser die URL „fritz.box“ und melden Sie sich an. Klicken Sie zunächst in der linken Spalte auf „Heimnetz/Netzwerk“ und dann auf den Bleistift neben dem Gerät, auf dem Skype läuft. Wenn Sie einen Haken bei „Dieses Gerät priorisieren“ setzen und mit „OK“ beenden, bevorzugt die Fritzbox alle Internet-Anwendungen, die auf dem betreffenden Gerät ausgeführt werden. Das kann nützlich sein, wenn man im Homeoffice immer denselben PC oder Laptop verwendet, um sich mit dem Firmennetz zu verbinden.

Alternativ kann man einzelnen Programmen wie Zoom, Netflix oder Spielen Vorrang einräumen. Deren Datenströme bevorzugt die Fritzbox dann grundsätzlich und unabhängig davon, von welchem Heimnetzgerät sie gesendet werden. Um den Skype-Verkehr zu bevorzugen, klicken Sie links im Menü auf „Internet/Filter/Listen/Netzwerkanwendungen“ und schließlich „Netzwerkanwendung hinzufügen“. Schreiben Sie dann „Skype“ in das Feld „Netzwerkanwendung“ und klicken auf „Neues Protokoll“. Wählen Sie „TCP“ und lassen Sie die Angabe der Ports auf „beliebig“; dieser Parameter ist bei Skype nicht fest, aber die Fritzbox erkennt die Skype-Kommunikation und findet den richtigen Port selbstständig. Übernehmen Sie die Einstellungen mit „OK“ und wiederholen Sie das Ganze für UDP. Viele andere Internetanwendungen verwenden feste Protokolle und Ports, was an vielen Stellen im Internet dokumentiert ist, zum Beispiel auf der Seite www.portforward.com.

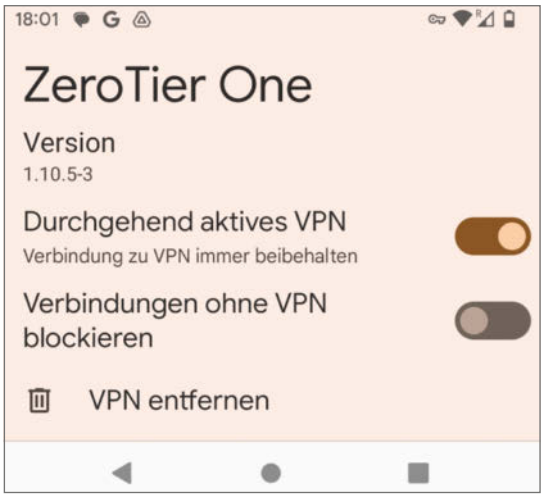
Zusätzlich kann man beide Regeln miteinander kombinieren, um einer bestimmten Anwendung nur auf einem bestimmten Gerät Vorrang einzuräumen. Klicken Sie dafür auf „Internet/Filter“ und dann auf „Priorisierung/Priorisierte Anwendungen/Neue Regel“. Wählen Sie dann Ihr Gerät und den von Ihnen erstellten Anwendungsfilter aus. (dz@ct.de)

## Instabiles VPN mit ZeroTier

! er Android-Client von ZeroTier One baut seit neuestem in der Grundkonfiguration keine zuverlässigen Tunnel auf. Die brechen immer mal wieder zusammen, obwohl das WLAN-Signal sehr gut ist, wenn man sich zum Beispiel vom Android abmeldet. Auch funktioniert der VPN-Zugriff über eine Mobilfunkverbindung nicht. Aber es gibt Abhilfe.

Suchen Sie die Android-Einstellungen Ihres Smartphones oder Tablets und öffnen „VPN“. Dort tippen Sie auf das Getrieberad neben ZeroTier und aktivieren dann den Schieber „Durchgehend aktives VPN“. Danach startet der ZeroTier-Client automatisch neu, wenn er sich mal verhaspelt hat. (dz@ct.de)

Wenn der ZeroTier-Client auf Android nur instabile VPN-Tunnel aufbaut, kann man sich mit der Einstellung „Durchgehend aktives VPN“ behelfen.

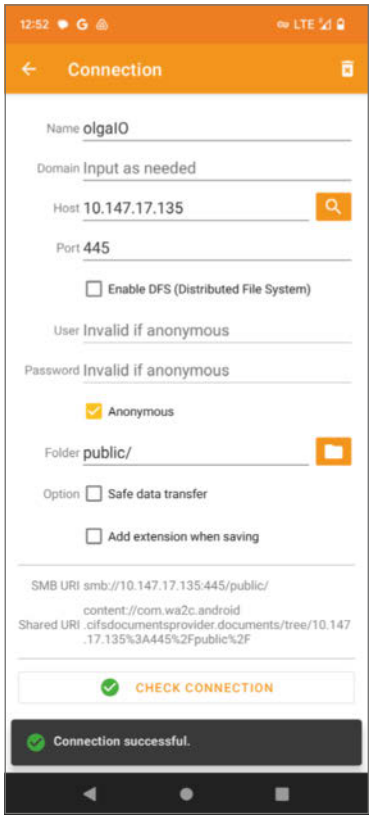



## ZeroTier mit Android

**? Ihre positiven Erfahrungen mit ZeroTier kann ich nur bestätigen. Ich nutze es auf Windows-PCs schon seit Langem, es funktioniert gut. Dank Ordnerfreigabe kann man damit auch über das Internet Datensicherung betreiben. Nur beim Übertragen von Dateien zwischen einem Windows-PC und einem Android-Smartphone komme ich nicht weiter. Ich habe auf Android die ZeroTier-App installiert und der ping-Befehl zeigt auch an, dass beide Geräte verbunden sind. Was fehlt mir denn jetzt noch?**

! Sie brauchen einen SMB-Client auf Ihrem Mobilgerät. Wenn der erst mal die Verbindung aufgebaut hat, können Sie damit von Android aus Dateien von und zu einer Windows-Freigabe kopieren.

In unseren Versuchen hinterließ der „CIFS Documents Provider“ den besten Eindruck. „Easy Smb“ (Im Play Store heißt diese App „SMB Client“; sie stammt von AppAzing.net.) hat aber auch funktioniert und sicherlich sollte es auch mit diversen anderen SMB-Clients klappen. (dz@ct.de)




**Mit dem CIFS Documents Provider übertragen Sie Dateien zwischen Ihrem Android-Gerät und einer Windows-Freigabe auch per ZeroTier-VPN.**

## Wake-on-Lan funktioniert nicht

**? Ich habe einen Windows-Rechner mit dem Mainboard GA-A320M-S2H von Gigabyte, bei dem es mir partout nicht gelingt, diesen übers Netzwerk aufzuwecken. In den Eigenschaften des Netzwerkadapters ist die Option „Gerät kann den Computer aus dem Ruhezustand aktivieren“ auch ausgegraut.**

! Probleme mit dem Standby-Zustand beziehungsweise mit dem Aufwecken sind meist schwer zu diagnostizieren. Zunächst sollten Sie mit dem Befehl `powercfg /DEVICEQUERY wake_programmable` auf der Kommandozeile prüfen, ob der Netzwerkadapter dort aufgeführt ist. Falls nicht, hilft ein Blick ins BIOS-Setup, ob dort die Energiesparfunktion ErP deaktiviert ist.

Bei manchen Mainboards liegt es aber auch schlicht an einem Firmware-Bug wie bei Ihrem Gigabyte GA-A320M-S2H. Dort funktioniert das Einschalten des Rechners per Netzwerk erst mit einer BIOS-Version ab Version F55. Dann lässt sich im Geräte-Manager von Windows in den Eigenschaften des Netzwerkadapters auch die vorher ausgegraute Option setzen. (chh@ct.de) (dz) c't

**Allgemeinzuteilungen für WLAN und SRD-Anwendungen**
ct.de/w38c

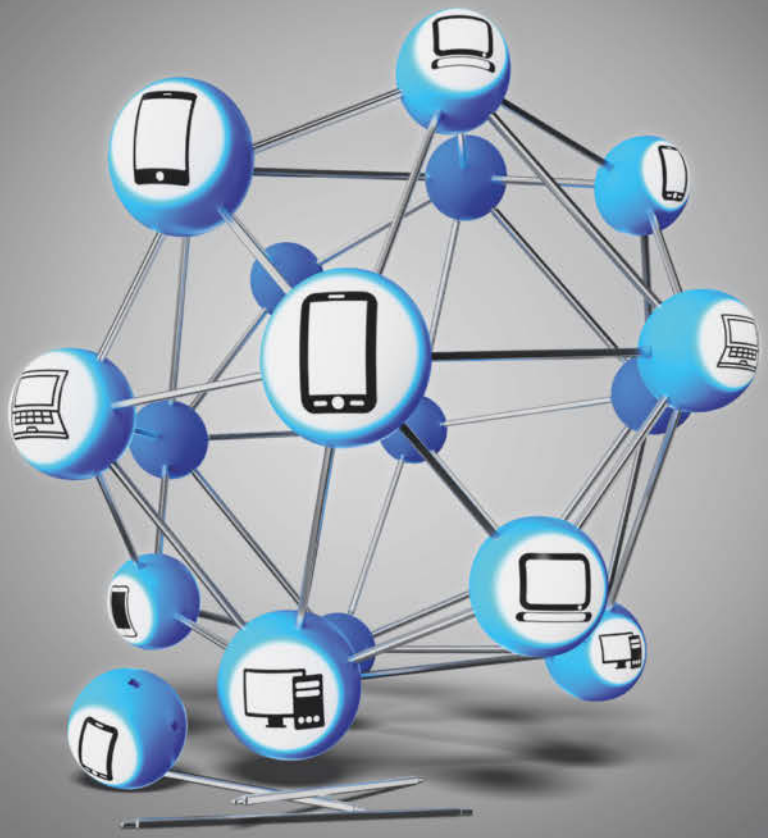
**Fritzbox-Einbaurahmen (Auswahl)**
ct.de/w38c

# VPN-Vernetzung mit Peer-to-Peer-Turbo

Bild: Andreas Martini

**Fortgeschrittene VPN-Anwendungen koppeln Geräte mit Direktverbindungen, sprechen kleine Arbeitsgruppen an und nehmen dem Admin viel Arbeit ab. Außerdem stellen wir ein mächtiges Werkzeug zur digitalen Selbstverteidigung auf Smartphones vor, das ebenfalls auf VPN gründet.**

Von **Dušan Živadinović**



Viele Anwendungen verwenden VPN-Techniken, aber teils für sehr unterschiedliche Zwecke. In der folgenden Artikelserie stellen wir sehr fortgeschrittene, aber zugleich sehr komfortable VPN-Anwendungen vor. An der Speerspitze der Entwicklung steht der Smartphone-Schutz Pretty Good Phone Privacy. Und wenn Sie entfernte Geräte miteinander koppeln wollen, sollten Sie Peer-to-Peer-VPNs kennen. Was sie leisten, stellen wir anhand von Nebula, Twingate, Tailscale und ZeroTier vor. Damit vernetzt man ferne Standorte und Geräte zum Beispiel für Freigaben und für die Fernwartung. Aber anders als bei herkömmlichen VPNs wie IPsec oder WireGuard steht dabei kein zentraler VPN-Server als Drehscheibe im Mittelpunkt. Dabei kommunizieren die Clients direkt miteinander, Peer-to-Peer.

Mit Pretty Good Phone Privacy zieht das US-Startup Invisv viel Aufmerksamkeit auf sich. Die Firma verspricht eine Tarnkappe für Smartphones, die sogar vor den Augen von Mobilfunknetzbetreibern schützt. Mehr dazu im Abschnitt „Spurlos funken“.

Die Peer-to-Peer-VPNs gehen auf gestiegene Schutzanforderungen und auf eine Modernisierung der Architektur zurück. In herkömmlichen VPNs bildet der Server den zentralen Umschlagpunkt und somit einen Engpass: Ein langsamer Internetanschluss des Servers bremst die Clients ebenso aus wie eine Serverüberlastung. Der Peer-to-Peer-Ansatz löst den Umschlagpunkt auf, Clients kommunizieren direkt miteinander. Zu dieser VPN-Klasse gehören etwa Tinc, yggdrasil und auch manche Selbstbauanleitung (siehe ct.de/wxw1).

Die Verteilung von kryptografischen Schlüsseln und Konfigurationen erledigt man per Browser in einem zentralen Dashboard per Mausklick.

Ein Beispiel ist ZeroTier, mit dem man Server, PCs, NAS-Geräte und Smartphones vernetzt. Das geht so schnell, dass man von Blitz-VPNs sprechen kann. Mehr dazu lesen Sie in den nachfolgenden Artikeln.

