

Bundesnetzagentur für Elektrizität, Gas,
Telekommunikation, Post und Eisenbahnen
Abteilung 4
Referat 461
Tulpenfeld 4
53113 Bonn

02.06.2023

Netzabschlusspunkt bei PON

Sehr geehrter Herr Marwinski, sehr geehrter Herr Hopp,

namens der unterzeichnenden Verbände und Unternehmen möchten wir uns noch einmal für das sehr konstruktive Gespräch zum Thema „Netzabschlusspunkt bei PON“ am 24.02.2023 in Ihrem Hause bedanken. Wir glauben, dass im Verlaufe des Gesprächs deutlich geworden ist, dass es sich um eine sehr komplexe Materie handelt, die einer sorgfältigen Aufarbeitung und Bewertung bedarf. Insbesondere möchten wir diese Gelegenheit noch einmal nutzen, um erneut herauszustellen, dass das Ziel der geführten Diskussion darin besteht, eine technologie- und topologiegerechte Definition des Netzabschlusspunktes für PON zu finden, nicht jedoch darin, in irgendeiner Art und Weise die Hoheit über Router den Netzbetreibern zuzuweisen. Es ist aus unserer Sicht völlig unstrittig, dass Router als Telekommunikationsendgeräte zu qualifizieren sind, für welche eine uneingeschränkte Wahlfreiheit der Endkunden besteht. Konkret bedeutet das: Endnutzer können jeden technisch geeigneten Router Ihrer Wahl hinter dem vom Provider gestellten ONT anschließen, z. B. im Bridgmodus. Wir legen daher Wert auf die Feststellung, dass wir die Routerwahlfreiheit respektieren und uns für einen kontrollierten, aktiven Netzabschlusspunkt in Glasfasernetzen einsetzen.

Am Ende des Termins haben wir eine Reihe von (vor allem technischen) Fragen der BNetzA mitgenommen, die wir im Folgenden gerne beantworten, um die Diskussion weiter zu strukturieren und voranzubringen.

Hinsichtlich der grundlegenden juristischen Aspekte dürfen wir dabei auf unsere ausführliche Darstellung in unserem Schreiben vom 09.06.2022 verweisen, das wir als Anlage nochmals beifügen. Sollte es diesbezüglich noch weitere Fragen oder Anmerkungen Ihrerseits geben,

können wir diese aber gerne aufgreifen. Insbesondere aber stellen wir ausdrücklich klar, dass die im Schreiben vom 09.06.2022 enthaltenen Anträge auch förmlich gestellt werden:

Es wird beantragt,

1. festzustellen, dass in Passiven Optischen Netzen (PON) der Netzabschluss nach dem ONT und vor einem Router o. ä. zu verorten ist;
2. hilfsweise festzustellen, dass in Passiven Optischen Netzen (PON) der Netzabschluss in Anwendung des § 73 Abs. 2 TKG ausnahmsweise nach dem ONT und vor einem Router o. ä. zu verorten ist sowie
3. höchst hilfsweise festzustellen, dass in Passiven Optischen Netzen (PON) diejenigen Geräte zum Telekommunikationsnetz gehören, welche vor dem – aus Netzsicht – ersten für den Internetzugangsdienst (per IP-Adresse) adressier- und identifizierbaren Gerät liegen.

Insoweit bitten wir um Einleitung eines förmlichen Verfahrens, in dem wir gern für weitere Diskussionen und Erläuterungen zur Verfügung stehen.

Zu den einzelnen Punkten aus dem Termin vom 24.02.2023 geben wir nachfolgend detaillierte Antworten und Informationen.

Inhalt

I.	Absicherung gegen Störungen.....	4
II