## Burgverbesserung

Andere Hersteller haben das Peer-to-Peer-Konzept mit zusätzlichen Schutzmaßnahmen für Unternehmen aufgebohrt. Manche sprechen mit kostenlosen Einstiegsangeboten auch kleine Arbeitsgruppen und Privatnutzer an, zum Beispiel um Familienmitglieder zu vernetzen.

Viele Sicherheitskonzepte gehen davon aus, dass es genügt, interne Infrastrukturen ähnlich einer Burg mit Firewalls abzuschotten. Und da Mitarbeiter auch mal von draußen ins Firmennetz müssen, richtet man hinter der Firewall VPN-Server ein, zu denen ähnlich einer Zugbrücke ein gut geschützter Zugang führt. Das interne Netz gilt als sichere Umgebung für Unternehmensanwendungen.

Doch längst sind Fachleute überzeugt, dass auch das interne Netzwerk voller Gefahren steckt. Beispielsweise können Phishing-Mails zum Herunterladen von Schadsoftware verleiten.

Hinzu kommt, dass viele Mitarbeiter im Homeoffice bleiben und viele Applikationen vom abgeschotteten Firmenserver in die Cloud wandern. So sind immer mehr Mitarbeiter und Betriebsmittel übers Internet verstreut. Ein traditionelles VPN ist daher schwer zu verwalten.

Nach neueren Konzepten ist keinem Netzwerkgerät und keinem Nutzer zu trauen, jeglicher Zugriff auf Firmenressourcen muss authentifiziert, autorisiert und verschlüsselt werden (Zero Trust). Zusätzlich schränkt man den Zugriff auf die für die Arbeit erforderlichen Ressourcen und Applikationen ein (Least Privilege). So schrumpft die Angriffsfläche und es spielt keine Rolle, wo sich Mitarbeiter physisch aufhalten.

Zu dieser VPN-Klasse gehören Tailscale, Twingate und Nebula, die wir im nachfolgenden Artikel vorstellen. Tailscale gründet auf dem modernen WireGuard. Das gilt auch für das noch junge NetBird, an dem das Saarbrücker CISPA Helmholtz Center für Informationssicherheit mitwirkt. Das c’t-Magazin widmet NetBird einen separaten Beitrag in einer der kommenden Ausgaben.

## Spurlos funken

VPNs können andererseits auch im Mobilfunk die Privatsphäre schützen. Kritiker sehen diese Privatsphäre längst ausgehöhlt und halten Smartphones mit GPS für digitale Plaudertaschen.

Eine durchgehende digitale Selbstverteidigung fällt da schwer. Selbst Apples Private Relay und Google One VPN schützen nur die Kommunikation vor Mitlesern und verbergen die IP-Adresse der Nutzer. Dafür setzen beide die Kryptografietechnik RSA Blind Signatures ein und entkoppeln so die Nutzdaten von der Kundenauthentifizierung, sodass sich keine Benutzerprofile erstellen lassen. Der Verschleierer Invisv entkoppelt zusätzlich mit eigenen eSIMs die Identität des Mobilfunknutzers von der SIM-Karte (genauer: IMSI). Leider ist PGPP in Deutschland nicht zu bekommen. Warum das so ist und wie die Technik funktioniert, lesen Sie im Artikel „Smartphoneschutz per PGPP“. (dz) c't

**Peer-to-Peer-VPNs**
**ct.de/wxw1**

Bild: Andreas Martini

# VPNs für PCs und Smartphones

**Egal, ob Sie in der Welt verteilte Arbeitskräfte zusammenbringen oder nur die PCs der Verwandtschaft warten müssen: Mit einem Peer-to-Peer-VPN fangen Sie beide ein, ohne dafür Krypto-Zaubersprüche aufsagen zu müssen. Wir stellen vier Kandidaten vor.**

Von **Benjamin Pfister**

Peer-to-Peer-VPNs wurden als Infrastruktur von Tauschbörsen bekannt. Die Technik steckt aber längst auch in Anwendungen zum Vernetzen ferner Geräte und Server über zentrale Dashboards. Das unterscheidet sie erheblich von den gängigen VPNs. Wir stellen Nebula, Twingate, Tailscale und ZeroTier vor. Nebula darf man gratis nutzen, die übrigen drei bieten kostenlose Einstiege für kleine Arbeitsgruppen oder wenige Geräte. Die Preise für mehr Geräte oder Netze starten unter 10 US-Dollar.

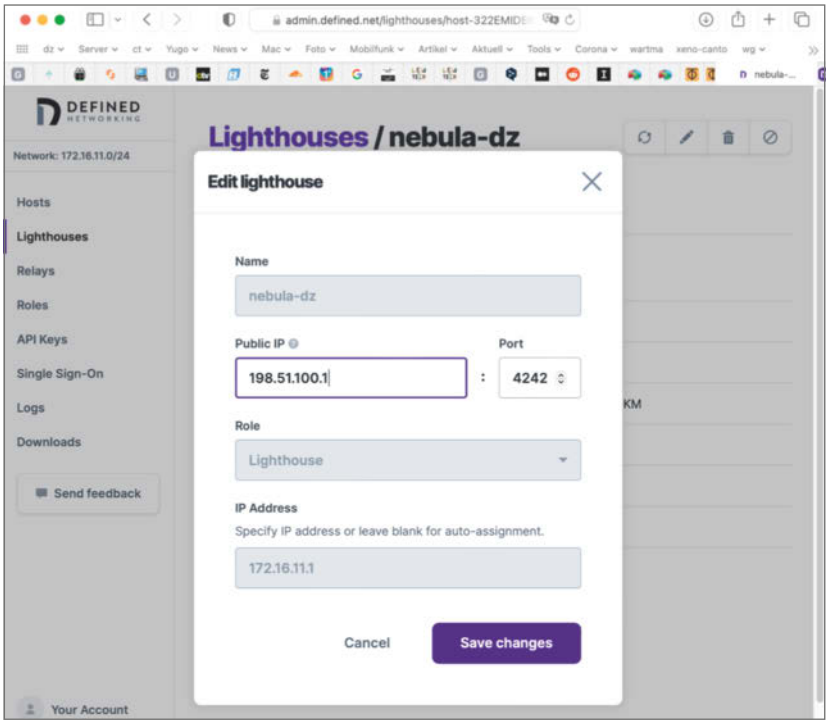
Ein klassisches VPN erlaubt es entfernten Rechnern, über verschlüsselte Tunnel auf ein lokales Netzwerk zuzugreifen. Die so vernetzten Systeme können miteinander kommunizieren, aber das immer nur über den VPN-Server. Den Tunnelaufbau stoßen VPN-Clients selbst an, von der Seite des VPN-Servers geht das nicht; allein schon, weil die meisten Clients hinter einem Router stehen, der ohne Weiteres keine Verbindung von außen zulässt.

Peer-to-Peer-VPNs lösen das anders: Eine Zentrale verwebt alle angemeldeten Systeme zu einem virtuellen gemeinsamen Netz, in dem die Daten direkt von Client zu Client fließen. Dazu müssen alle Clients die Zentrale kontaktieren. In Peer-to-Peer-VPNs sind Clients und Server gleichermaßen erreichbar, stehen auf derselben Hierarchiestufe.

Die Software entscheidet, welchen Weg die Pakete nehmen, ob direkt von einem Teilnehmer zum anderen oder über Dritte.

Ein klassischer Tunnel vermittelt Clients erstmal nur den Zugang zu einem entfernten Netz. In Firmen ist das oft nur eines von mehreren Segmenten. Dort stecken aber nicht unbedingt alle Server, die ferne Anwender für ihre Arbeit brauchen – zu manchen müssen Firmen-Admins zusätzliche Routen zu anderen Segmenten setzen, etwa zum abgeschotteten Dateiserver.

Bei Peer-to-Peer-VPNs wird der Server ebenfalls zum Peer, ist also ohne manuell gesetzte Routen erreichbar. Manche Peer-to-Peer-VPNs führen das Konzept noch weiter und verhalten sich wie ein lokales Netz: Sie können wie ein Switch auch Pakete an mehrere oder alle Teilnehmer gleichzeitig weiterleiten, also auch Broadcast- und Multicast-Pakete, die für Namensdienste wie mDNS unerlässlich sind.




**Das Peer-to-Peer-VPN Nebula braucht für die Kommunikation der Clients eine Zentrale mit statischer öffentlicher IPv4-Adresse, das Lighthouse.**

## Helfende Zentrale

Die Zentrale hilft dem Admin dabei, die Peer-to-Peer-Kommunikation aufzusetzen und Systeme, Nutzer, Zugänge und Netzwerke zu verwalten. Eine Weboberfläche dafür ist Standard (Dashboard).

Zunächst bauen Clients selbstständig IP-Sitzungen zur Zentrale auf, authentifizieren sich und laden die Koordinaten (IP-Adressen, Namen, etc.) der übrigen Clients herunter. Die Zentrale leitet dann einige UDP-Pakete von Client zu Client, bis beide Router auf den Clientseiten diesen Verkehr als legitim einstufen (UDP-Hole-Punching). Fortan kommunizieren sie trotz IPv4-NAT und IPv6-Firewall von Peer zu Peer.

Es gibt freilich Unterschiede. Die besseren Zentralen verteilen Schlüssel, Zertifikate, Clientkonfigurationen, DNS-Einstellungen und Sicherheitsregeln per Mausklick. Das ist bei Tailscale, Twingate und ZeroTier der Fall.

Einige der Peer-to-Peer-VPNs enthalten Funktionen von Software-defined Networks (SDN): Der Administrator kann das virtuelle Netz beliebig aufteilen und bestimmen, wer überhaupt in welches Subnetz kann, wer mit wem mithilfe welcher Protokolle sprechen darf und über welchen Weg bestimmte Protokolle laufen. Benutzer und Zugangsschutz sind voneinander getrennte Rollen. Manche der VPNs fordern vor dem Zutritt und jedem Applikationszugriff eine Sicherheitsprüfung, auch dann, wenn er in einem vertrauenswürdigen Netz wie einem Firmen-LAN steckt (Sicherheitsmodell Zero-Trust).

Das wichtigste Auswahlkriterium ist die Sicherheit einer Implementierung. Peer-to-Peer-VPNs sollten genauso wie IPsec- oder Wireguard-VPNs möglichst quelloffen und alle paar Jahre Prüfungen unabhängiger Fachleute bestanden haben (Security Audit).

Hinter der oft einfachen Bedienung über ein Dashboard steckt eine meist komplexe Infrastruktur aus Peer-to-Peer-Vermittlern, Relays, Datenbanken und Diensten. Das Einrichten und Verwalten kann viele Admin-Stunden kosten. Deshalb bieten manche Hersteller betriebsfertige Pakete an (Software as a Service, SaaS), die oft auf Servern in den USA laufen. Zum Experimentieren und für Anwendungen ohne besondere Sicherheitsanforderungen eignen sich solche Angebote gut.

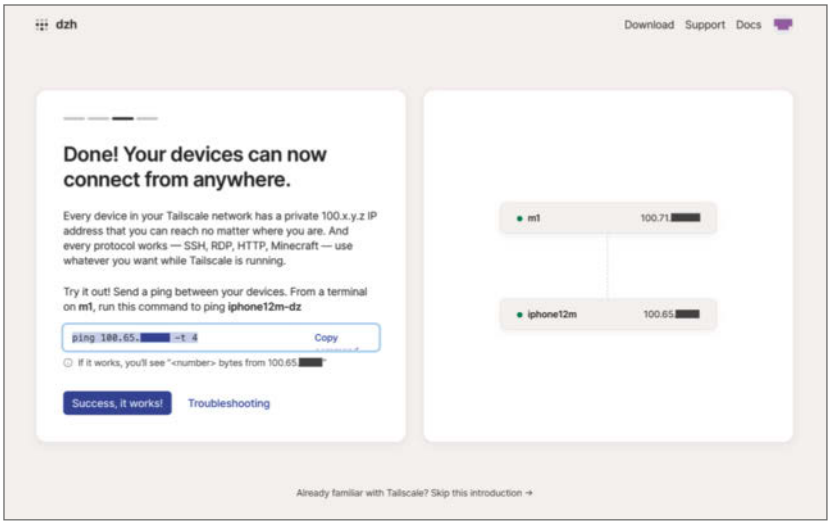
Es liegt aber auf der Hand, dass die löffelfertigen Pakete im Fokus von Angreifern stehen, denn bei gelungenem Einbruch kapern Angreifer sehr viele PCs auf einmal. Bislang wurde uns solch ein Coup nicht bekannt, aber wer die Sicherheit nicht anderen überlassen will, betreibt die Infrastruktur lieber selbst in

einem eigenen IP-Adressbereich (Self-Hosting). Diese Option bieten Nebula, Tailscale und teilweise auch ZeroTier. Self-Hosting bietet sich auch an, um die DSGVO-Richtlinien einzuhalten, wenn man etwa einen Heimarbeitsplatz an die Firma koppelt.

Die Clients sollen für möglichst alle gängigen Betriebssysteme erhältlich sein, also für PCs mit Windows, Linux, macOS und FreeBSD sowie für Smartphones und Tablets mit Android und iOS. Für IoT- und Smart-Home-Geräte, die sich nicht aufrüsten lassen, braucht man Clients als Vermittler in Routern und Firewalls.

Clients können in gleichen und auch in völlig unterschiedlichen Subnetzen stehen, sehen aber erstmal nur einander. Zum Beispiel können Clients physisch in Güstrow und Gelsenkirchen in Heimnetzen mit den Adressbereichen 192.168.178.x und 192.168.1.x sitzen, aber zum selben virtuellen Netz 172.22.2.x gehören. Dabei bildet 172.22.2.x ein von den physischen Netzen unabhängiges Overlay-Netz.

IP-Pakete, die nicht für das lokale Subnetz gedacht sind, gehen entweder über den physischen Anschluss direkt ins Internet oder über den VPN-Tunnel in das Overlay-Netz (Split Tunnel). Full-Tunnel-VPNs, bei denen alle Pakete durch den Tunnel reisen, bieten Tailscale und ZeroTier als Optionen an.




**Tailscale gründet auf dem modernen WireGuard. Das Dashboard begleitet den Admin dabei, erste Clients einzubinden und die Verbindung zu testen.**

## Nebula

Nebula bildet Layer-3-Netzwerke, sie übertragen also weder Broadcasts noch Multicasts. Nebula-Clients kommunizieren im Overlay-Netz nur per IPv4, IPv6 fehlt. Charmanterweise besteht die Clientanwendung aus einem einzigen Binary, das man über Yaml-Dateien konfiguriert, also etwa Adressen von DNS-Resolvern oder Zugriffsregeln einträgt. Ein Knoten kann als Relay einspringen, um anderen aus der Klemme zu helfen, falls deren UDP-Hole-Punching scheitert. Nebula ist auch die Technik hinter dem Instant-Messaging-Dienst Slack.

Admins gewähren Clients den Zugang mit Zertifikaten einer eigenen Zertifizierungsstelle und filtern Verkehre beispielsweise anhand von IP-Adressen oder Namen und sie fassen Clients zu Gruppen zusammen. Das zentrale Management erscheint uns noch ausbaufähig. Es gibt lediglich einen zentralen Server, das Lighthouse, der den Clients vermittelt, auf welchen Wegen sie einander erreichen. Ist der nicht erreichbar, steht der Rest im Dunkeln.

Für den Schlüsselaustausch setzt Nebula auf die Methode Elliptic Curve Diffie-Hellman (ECDH), der Verkehr wird wahlweise per AES-GCM 256 oder ChaCha20-Poly1305 verschlüsselt. Alle drei Verfahren gelten als sicher.

An Nebula gefällt, dass man IP-Verkehr anhand von Gruppen filtern kann, die im Zertifikat abgelegt sind, nicht bloß anhand von IP-Adressen. Einige Firmen bieten Nebula-Infrastrukturen als Dienstleistung mitsamt Webinterface an, darunter Defined Networking von den Nebula-Gründern (kostenloser Betrieb mit bis zu 100 Hosts). Falls man das Lighthouse selbst hostet, muss man auch Zertifikate und Konfigurationen selbst erzeugen und verteilen.

## Tailscale

Tailscale ist ein Peer-to-Peer-VPN, das auf Wireguard gründet. Tailscale-Peers können aber nicht mit WireGuard-Peers sprechen. Der Hersteller nennt als Beispielanwendungen Zugriffe auf das Heimnetz, etwa als Plattform für verteilte selbstständige Entwickler. Dafür bietet Tailscale Let's-Encrypt-Zertifikate für interne Hosts und sogar für den Reverse-Proxy Traefik. Über das API von Tailscale kann man eigene Monitoring-Projekte für die Hausautomation „Home Assistant" aufsetzen.

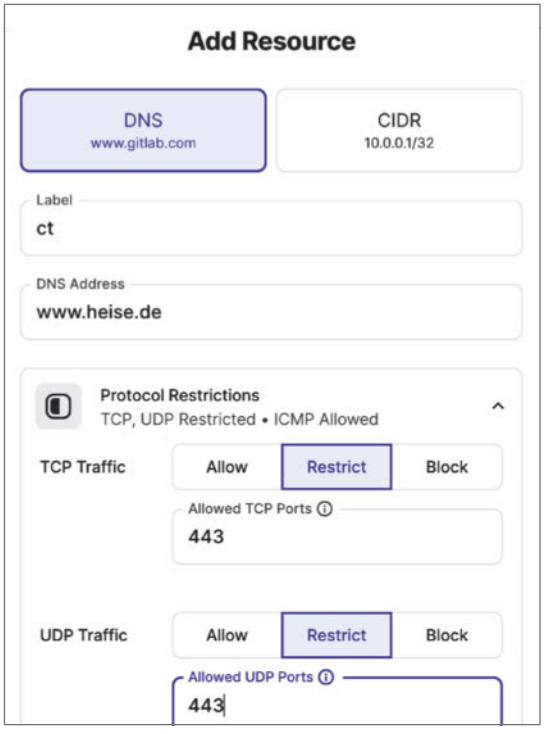
Das Login vermittelt ein Identity Provider (Microsoft, Google oder GitHub). Die Authentifizierung muss der Anwender nach einer konfigurierbaren Frist erneuern (Standard: 180 Tage). Für Geräte ohne inter-

aktives Login generiert der Admin einen Schlüssel und zum Erhöhen der Sicherheit lassen sich Clients manuell im Webinterface autorisieren.

Die Clients bilden ein Overlay-Netz, das Tailnet. Die Architektur entspricht einem Layer-2-Netz ohne Broadcasts und Multicasts. Den Kontakt zu anderen Subnetzen vermitteln auf den Endpunkten installierte Subnet-Router. Optionale Exit-Nodes bringen den Clientverkehr aus dem Tailnet ins Internet.

So wie WireGuard, braucht auch Tailscale für die Tunnelverschlüsselung einen privaten und einen öffentlichen Schlüssel, die jeder Knoten selbst generiert. Anschließend verbindet er sich mit dem Koordinierungsserver (login.tailscale.com), verknüpft den öffentlichen Key mit der ID des gewählten Identity Providers und sendet den öffentlichen Key und den Tailscale-Domainnamen mitsamt seiner Koordinaten an den Server. Dann holt er die Koordinaten der anderen Teilnehmer und erreicht sie anschließend darüber direkt. Dabei nutzt der Client für IPv6 die Unique Local Addresses (fd00::/8) und für IPv4 das Subnetz 100.64.0.0/10.

Falls das UDP-Hole-Punching scheitert, kommunizieren Clients über ein HTTPS-Relay miteinander (Designated Encrypted Relay for Packets, DERP). Dafür weisen sie sich mit WireGuard-Schlüsseln aus (der DERP-Server nutzt die Keys als abstrahierte Adressen). Tailscale-Clients verschlüsseln ihren Verkehr per ChaCha20-Algorithmus und authentifizieren sich mittels ED25519-Signaturen – beide gelten als sicher.




**Mit Twingate definieren Admins im Dashboard, auf welche Ressourcen Anwender über ihren Twingate-Client zugreifen dürfen. Unter anderem kann man bestimmen, welche Protokolle und Ports dafür benutzt werden dürfen.**

Die öffentlichen Schlüssel und die Richtlinien lagern auf dem Coordination Server (Closed Source), der über login.tailscale.com angesprochen wird. Die Kommandozeilen-Clients und der DERP-Server sind quelloffen. Den Code der Client-GUI hat der Hersteller nur für quelloffene Betriebssysteme offengelegt.

Zugang zu einem Netzwerk erhalten nur Konten derselben Maildomain. Das erschwert die Nutzung mit Partnern. Zur Namensauflösung kann man eigene Resolver verwenden oder das MagicDNS von Tailscale. Mit MagicDNS registrieren sich Clients selbstständig beim Tailnet-Resolver. Dazu nutzt MagicDNS den Maschinen- und Tailnet-Namen. So spricht man Tailnet-Clients anhand ihrer Hostnamen an. Auch lassen sich IP-Adressen von internen Hosts über private DNS-Resolver auflösen.

Die Funktion „Service Discovery“ informiert im Webinterface über verwendete Dienste im Tailscale-Netz. Dafür senden Tailscale-Clients Protokollnamen und Portnummern wie TCP und 443 an den Webservice, der den übergeordneten Dienstnamen (z. B. HTTPS) ergänzt und einblendet.

Zu den Stärken von Tailscale gehören die übersichtliche Konfiguration und Verkehrssteuerung. Dafür trägt der Admin Attribute wie Usernamen, Gruppen, Tags und Hosts in der Zentrale ein und definiert so, wer mit wem und über welche Dienste kommunizieren darf.

Tailscale gibt es als SaaS-Anwendung; mit dem quelloffenen Coordination Server Headscale ist auch Self-Hosting möglich. (ct.de/w8sf).

## Twingate

Twingate bildet Layer-3-Netze für den geregelten Zugriff auf interne Ressourcen und erscheint für Firmen und Anwender mit hohen Sicherheitsanforderungen interessant, denn jede Kommunikationsbeziehung muss explizit gestattet werden (Zero-Trust-Ansatz). Den Netzwerkbeitritt, die Anmeldung an die Adminoberfläche und den Zugriff auf Ressourcen sichert Twingate vorbildlich per Zwei-Faktor-Authentifizierung ab. Eine Möglichkeit zum Self-Hosting fehlt.

Das Webinterface läuft auf einem zentralen Controller. Admins melden sich daran über einen Identity Provider an (Azure, Google, Okta, One Login oder

Jump Cloud). Die gesamte Infrastruktur besteht aus Controllern, Clients und Relays – die können irgendwo im Internet stehen – sowie aus Konnektoren hinter der Firewall. IP-Verbindungen zu Ressourcen hinter der Firewall vermittelt immer ein Konnektor. Über den Controller bestimmt der Admin, welche Clients, Relays und Konnektoren zusammenspielen.

Praktisch daran ist, dass DNS-Anfragen von Clients für interne Dienste immer beim zuständigen Konnektor landen, der sie lokal auflöst. Andernfalls kann es passieren, dass Clients Dienste nicht finden, weil sie ihre DNS-Anfragen an einen externen DNS-Server schicken, aber externe DNS-Server kennen keine firmeninternen Server. Zusätzlich kann der Admin DNS-Anfragen der Clients per DNS-over-HTTPS schützen. Dann verschlüsseln sie alle DNS-Anfragen sowohl für Twingate-Ressourcen als auch für Domains im Internet.

Zugriffe auf interne Ressourcen regelt der Admin mittels Access Control Lists (ACL), die er an Benutzer und Konnektoren verteilt. So kann er anhand von Domainnamen und Subnetzbereichen filtern und TCP-, UDP- und ICMP-Verkehr entweder global gestatten oder bei UDP und TCP auf bestimmte Ports einschränken.

Twingate kann man kostenlos mit bis zu fünf Benutzern und bis zu zehn Netzwerken nutzen. Für größere Teams gibt es Abos ab 5 US-Dollar pro Monat.

## ZeroTier

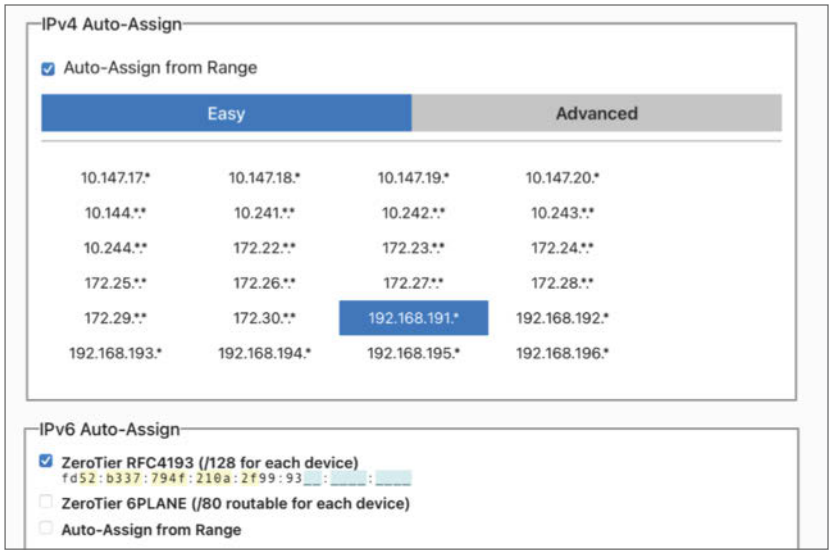
ZeroTier knüpft virtuelle Layer-2-Netze und befördert auch Broadcast- und Multicast-Pakete. Der gleichnamige Hersteller bezeichnet sein Produkt zwar vollmundig als einen „Smart Ethernet Switch for Planet Earth“, doch andere Peer-to-Peer-VPNs sind in puncto Anwendungsfilterung weiter. Aber ZeroTier, kurz ZT, kommt einem Switch ziemlich nahe und erleichtert so besonders Nutzern ohne große Vorkenntnisse den Zugriff auf entfernte Freigaben und Dienste. Wie einfach das geht, lesen Sie im Artikel „PCs und Heimnetze mit ZeroTier vernetzen“.

Der Hersteller bietet eine fertige Infrastruktur an. Beim Self-Hosting bleibt ein Teil der Herstellerinfrastruktur immer angekoppelt. So möchte der Hersteller störungsfreien Betrieb auch dann gewährleisten, wenn Self-Hosting-Elemente ausgefallen sind. Nach dem Erstellen eines Kontos (authentifiziert über Mailadresse, Google, GitHub oder Microsoft), genügen zwei Klicks, um ein privates oder öffentlich zugängliches Netzwerk anzulegen. Um Clients in ein öffentliches ZT-Netz zu bringen, gibt man ihnen die 16-stellige Netz-ID. Den Beitritt

### Peer-to-Peer-VPNs

| Bezeichnung | Nebula | Tailscale | Twingate | ZeroTier |
|---|---|---|---|---|
| Architektur | Peer-to-Peer/ Peer-Relay | Peer-to-Peer/Fallback: Hub and Spoke | Peer-to-Peer/Fallback: Hub and Spoke | Peer-to-Peer/Fallback: Hub and Spoke |
| Basisprotokoll | Abgeleitet von TINC | WireGuard/Fallback: HTTPS | QUIC | ZeroTier UDP 9993 |
| Verschlüsselungsverfahren | AES-256-GCM, ChaCha20-Poly1305 | ChaCha20 | TLS 1.3 (auf Basis von QUIC) | 256 Bit Salsa20/Poly1305 |
| Push-Konfig: Routing, DNS | ✓, ✓ (experimentell) | ✓, ✓ (MagicDNS, frei wählbare Resolver) | ✓, ✓ (frei wählbare Resolver) | ✓, ✓ (ZeroNSD, frei wählbare Resolver) |
| Broadcast, Multicast | – / – | – / – | – / – | ✓ / ✓ |
| 2 FA/Filterregeln | – / ✓ | ✓ (abhängig vom Identity-Provider)/✓ | ✓ / ✓ | ✓ (abhängig vom Identity-Provider)/✓ |
| eigene Schlüssel/autom. Schlüsselverwaltung | ✓ / – | – / ✓ | – / ✓ | – / ✓ |
| unterstützte Betriebssysteme | FreeBSD, Linux, macOS, Windows, Android, iOS | FreeBSD, Linux, macOS, OpenBSD, Windows, Android, iOS | ChromeOS, Linux, macOS, Windows, Android, iOS | FreeBSD, Linux, macOS, OpenBSD, Windows, Android, iOS, div. NAS-Geräte und Router |
| Security Audits | ✓ (laut Angaben von Slack) | ✓ | ✓ | veraltet, weil ZeroTier auf Salsa20/ Poly1305 umgestellt hat |
| Open Source/ Self-Hosting | ✓ / ✓ | ✓ (außer GUI Clients)/ ✓ (mit Headscale) | – / – | ✓ / ✓ |
| kostenloser Einstieg | ✓ (Kosten für vServer ab 5 €/Monat) | max. 25 Benutzer, max. je 5 Geräte (GitHub Community-Tarif) | max. 5 Benutzer und 10 Netze (Personal-Free-Tarif) | max. 25 Geräte, beliebig viele Netze (Basic-Free-Tarif) |
| Preisstaffelung | – (Kosten für vServer ab 5 €/Monat) | ab 6 US-$ pro Monat | ab 5 US-$ pro Monat | ab 5 US-$ pro Monat |

✓ vorhanden – nicht vorhanden




**Praktisch an Peer-to-Peer-VPNs ist, dass eine Zentrale elementare Konfigurationen automatisch an Clients verteilt. So kann man in ZeroTier beispielsweise den IP-Adressbereich des gesamten ZeroTier-Netzwerks mit einem Mausklick ändern.**

zu einem privaten ZT-Netz nickt der Admin mit einem Klick im Webinterface ab.

Im Webinterface ist auch der IPv4-Adressbereich des ZT-Netzwerks aufgeführt; bei Bedarf kann man es leicht ändern, etwa bei Adresskollisionen und auch mehr als ein Subnetz zuweisen. Gleiches gilt für IPv6-Adressen, wobei man nicht nur lokale, sondern auch globale IPv6-Adressen konfigurieren kann; das Präfix muss freilich ein separat konfiguriertes Gateway wie ein vServer zuliefern. Wie das geht, beschreiben wir detailliert im Artikel „Google One VPN für PCs und Smartphones“. Ab Version 1.6 kann man Clients auch DNS-Resolver und Suchdomains zuweisen und Weiterleitungsregeln für den Datenverkehr einrichten.

Vollwertige Clients gibt es für macOS, Linux, Windows, FreeBSD und OpenBSD. Für einige Router, darunter Mikrotiks RouterOS und für OpenWRT gibt es ebenfalls ZT-Clients. Die iOS- und Android-Apps hängen im Entwicklungsstand zurück und können selbstgehosteten ZT-Infrastrukturen nicht beitreten. Der Android-Client eignet sich nicht für Full-Tunnel-VPNs.

Die Peers bringt ein Root Server (Moon oder Planet genannt) per UDP-Hole-Punching zusammen. Falls das scheitert, vermittelt er zwischen den Clients. Ein Managementserver teilt den Clients Konfigurationen und Schlüssel zu. Weil sie vor und nach dem Wechsel auf Peer-to-Peer verschiedene Pfade nutzen, sind auch die Paketlaufzeiten und -schwankungen unterschiedlich (Jitter), was beispielsweise bei VoIP-Telefonaten und Videokonferenzen verzerrte Wiedergaben zur Folge haben kann.

ZeroTier ignoriert in TCP-Headern gesetzte Don't-Fragment-Bits. Das ermöglicht Fragmentierungsangriffe und erhöht die Latenz, weil Ziel-Hosts die Fragmente erst puffern und zusammensetzen müssen.

Das ZeroTier-Protokoll ist auf die Ebenen VL1 und VL2 aufgeteilt. Die Basiskommunikation mit Schlüsselverteilung, Authentifizierung und Verschlüsselung läuft über VL1. Die VL1-Ebene wird mit 256 Bit langen Salsa-20-Schlüsseln chiffriert, was als zeitgemäß gilt.

Die VL2-Ebene verhält sich wie ein zentraler, verteilter und gemanagter Switch. Sie bringt ZT-Clients über Routergrenzen hinweg ins gemeinsame ZT-Netz. Hosts tauschen darüber wie in einem physischen Ethernet-Segment Broadcasts und Multicasts aus. Im zentralen Management erstellt man Regelwerke mit statuslosen Paketfiltern oder leitet den Verkehr wie bei einem echten Switch zur Fehleranalyse an mitschreibende PCs aus. Für den Zugriff auf private Netze hinter ZT-Nodes konfiguriert man statische Routen, die die Zentrale an alle Hosts pusht. Das tatsächliche Routing richtet man dann etwa auf einem Raspi mittels Firewallregeln in iptables ein.

ZeroTier eignet sich für private Anwendungen mit üblichem Schutzbedarf, also etwa für Fernwartungen oder Zugriffe auf Netzwerkspeicher. Als Self-Hosting-Variante erscheint ZT auch für kleine Unternehmen interessant, um etwa mit Notebooks mobile Mitarbeiter anzubinden.

## Fazit

Peer-to-Peer-Anwendungen sind vielseitig und das Ausloten macht Freude, selbst wenn man bereits ein zuverlässiges VPN betreibt. Wer detaillierte Kontrolle über Netzwerkgeräte, Anwender, Protokolle und Applikationen braucht, sollte Twingate und Tailscale in die engere Wahl ziehen, allerdings fehlt Twingate eine Self-Hosting-Option.

Wenn das eine Bedingung ist, gebührt neben Tailscale auch Nebula ein vertiefter Blick. Nutzer, die mehr Gewicht auf einfache Gerätevernetzung legen, haben mit ZeroTier einen starken Kandidaten, Self-Hosting-Option inklusive. (dz) c't

**Peer-to-Peer-VPN-Infos**
**ct.de/w8sf**

Bild: www.freepik.com

# Smartphoneschutz per PGPP

**Pretty Good Phone Privacy ist ein Dienst, der die Kommunikation von Smartphonenutzern ähnlich einem VPN schützt und das Tracking trotz GPS drastisch erschwert. Auch führt er IMSI-Catcher hinters Licht. Wir haben den Dienst ausprobiert.**

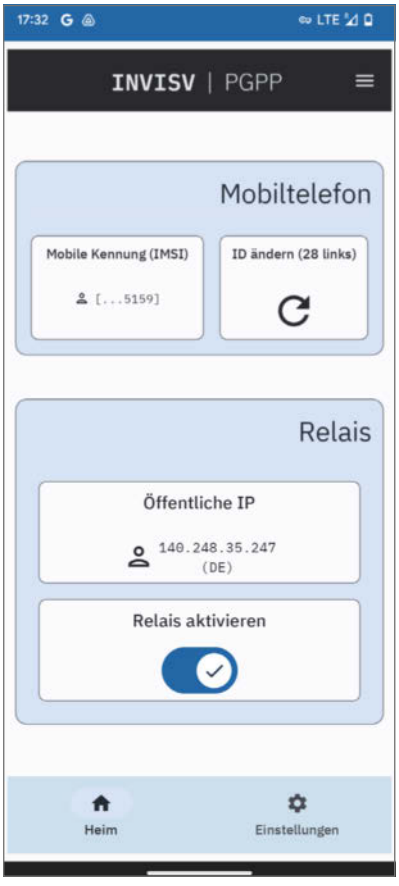
Von **Dušan Živadinović**

Pretty Good Phone Privacy (PGPP) stammt vom US-Startup Invisv, das die Professoren Paul Schmitt und Barath Raghavan 2022 gegründet haben. Mit der augenzwinkernden Abkürzung PGPP stellen sie ihren Dienst namentlich neben die berühmt-berüchtigte E-Mail-Verschlüsselung PGP. Der Smartphonedienst PGPP bietet aber gleich vier Schutzfunktionen: Verschleierung der IP-Adresse, Schutz des Internetverkehrs vor Mitlesern, Mobilfunkzugang zum Internet und darauf fußend die Verschleierung der Nutzer-Identität gegenüber dem Mobilfunknetzwerk.

Bevor Sie es selbst ausprobieren: Die beiden letzten Funktionen bietet Invisv für Deutschland aus rechtlichen Gründen nicht an. Mobilfunkanbieter dürfen SIM-Karten nur unter Vorlage eines Ausweises aktivieren und müssen die Kundendaten mitsamt der zugeteilten SIM-Kennung für die Vertragsdauer aufbewahren, was bei PGPP schlicht nicht geht, weil es ja gerade die Identität verschleiert. Für Kunden aus Deutschland bleibt nur der Relay-Tarif übrig, der für fünf US-Dollar monatlich den Smartphoneverkehr verschlüsselt und die IP-Adresse verschleiert.

In diversen anderen Ländern kann man PGPP ohne Weiteres buchen, darunter Dänemark, Großbritannien, Niederlande, Portugal und USA. Und Invisv-Kunden mit ausländischen SIMs können PGPP im Roaming-Modus auch in Deutschland nutzen. Damit dürfte die Technik mindestens hiesige Strafverfolger interessieren.

Alle Funktionen stecken in der gleichnamigen App, die derzeit nur für Android-Smartphones erhältlich ist; der Relay-Client soll laut Invisv „bald“ in den Browser Vivaldi integriert werden (Stand September 2023). Heruntergeladen von der Webseite des Herstellers (siehe ct.de/weam), ist sie ruckzuck installiert. Um die Dienste zu nutzen, bucht man mittels einer Kreditkarte einen Tarif (40 oder 90 US-Dollar monatlich) und bekommt dann übers Internet eine eSIM, die ihresgleichen sucht: Über einen Button der App kann man nämlich die International Mobile Subscriber Identity ändern (IMSI) und damit viele Smartphonespuren verwischen.




**Oben rechts befindet sich der Zauberknopf: Mit der App PGPP lässt sich die eigentlich unveränderliche mobile Kennung einer SIM-Karte (IMSI) per Fingertipp doch ändern. Das erschwert das Tracking erheblich.**

Die IMSI ist eine Kennung der SIM und normalerweise mit einer Kundenidentität verknüpft, weshalb auf ihr die Mobilfunkabrechnung fußt. Darum senden Handys die IMSI an das Mobilfunknetz schon beim Einschalten. In der Mobilfunkspezifikation gilt sie als unveränderlich und weltweit eindeutig.

Zusammen mit der GPS-Funktion können Mobilfunknetzbetreiber detaillierte Standortverläufe anlegen und manche schlachten diese mit anderen Metadaten des Kunden für Werbezwecke aus (siehe ct.de/weam). Gelegentlich ist die IMSI auch Ziel von Angreifern, die mit IMSI-Catchern Nutzer verfolgen und abhören.

PGPP unterbindet die Trackingvariante und den Lauschangriff, indem es die Identität des Nutzers von der IMSI entkoppelt. Dafür generiert man mittels der PGPP-App eine neue IMSI, zum Beispiel täglich. Da Invisv die Identität des Nutzers nicht kennt, weiß die Firma nicht, welche ihrer Kunden welche IMSI benutzt haben. Man erhalte laut Anbieter lediglich vom Bezahldienst Teile der Kreditkartennummer und das Datum des eSIM-Kaufs, aber keine Merkmale des Smartphones.

## Blindsignaturen

Um die Verknüpfung der Identität mit der IMSI aufzuheben, setzt Invisv die Kryptotechnik Blind Signatures ein. Diese bereits 1983 entwickelte Methode verwenden heute zum Beispiel elektronische Wahlmaschinen. Damit gewährleisten sie, dass nur registrierte Wähler zum Zug kommen, aber niemand erfährt, welche Kandidaten sie wählen.

Invisv nutzt Blindsignaturen, um sicherzustellen, dass ein Smartphone den Bezahlvorgang für einen der beiden Mobilfunktarife korrekt abgeschlossen hat. Weil dabei Blindsignaturen und andere Elemente zwischen Smartphone und Invisv-Servern wandern, kann sich das Erzeugen einer neuen IMSI einige Sekunden bis Minuten hinziehen, je nachdem, wie schnell der Internetanschluss ist. Kaufspuren sind erst dann komplett verwischt, wenn der Dienst mit einer Prepaidkreditkarte bezahlt wird, die nicht mit dem Namen einer Person verknüpft ist.

## Relay-Sprung

Zusätzlich verschleiert Invisv über ein Relay die IP-Adresse und verschlüsselt den Smartphoneverkehr. Beides bekommt man bei Apple mit iCloud Private Relay und bei Google mit dem Dienst One VPN bereits seit 2022 (ab 0,99 Euro bzw. ab 10 Euro monat-

lich). Google One VPN haben wir ausführlich getestet (ct.de/weam).

Die Parallelen überraschen nicht: Paul Schmitt hat die Relay-Technik und Blindsignaturen an der Universität Princeton für den Privatsphärenschutz verknüpft und 2019 vorgestellt. Apple, Fastly und Cloudflare haben sie aufgegriffen und unter dem Dach der Internet Engineering Task Force diverse Spezifikationen verfasst (z. B. Oblivious DNS-over-HTTPS, RFC 9230).

Deshalb funktioniert der Surfschutz bei Apple, Google und Invisv gleich: Zunächst wird die Kundenauthentifizierung mit Blindsignaturen von den Nutzdaten separiert. Dann laufen Internetdaten verschlüsselt über zwei Stationen, von denen die erste (Relay) den verschlüsselten Inhalt nicht einsehen kann und die zweite zwar entschlüsseln kann, aber nicht weiß, von wem die Daten stammen.


**Zusätzlich kann PGPP über eine Relay-Funktion den Internetverkehr des Smartphones schützen und die IP-Adresse des Nutzers verschleiern.**

Das Relay betreibt jeder Anbieter selbst. Die zweite Station steuert ein unabhängiger CDN-Anbieter wie Fastly bei. Er leitet die Daten des Smartphones zum Ziel im Internet weiter, weshalb es den Anschein hat, als wäre Fastly der Absender.

Alle drei Anbieter versuchen, stets die nächstgelegenen Internetausgänge des CDN-Anbieters zu verwenden. Im Test mit PGPP klappte das gut, aber es kommt vor, dass Videostreams stottern, wenn die Streams fälschlich nicht vom nächstgelegenen Rechenzentrum kommen, sondern etwa aus dem Ausland. Die Ursache ist, dass Streaminganbieter manche IP-Adressen falschen Standorten zuordnen. In solchen Fällen kann es helfen, die Relay-Funktion neu zu starten, um eine neue IP-Adresse von Fastly zu bekommen.

Wie manche andere VPN-Anwendung, so kann auch PGPP bei Bedarf automatisch anspringen und auch jeglichen Verkehr blockieren, falls die Relay-Funktion gerade nicht läuft. Beide Optionen schützen das Smartphone automatisch in öffentlichen WLAN-Hotspots.

## Home, sweet home

Wir haben vom Hersteller einen Zugang für PGPP erhalten und konnten den Dienst einige Wochen lang testen. Dafür haben wir ein Google Pixel 6a mit aktuellem Android verwendet. Die eSIM buchte sich automatisch und reibungslos in das O2-Netz ein. Auch ließ sich das Smartphone als Mobilfunk-Gateway für angekoppelte Notebooks nutzen (Tethering). Jedoch läuft der Notebookverkehr nicht über das Relay, laut Hersteller aufgrund von Android-Einschränkungen.

Schaltet man das Relay ab und surft per Mobilfunk weiter, sollte das Smartphone eigentlich eine IP-Adresse aus dem Vorrat des Roaming-Netzwerks benutzen, im Testszenario also von O2. Stattdessen bekommt es jedoch Adressen von Invisv-Partnern, beispielsweise vom Londoner Unternehmen OVH oder vom New Yorker Local Internet Registry Equinix.

Das verwundert zunächst, doch PGPP funktioniert nur im Zusammenspiel mit dem zugehörigen Gateway von Invisv. Deshalb erzwingt Invisv, dass Roaming-Partner die Smartphonedaten ins Heimatnetz der eSIM schicken (home routed roaming), also zu einem Invisv-Standort. Dort purzeln die Smartphone-

## PGPP-Tarife von Invisv

| Tarifmerkmal/ Bezeichnung | Relay | Mobile Core | Mobile Pro |
|---|---|---|---|
| Datenvolumen/ Geschwindigkeit | – | 9 GByte/max. Speed bis 300 MByte täglich, danach 256 Mbit/s | Flatrate/max. Speed je nach Netz auch im Roaming |
| IMSI-Wechsel pro Monat | – | 8 | 30 |
| Adressverschleierung und Datenverschlüsselung | ✓ | ✓ | ✓ |
| Preis | 5 US-Dollar pro Monat | 40 US-Dollar pro Monat | 90 US-Dollar pro Monat |

daten über die Infrastruktur eines der Festnetzprovider ins Internet, die Invisv gebucht hat.

## eSIM-Quelle

Invisv bezieht eSIMs vom kanadischen Unternehmen Telna, das wiederum mit Mobilfunknetzbetreibern weltweit zusammenarbeitet. Das Smartphone erhielt eine eSIM des polnischen Providers Play. Invisv gibt an, dass PGPP auf allen Kontinenten verfügbar ist. Auch der polnische eSIM-Anbieter ist in vielen Ländern als Roaming-Partner akzeptiert. Mit etwas Glück könnte PGPP also auch in Ländern wie Iran oder China funktionieren.

Zur eSIM gehört weder eine Rufnummer noch der SMS-Dienst, sodass man beispielsweise den Signal-Messenger nicht registrieren kann.

**Blindsignaturen, PGPP-Infos**

**ct.de/weam**

Neben der IMSI hat ein Smartphone viele Merkmale, die es wiedererkennbar machen, darunter die weltweit eindeutige Gerätekennung (International Mobile Equipment Identity, IMEI). Invisv versichert, dass Tracking auf IMEI-Grundlage unüblich sei und glaubt, dass große Provider Jahre brauchen werden, um ihre Methoden umzustellen.

Außerdem stecken in Android Funktionen zum Protokollieren von GPS-Daten (Location Tracking), die Google in den USA auf staatliche Weisung abfragen muss. Wer auch diese Trackingoption loswerden will, muss den steinigen Weg gehen und ein angepasstes Android wie GrapheneOS installieren.

## Fazit

Invisv dürfte mit seinem Dienst viele Interessenten ansprechen und Strafverfolgern weitere graue Haare bescheren. Derweil führt die Firma die hier vorgestellten Konzepte mit weiteren Anwendungen fort, darunter dem Videokonferenzsystem Booth, das sich noch in der Beta-Entwicklungsphase befindet und im Browser läuft.

Möglicherweise regt PGPP dennoch den einen oder anderen Mobilfunknetzbetreiber an, es Invisv nachzumachen, um mit Privatsphärenschutz Mitbewerbern Kunden abzujagen. Aus Anwendersicht ist mit den PGPP-Diensten ein großes Datenloch deutlich kleiner geworden, aber wegen beispielsweise Trackern in Apps nicht geschlossen. Umfassenden Schutz vor unerwünschtem Tracking und Malware bekommt man erst mit weiteren Werkzeugen. (dz) c't

Bild: Andreas Martini

# PCs und Heimnetze mit ZeroTier vernetzen

**Brauchen Sie Zugriff auf entfernte Bildschirm- oder Dateifreigaben? Wollen Sie Server unterwegs fernwarten oder eine LAN-Party über mehrere Standorte organisieren? Mit der Software ZeroTier gelingt all das überraschend einfach. Wir zeigen, wie Sie damit umgehen.**

Von **Dušan Živadinović**

Ein zentrales Dashboard vereinfacht das Vernetzen entfernter Geräte gegenüber anderen VPN-Lösungen wie WireGuard, OpenVPN oder IPsec drastisch. Der Benutzerkomfort erinnert an frühe Ein-Klick-VPNs wie Hamachi. ZeroTier räumt die VPN-typischen Stolpersteine beiseite und automatisiert die Schweißtreiber so weit, dass sich der Netzwerkadmin ganz auf das Koppeln der Geräte konzentrieren kann. Beispielsweise nimmt ihm die Software das Verwalten der kryptografischen Schlüs-

sel ab, ebenso den Tunnelaufbau und überwindet dabei automatisch Hindernisse wie die Adressübersetzungen (NAT) von Routern.

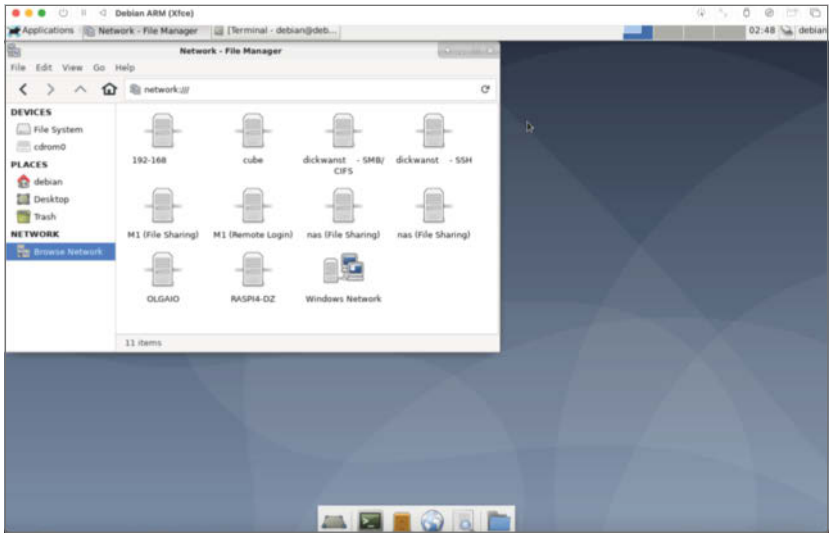
ZeroTier gibt es etwa seit 2013. Inzwischen hat die gleichnamige, in Kalifornien ansässige Firma eine breite Fan-Gemeinde, zu der Netzwerker, Gamer und Bastler gehören. Auch ein IBM-Entwickler führt in einem Blog von Januar 2023 vor, wie er das Tool verwendet (ct.de/wjnp).

In diesem Beitrag zeigen wir, wie einfach man ZeroTier-Netze (kurz ZT-Netze) einrichtet. Überraschend sind sie auch in Spielerkreisen in Gebrauch, als Rückgrat für Spiele über entfernte Standorte, obwohl die betreffenden Spiele eigentlich nur für lokale Netze ausgelegt sind. Die erhöhte Signallaufzeit scheint diesen Gamern die Spiellust nicht zu verderben. Auf ct.de/wjnp finden Sie verschiedene Listen von Games, die erfolgreich getestet worden sind („Race07“, „SWAT 4: TBA“ und viele andere).

Erste Geräte sind selbst ohne Netzwerkkenntnisse so schnell vernetzt wie eine Kaffeepause vorüber ist. Anschließend kann man das Netz erweitern. Wir zeigen beispielsweise, wie Sie auf Ihre Clients nicht nur über IP-Adressen zugreifen, sondern anhand von leichter merkbaren Hostnamen.

Vor dem Start einige warnende Worte: Die Quellen der diversen Clients, Server und anderer Infrastrukturelemente sind zwar offengelegt, aber ZeroTier verwendet proprietäre Protokolle. Diese wurden von unabhängiger Stelle auf Sicherheit geprüft, aber später hat ZeroTier die Verschlüsselung modernisiert, sodass ein Restrisiko für unbefugte Datenabflüsse bleibt. Mehr dazu finden Sie im Kasten „Sicherheits-Check“.

Der Zugang zu ZeroTier-Netzen lässt sich nur auf Geräteebene regeln, eine User-Authentifizierung fehlt. Daher sollte man neue Clients nur handverlesen in sein Netz lassen. Umgekehrt gilt: Wer eine Einladung erhält, einem ZT-Netz beizutreten, sollte sicher sein, dass der Anbieter vertrauenswürdig ist.




**ZeroTier bildet ähnlich wie Switches Layer-2-Netzwerke, sodass Linux und macOS auch ferne Freigaben auf dem Desktop darstellen, als wären sie im selben Netz.**

## Schnellstart

Öffnen Sie im Browser die Webseite zerotier.com, legen Sie ein Konto an (Sign Up) und melden Sie sich auf my.zerotier.com an. Dort verwalten Sie alles zentral in einem Dashboard.

Klicken sie auf „Create A Network“, um ein Netz zu erzeugen. Zur Identifikation erhält es einen Namen und eine 16-stellige ID (linke Spalte) und für den Betrieb ist schon ein privater IPv4-Adressbereich vorgesehen. Wenn Sie auf den Namen klicken, erscheint die Managementseite. Dort können Sie den Namen nach Belieben ändern. ZT-Netze sind in der Grundeinstellung privat, was bedeutet, dass Clients nur nach Genehmigung beitreten können. Wir gehen im Weiteren davon aus, dass Sie das Netz in Privateinstellung betreiben.

Installieren Sie nun einen ZeroTier-Client auf einem Ihrer Geräte. Sie finden die Software im Dashboard über den Menüpunkt „Download“. Folgen Sie der Anleitung für die jeweilige Plattform.

Clientnutzer und ZT-Netzbetreiber müssen einer Vernetzung beide zustimmen. Auf Clients geht das über die Option „Join New Network“. Dort trägt man die 16-stellige ID eines ZT-Netzwerks ein und schon klopft der Client beim ZT-Netz an. Für Clients mit Kommandozeilensteuerung (z. B. Linux) sieht das so aus; setzen Sie für Netzwerk-ID ihre ID ein:

```
zerotier-cli join Netzwerk-ID
```

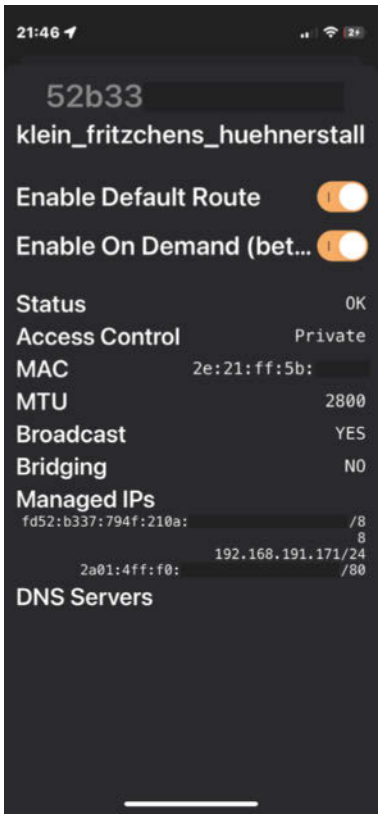
ZT-Betreiber genehmigen den Beitritt im Dashboard im Bereich „Members“. Alle neuen Clients warten dort auf Einlass, auch ein Client, der auf demselben PC läuft, auf dem Sie das Dashboard bedienen. Er betritt das Netzwerk, wenn Sie links in der Spalte „Auth?“ beim jeweiligen Client ein Häkchen setzen. Wenn Sie es wegnehmen, wartet er wieder draußen.

In der Spalte „Name/Description“ kann man einen Namen und eine Kurzbeschreibung eintragen. In den übrigen Spalten stehen zugewiesene IP-Adressen, Onlinestatus, Clientversion und die Quell-IP-Adresse des Clients, beispielsweise 10.147.14.14. Wenn Sie mindestens einen weiteren Client aufnehmen, können Sie den Kontakt testen, beispielsweise von einem PC aus mit:

```
ping 10.147.14.14
```

Ersetzen Sie 10.147.14.14 durch die IP-Adresse, die dem Zielgerät laut Dashboard zugewiesen ist. Anhand der Adressen öffnen Sie auf einem Desktop-PC entfernte Freigaben von Geräten mit ZeroTier-Clients, ganz so, als wären sie in Ihrem lokalen Netz. Auf Linux-PCs und Macs kann man Bildschirm-, Drucker- und Dateifreigaben sogar anhand der Namen und auf einem grafischen Desktop per Mausklick öffnen.

In der Spalte „Address“ stehen die zehnstelligen Node-IDs der Clients. Falls Sie Geräte von anderen Nutzern in Ihr Netz aufnehmen, beispielsweise zur Fernwartung, vergewissern Sie sich mit einem Anruf oder einer Textnachricht, um wessen Client es sich handelt. Tragen Sie dann einen wiedererkennbaren Namen zur jeweiligen Node-ID ein, beispielsweise „Werners Raspi“.




**Der ZeroTier-Client für iPhones kann für den Schutz in Hotspots den VPN-Tunnel automatisch aufbauen und auch ein fernes Internet-Gateway nutzen. ZeroTier gibt es auch als Android-Client.**

## Layer-2-Spaziergang

ZeroTier verhält sich wie ein Ethernet-Switch, der IPv4-, IPv4-ARP- und IPv6-Ethernet-Pakete befördert (Layer-2-Architektur). Deshalb funktionieren die üblichen Befehle, um lokale Ethernet-Segmente zu erkunden. So kann man auf Linux mit den Befehlen `arp -a` und `ip -6 -r neighbor show` IPv4- und IPv6-Nachbarn suchen (`ndp -a` auf macOS, `Get-NetNeighbor` in der PowerShell auf Windows).

Der Layer-2-Architektur ist zu verdanken, dass in Heimnetzen gebräuchliche, dezentrale Namensauflösungen funktionieren (mDNS, NetBIOS). ZeroTier befördert nämlich Ethernet-Broadcasts und Multicasts zwischen den Clients. Broadcasts sind für viele Spiele unerlässlich, mDNS für dezentrale Namensauflösungen.

Wir haben ZeroTier überwiegend in der oben beschriebenen Konfiguration benutzt, also ohne Gateway zum Internet, sondern in der Split-Tunnel-Konfiguration. Ziele, die sich im Internet befinden, werden dabei über den gewählten Provider angesprochen, und nur die für das ZT-Netz bestimmten Pakete gehen in den ZT-Tunnel. Wie man ZeroTier für den Full-Tunnel-Betrieb konfiguriert, haben wir in c’t 9/2023 ab Seite 170 beschrieben.

## Zentrales DNS

In einem ZT-Netz kann man viele Geräte über Namensdienste wie NetBIOS oder mDNS anhand ihrer Hostnamen ansprechen und muss sich ihre IP-Adressen nicht merken. Manche Geräte spielen aber nicht mit und senden beispielsweise keine mDNS-Annoncen.

In solchen Fällen kann man zusätzlich einen eigenen DNS-Resolver verwenden. Dafür muss man im Dashboard dessen IP-Adresse und unbedingt auch einen Domainnamen eintragen; andernfalls übernimmt das Dashboard den Eintrag nicht. Anschließend pusht ZeroTier die DNS-Einstellungen umgehend an die Clients.

Wer keinen eigenen Resolver betreibt, kann ZeroNSD nehmen. Dabei handelt es sich um einen

vom Hersteller auf ZeroTier maßgeschneiderten Resolver. Er sammelt nach dem Start die Namen und IP-Adressen der Hosts eines ZT-Netzes selbstständig ein und fügt sie einer internen Domain wie kleintier.zoo hinzu.

Mit etwas Linux-Know-how ist die Installation nebenbei erledigt. Wir haben gute Erfahrungen mit ZeroNSD in VMs auf Synology-NAS-Geräten gemacht (DS1621+ und RS1619). Dafür haben wir die aktuelle Debian-Distribution verwendet. Um ZeroNSD einzurichten, installieren Sie zunächst den ZeroTier-Client auf einem Linux-Gerät und melden ihn an dem ZT-Netz an, für das sie den Namensdienst einrichten wollen.

ZeroNSD nutzt das ZeroTier-API, um Teilnehmer eines ZT-Netzwerks zu finden. Für den Zugriff auf das API braucht der Server eine Zeichenfolge, Token genannt, die Sie im ZeroTier-Account erzeugen. Öffnen Sie dazu im Browser my.zerotier.com, klicken Sie in der Menüzeile auf „Account“ und weiter unten auf „New Token“. Tragen Sie einen Namen ein (z. B. zeronsd) und setzen Sie die 32 Zeichen lange Zeichenkette anstelle von knzlprz in den folgenden Befehl:

```
sudo bash -c "echo knzlprz↵
↳ /var/lib/zerotier-one/token"
```

Erlauben Sie mit dem chmod-Befehl nur dem während der ZeroTier-Client-Installation erstellten Nutzer zerotier-one, auf die Datei zuzugreifen:

```
sudo chown zerotier-one:zerotier-one↵
↳ /var/lib/zerotier-one/token
sudo chmod 600 /var/lib/↵
↳zerotier-one/token
```

Laden Sie nun das Installationsarchiv von ZeroNSD mit `wget` herunter und installieren Sie es mit `dpkg`; setzen Sie gegebenenfalls anstatt der Version 0.5.2 die aktuelle ZeroNSD-Version ein:

```
wget https://github.com/zerotier/↵
↳zeronsd/releases/download/v0.5.2/↵
↳zeronsd_0.5.2_amd64.deb
sudo dpkg -i zeronsd_0.5.2_amd64.deb
```

Im nächsten Schritt konfigurieren Sie ZeroNSD und legen für den automatischen Start ein systemd unit file an. Dabei teilen Sie ZeroNSD die für das Netz gedachte Domain sowie die Netz-ID mit. Bei internen Domains sind keine Endungen erlaubt, die im Internet verwendet werden, und auch „local“ nicht, weil das von mDNS belegt ist. Stattdessen kann man aber „lokal“ nehmen, oder „daheim“. Wir verwenden im Beispiel „kleintier.zoo“ und die abgekürzte Netzwerk-ID 4242caac. Ersetzen Sie sie im folgenden Befehl durch Ihre Domain und Ihre Netzwerk-ID:

```
sudo zeronsd supervise -t↵
↳ /var/lib/zerotier-one/token -w -d↵
↳ kleintier.zoo 4242caac
```

Der Befehl erzeugt einen Dienst mit dem Namen zeronsd gefolgt von der Netzwerk-ID. Mit dem üblichen systemctl wird der Dienst aktiviert und gestartet; setzen Sie wiederum Ihre Netzwerk-ID ein:

```
systemctl daemon-reload
sudo systemctl enable zeronsd-4242caac
sudo systemctl start zeronsd-4242caac
```

Testen Sie mit dem Ping-Befehl, ob das Übersetzen der Domainnamen in IP-Adressen funktioniert. Setzen Sie dabei einen im Dashboard eingetragenen Clientnamen sowie die Domain ein, die Sie konfiguriert haben:

```
ping katze.kleintier.zoo
```

## ZT-Router

In der bisher geschilderten Konfiguration sind lediglich ZeroTier-Clients miteinander verknüpft. Mit kleinen Tricks greift man aber auch auf Netzwerke dahinter zu. Wir haben das mit einem Raspi ausprobiert. Dazu trägt man die Route zum entfernten Netz im Dashboard ein. Ein Beispiel steht im Screenshot rechts.

Dabei teilt man Clients mit, dass das Subnetz 192.168.0.0 über den ZeroTier-Client 192.168.196.54 erreichbar ist. ZeroTier sendet die neue Route umgehend an die Clients. Dabei springt die Anzeige der Route kurz auf Rot und dann wieder auf Schwarz, wenn die Clients aktualisiert sind. Das Zurücknehmen von Routen klappte in einem Fall nicht; die Anforderung setzte die Zentrale erst nach Aus- und Einloggen um.

Das restliche Routing richtet man auf dem Raspi ein, auf dem ein ZeroTier-Client im betreffenden Netz läuft. Schalten Sie dort die Paketweiterleitung ein:

```
sudo sysctl -w net.ipv4.ip_forward=1
```

Öffnen Sie mit `sudo nano` die Datei `/etc/sysctl.conf`, um diese Einstellung fest einzutragen. Entfernen Sie dafür das Raute-Zeichen # vor dieser Zeile:

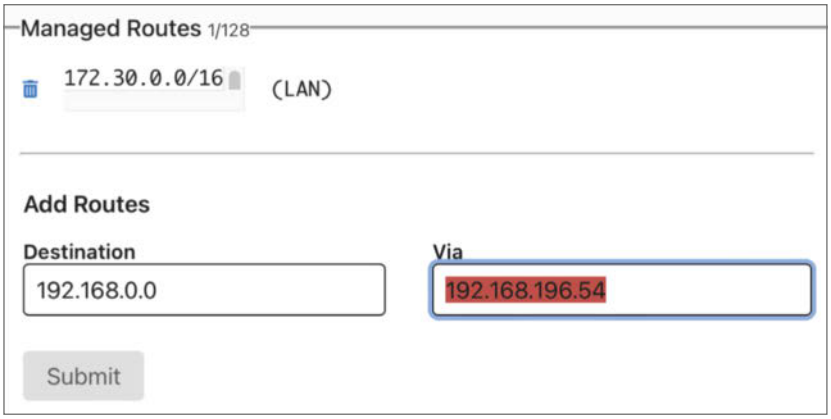
```
net.ipv4.ip_forward=1
```

Lesen Sie in der Ausgabe von `ip a` die Interfacenamen des aktiven Ethernet- und des ZeroTier-Interfaces aus. Unsere Beispiele lauten ens3 und ztr4nx3mbw.

Tragen Sie beide als Shell-Variablen ein, indem Sie in das Terminal tippen (ersetzen Sie ens3 und ztr4nx3mbw durch die Interfacenamen Ihres Raspi):

```
PHY_IFACE=ens3; ZT_IFACE=ztr4nx3mbw
```

Die Routingregeln setzt die Linux-Firewall um, die man zum Beispiel mit iptables konfiguriert. Dafür installiert man `iptables` auf dem Raspi:




**Um beispielsweise mit einem Raspi auf das gesamte Heimnetz zuzugreifen, richtet man im ZeroTier-Dashboard zunächst eine statische Route ein.**

```
sudo apt install iptables
```

Die Routingregeln lauten:

```
sudo iptables -t nat -A POSTROUTING↵
↳ -o $PHY_IFACE -j MASQUERADE
sudo iptables -A FORWARD -i↵
↳ $PHY_IFACE -o $ZT_IFACE -m state↵
↳ --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i $ZT_IFACE↵
↳ -o $PHY_IFACE -j ACCEPT
```

Speichern Sie sie mit iptables-persistent, damit sie bei Neustarts automatisch aktiviert werden:

```
sudo apt install iptables-persistent
sudo bash -c iptables-save >↵
↳/etc/iptables/rules.v4
```

Ist alles erledigt, bringen Sie einen ZT-Client per Mobilfunk ins Internet, sodass er vom Zielnetz entfernt ist und testen Sie per Ping, ob er das Zielnetz über ZeroTier erreicht. Wenn das Netz den Adressbereich 192.168.178.x belegt, dann kann man den zugehörigen Router mit diesem Befehl anpingen:

```
ping -c3 192.168.178.1
```

## Clientunterschiede

Die Clientimplementierungen sind teils sehr unterschiedlich, wobei die Smartphoneclients den Desktopvarianten hinsichtlich des Funktionsumfangs hinterherhinken.

Der Android-Client lag Anfang 2023 mit der Version 1.8.9-1 noch etwas hinter der Entwicklung anderer Implementierungen zurück. Im Sommer lieferte ZeroTier aber die Version 1.10.6-2 aus, mittels der auch Androids ihren gesamten Verkehr durch den ZT-Tunnel zu einem Gateway leiten können. Damit kann der ZeroTier-Client auch Android-Smartphones in unbekannten WLAN-Hotspots schützen.

Der iOS-Client, Version 1.8.10, kann das Gerät zwar wie Android „Bei Bedarf verbinden“ und auch den gesamten Verkehr über ein ZT-Gateway tunneln – aber nur mit IPv4.

Der macOS-Client (zerotier-cli 1.10.6) arbeitete im Test überwiegend zuverlässig. Bei schnellen Wechseln zwischen Ethernet und diversen WLANs verhaspelte er sich aber gelegentlich und baute keinen funktionierenden Tunnel auf. Ein Neustart des Macs behob das Problem.

**ZeroTier-Projekt, Security-Audit, Full-Tunnel-Konfiguration**

**ct.de/wjnp**

## Sicherheitscheck

Das jüngste Security-Audit für ZeroTier stammt von 2020 und erweckt zunächst Vertrauen. Bei genauem Lesen wird dann klar, dass ZeroTier nicht uneingeschränkt empfehlenswert ist.

Doch ZeroTier hat später die Verschlüsselung auf Salsa20-Poly1305 modernisiert. Überdies schrieben die Auditoren der Firma Trail of Bits zuvor: „Insgesamt macht das Protokoll einen guten Eindruck, es dürfte gut gegen viele Netzwerkattacken geschützt sein – wenn es so implementiert wurde, wie gegenüber Trail of Bits beschrieben.“ Das heißt im Klartext aber: Die Autoren haben nur die Spezifikation geprüft und nicht den Code.

Das ist jedoch noch keine rote Ampel. In vielen Unternehmen laufen Closed-Source-Anwendungen mit Internetzugang, ohne jemals von unabhängiger Stelle geprüft worden zu sein. Beispiele sind Microsofts Skype und Teams, die beide Bildschirme freigeben können und deren Backends riesige Benutzerdatenbanken enthalten – da winkt so wie bei ZeroTier reiche Beute, falls ein Einbruch gelingt. Teams beherbergt zudem Office-Dateien und andere unternehmenskritische Daten. Wer solche Anwendungen als vertrauenswürdig einschätzt, kann auch ZeroTier verwenden.

## Fazit

Mit ZeroTier gelingt die Vernetzung von entfernten Geräten spielend leicht. Anschließend kann man sich auf die Aufgaben konzentrieren, die man erledigen wollte: Geräte fernwarten, Dokumente von der Firma aus daheim ausdrucken, Verwandten und Freunden über Bildschirmfreigaben in den Sattel helfen – was immer man mit einem Weitverkehrsnetz anstellen will. (dz) c't

Bild: www.freepik.com

# Google One VPN für PCs und Smartphones

**Wenn ein großer Konzern einen VPN-Dienst für Mobil- und Desktopplattformen zum Privatsphärenschutz anbietet, ist das normalerweise ein positives Zeichen. Aber es ist ausgerechnet Google, weshalb wir der Frage nachgegangen sind, wie gut die Datenkrake Kundendaten vor anderen, aber auch vor sich selbst schützt.**

Von **Dušan Živadinović**

Google bietet mit seinem „One VPN“ einen fortgeschrittenen Internetdienst zum Schutz der Privatsphäre in Netzwerken unbekannter Vertrauenswürdigkeit, also etwa Hotspots in Restaurants, auf Flughäfen oder im Ausland (one.google.com/benefits). Der Dienst erinnert an Apples „Private Relay“, der wie One VPN die IP-Adresse des Nutzers verbirgt und dessen Datenverkehr auf dem Weg zum Tunnelausgang vor Mitlesern durch Verschlüsselung schützt. One VPN kostet in Kombination mit mindestens 100 GByte Cloudspeicher ab 2 Euro pro Monat.

Anders als Private Relay, das auf iOS und macOS nur Apple-Anwendungen schützt, schleust One VPN sämtlichen Verkehr des Clients durch den Tunnel. Implementierungen für Android und iOS sind seit Längerem erhältlich, seit Ende 2022 auch für macOS und Windows. Auf aktuellen Pixel-Smartphones läuft

der Dienst gratis. Bis zu sechs Geräte und fünf Familienmitglieder dürfen das VPN weltweit gleichzeitig nutzen.

## Trotz Nulltarif-VPN

Das Angebot klingt gut, verwundert aber auch, denn es gibt ja eine Schutztechnik zum Nulltarif: Man verbindet sein Smartphone oder Notebook einfach per VPN mit dem Heimrouter oder -server. Der Schutzeffekt ergibt sich daraus, dass die Daten auf dem Weg nach Hause im Tunnel bleiben (z. B. IPsec, WireGuard, OpenVPN) und anschließend über den vom Nutzer gewählten Internetanbieter zum Ziel kommen. Dabei gelten deutsche Provider als vertrauenswürdig. Nachteilig ist, dass die Datenpakete der Clients je nach Position im Internet weiter reisen müssen als ohne den Umweg nach Hause, sodass sich etwa Webseiten langsamer aufbauen.

Wohl weil es bequemer einzurichten ist, buchen viele Anwender kommerzielle VPN-Angebote etwa von NordVPN. Manchen kommt gelegen, dass einige VPN-Anbieter helfen, Geoblocking von Netflix oder HBO zu umgehen, indem sie den Tunnelausgang in eine vom Streaminganbieter geduldete Region legen, also etwa in die USA.

Dabei ist die Branche skandalumwittert: Manche Anbieter haben ihren Sitz in Steueroasen oder werden gleich im halben Dutzend von einer einzigen chinesischen Firma kontrolliert. Auch sind Fälle von Datenhandel bekannt, obwohl fast alle versprechen, nicht zu erfassen, welche Ziele ihre Kunden im Internet ansteuern. So scheint auch Google als weltgrößte Datenkrake auf den ersten Blick gut in dieses dubiose Umfeld zu passen.

Aber der Schein trügt, denn Google trennt die Authentifizierung der Kunden von deren Surfverkehr kryptografisch mittels „RSA Blind Signatures“, sodass sich Surfprotokolle keinem Kunden zuordnen lassen. Die Technik entwickelte David Chaum schon 1983 (siehe ct.de/wvas). Sie erlangte Bekanntheit zunächst in elektronischen Wahlmaschinen. Dort gewährleisten Blind Signatures, dass nur registrierte Wähler zum Zug kommen, aber niemand erfährt, welchen Kandidaten sie wählen. Dasselbe Konzept nutzt Apple mit Private Relay. Gleich zwei Überprüfungen eines unabhängigen Sicherheitsunternehmens bescheinigen Googles Implementierung, dass sie wie gedacht funktioniert und vertrauenswürdig ist (siehe ct.de/wvas).

Wir haben den Dienst auf aktuellen Versionen von Android, iOS, macOS und Windows getestet und


**Googles VPN-App sieht man nicht an, welch großen Aufwand der Konzern treibt, um die Privatsphäre der Nutzer zu schützen. Danach bleiben nur anonyme Daten übrig, die Google aber, wenig überraschend, aggregiert verwertet.**

konnten dabei tatsächlich unterschiedliche Server von Google identifizieren. Die meisten Infos ließen sich der macOS-Implementierung entlocken, daher hier eine Zusammenfassung: Die App hält zwei HTTPS-Verbindungen zu Google-Servern offen (z. B. fra24s01-in-x0a.1e100.net). Im Terminal kann man sie sich zum Beispiel mit `sudo lsof -iTCP | grep VPN` anzeigen lassen. Die Nutzdaten verschlüsselt und tunnelt die Netzwerkerweiterung com.google.one.NetworkExtension. Weitere Details liefert der Befehl `scutil`. Damit liest man zunächst die Service-ID aus (z. B. 818E657B-CEA2-42C2-9C42-0C24E5592F42):

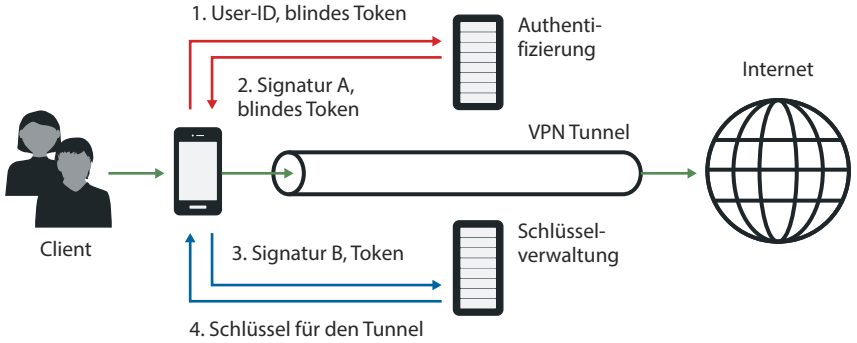
```
scutil --nc list | grep google
```

Dann zeigt die Status-Option weitere Details:

```
scutil --nc status 818E657B-CEA2-42C2-9C42-
0C24E5592F42
```

## Das Konzept von Googles One VPN

Google trennt für sein VPN-Angebot die Authentifizierung kryptografisch mittels zwei Servern (Authentifizierung und Schlüsselverwaltung) vom Tunnelverkehr des Anwenders. So lässt sich nicht erfassen, welche Ziele VPN-Nutzer im Internet ansteuern.




In der langen Befehlsausgabe stecken bei aktiviertem VPN Adressen verschiedener Google-Server, zu denen die App Verbindungen aufbaut. Darunter sind Googles Broadband Remote Access Server (BRAS), aber auch komplette URLs zur Authentifizierung und Schlüsselverwaltung (prod.zinc.cloud.cupronickel.goog/publickey und prod.zinc.cloud.cupronickel.goog/auth). Welche Rolle die Server spielen, hat das Security-Unternehmen NCC dokumentiert (ct.de/wvas).

## Schnell und sauber

In Analysen mit dem Netzwerkwerkzeug Wireshark kam heraus: Googles App stellt wie gewünscht sicher, dass DNS-Anfragen durch den Tunnel gehen. So können angefragte Surf-Ziele keinem Nutzer nachträglich zugeordnet werden. Jedoch nutzt One VPN auf Windows den im Betriebssystem konfigurierten DNS-Resolver. Webseiten, die diese Info auslesen, können auf die Zugehörigkeit des Nutzers zu einem Netzwerk rückschließen, also etwa zu einer Firma. Android, iOS und macOS nutzen hingegen Googles Resolver. Wer Wireshark zu kompliziert findet, kann Webdienste wie dnsleaktest.com nutzen. Bei unseren Geschwindigkeitsmessungen schnitt One VPN gut ab; mit der App ließ sich ein VDSL-Anschluss mit 243 Mbit/s in Empfangs- und 30 Mbit/s in Senderichtung voll auslasten. Google verspricht Durchsatzraten über 300 Mbit/s.

Die Paketlaufzeiten etwa zu Zielen in Deutschland und Europa liegen auf gleichem Niveau wie ohne den Tunnel (20 bis 60 ms). Das entspricht den Erwartungen, da Google seine Tunnelausgänge weltweit in die Datendrehkreuze legt, sodass die Signalwege oft dieselben sind. Da Google außerdem immer den nächstgelegenen Tunnelausgang wählt, schneidet der Dienst im Ausland in puncto Paketlaufzeit deutlich besser ab als der heimische VPN-Router, der nicht mitreisen kann.

Die App gibt sich auf Windows und macOS spartanisch: Man kann nur einstellen, ob die Software beim Booten mitstarten und den Tunnel automatisch aufbauen soll. Im Test scheiterte der Tunnelaufbau manchmal, aber stets ohne Fehlerangabe. Nach einem Neustart der App klappte es wieder.

Baut man auf macOS einen anderen Tunnel auf (etwa per WireGuard zur Firma), dann schaltet sich One VPN automatisch ab. So soll es sein. Aber nach Ende schaltet es sich nicht automatisch wieder ein (was Apples Private Relay durchaus macht), sodass es leicht passieren kann, dass man ohne VPN-Schutz weitersurft. Aber folgender Trick klappte meistens: Anstatt nach der Firmensitzung WireGuard zu be-

enden, startet man einfach den One-VPN-Tunnel. Dann beendet macOS den WireGuard-Tunnel selbstständig, bevor sich der Google-Tunnel öffnet.

## Schluckauf

Auf Windows sieht man den Tunnelstatus nur, wenn man die Task-Leiste öffnet. Auch wird One VPN nicht beendet, wenn man ein anderes VPN parallel startet; in der Folge scheitert die Internetkommunikation, bis man den zweiten Tunnel schließt. Das virtuelle Netzwerk-Interface steckt im Netzwerk- und Freigabecenter. Es liefert in gewohnter Windows-Manier Angaben zu IP-Adressen, Verbindungsdauer und Durchsatz.

Auch auf Windows klemmte der Tunnelaufbau gelegentlich. In diesem Zustand funktionierte der Internetzugriff gar nicht, weil One VPN den Verkehr schon in den Tunnel lenkt, der Tunnelausgang aber blockiert ist – Fehlermeldung Fehlanzeige.

Der Funktionsumfang des iOS-Clients ist ebenso dürftig wie der von macOS und Windows. Auf Android kann man zusätzlich einzelnen Apps genehmigen, den Tunnel zu umgehen und One VPN blockiert den Internetverkehr auf Wunsch, wenn der Tunnel nicht aufgebaut ist. Zu beachten ist, dass AdBlocker wie Blokada nicht gleichzeitig laufen können. Sie sind auf Android und iOS ebenfalls als VPN-Anwendungen deklariert, und von diesen darf immer nur eine auf das jeweilige VPN-API zugreifen.

**Downloads, Security-Audits**

ct.de/wvas

## Fazit

Insgesamt kann man sagen: Das Konzept ist vorbildlich, an der Umsetzung sollte Google aber noch feilen. One VPN ist so gut gelungen, dass es den Konzern trotz seines Sammeleifers in besserem Licht erscheinen lässt – vielleicht gibt es dieses Tool gerade deshalb. Zum guten und vertrauenswürdigen Eindruck tragen die unabhängigen Sicherheitsprüfungen sowie die quelloffenen Bibliotheken maßgeblich bei. Anbieter von Billig-VPNs können da nicht mithalten und kommen bestenfalls infrage, um Geoblockaden zu umgehen. (dz) c't

# Vorschau: c't KI-Praxis

**Ab 24. November im Handel und auf ct.de**

**Mit Künstlicher Intelligenz produktiv arbeiten**

Im Sonderheft c't KI-Praxis finden Sie Tests und praktische Anleitungen für die Arbeit mit Sprach-KIs. Sie erfahren, warum Sprachmodelle Fehler machen und wie Sie sie verringern können. Dies hilft Ihnen nicht nur, wenn Sie Ihre Fragen und Aufträge an einen der online angebotenen Chatbots übermitteln.

Wollen Sie beispielsweise aus Datenschutzgründen die Cloud-Dienste lieber vermeiden, können Sie auch Ihre eigene Sprach-KI nutzen. Wir erklären, wo Sie ein geeignetes Sprachmodell finden, wie Sie es lokal selbst hosten oder bei welchen Dienstleistern Sie es hosten können.

Dass generative KI immer produktiver einsetzbar ist, birgt Chancen und Risiken zugleich. Um Chancen zu nutzen und Risiken zu minimieren, helfen geeignete Spielregeln für den KI-Einsatz in Schule, Ausbildung und Beruf.

**Weitere Infos: ct.de/waqh**

## Themenschwerpunkte

**Die eigene Sprach-KI betreiben**
- Mit offenen Sprachmodellen experimentieren
- Open-Source-Sprach-KIs ohne Cloud betreiben
- KI-optimierte Server vom Hosting-Provider nutzen

**Grenzen der Sprachmodelle erkennen**
- Warum Sprachmodelle Fehler machen
- KI-Training: Was Sprachmodelle lesen
- KI-Fehler erkennen und verringern

**Sprachmodelle anwenden**
- Was ChatGPT-Plug-ins können
- Wie ChatGPT beim Programmieren hilft
- Test: SoftMaker Office 2024 und NX mit KI-Anbindung
- Mit der Sprach-KI Forschungsarbeiten sichten

**Bilder und Audio bearbeiten**
- Künstlerische Stile mit Midjourney simulieren
- Fake-Bilder in News erkennen
- Text-to-Speech: Anbieter von KI-Stimmen im Test
- Whisper wandelt Gesprochenes in Text um

**Regeln für Schule und Arbeit**
- Wie KI den Arbeitsmarkt verändern könnte
- Das Ringen um kluge Regeln für KIs
- Wie sich KI in der Bildung etabliert
- KI-Richtlinien im Unternehmen aufstellen

c't WORKSHOP

# WIR TEILEN KEIN HALBWISSEN
# WIR SCHAFFEN FACHWISSEN


## Dienste mit SELinux absichern

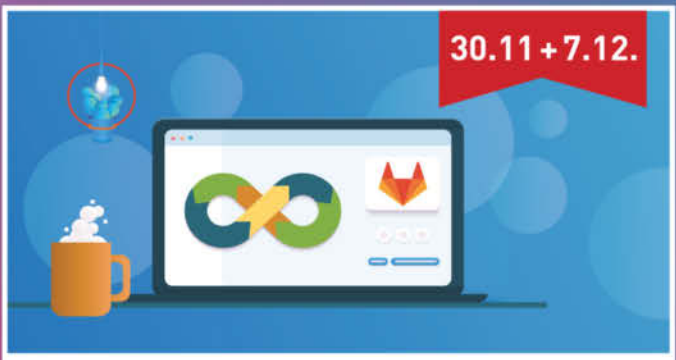
SELinux einfach abzuschalten, wenn es Probleme gibt, ist üblich, aber unklug. Der Workshop zeigt, wie man das System stattdessen so nutzt, dass alles besser abgesichert ist und trotzdem funktioniert.


## Einführung in GitLab

Der Workshop bietet einen Einstieg in den Betrieb einer eigenen Gitlab-Instanz. Sie lernen GitLab initial aufzusetzen, sowie Ihre Instanz zu konfigurieren und an eigene Anforderungen anzupassen.


## Docker und Container in der Praxis

Der Workshop richtet sich an Entwickler und Administrierende, die neu in das Thema einsteigen. Neben theoretischem Wissen über Container geht es um eigene Container-Erfahrungen.




## CI/CD mit GitLab

Der zweitägige Workshop bietet eine praktische Einführung in die GitLab-CI-Tools und zeigt, wie man damit Softwareprojekte baut, testet und veröffentlicht.

**Sichern Sie sich Ihren Frühbucher-Rabatt:**

**www.heise.de/ct/Events**

# Ihr Erste-Hilfe-Set:

## Das Notfall-System für den Ernstfall

**GRATIS:** Signatur-Updates bis Oktober 2024


NEUE VERSION 2023/24

**Komplett auf 32 GByte USB-Stick.** Desinfec't startet direkt vom Stick.

**Auch als Heft + PDF mit 28 % Rabatt**

**Mit den Virenscannern des Sicherheitstools** jagen Sie PC-Schädlinge, retten Ihre Daten und können auch gelöschte Daten wiederherstellen – ganz kinderleicht. Das und noch mehr bringt Ihnen **c't Desinfec't 2023/24:**

- ► DAS c't-Sicherheitstool als Download für USB-Sticks
- ► Windows-Trojaner & andere Schädlinge finden und löschen
- ► Verloren geglaubte Fotos und Dateien finden und wiederherstellen
- ► Daten aus defektem NAS bergen
- ► Für Profis: Malware-Analyse mit Experten-Tools

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 € • Desinfec't-Stick 19,90 €

**shop.heise.de/desinfect23**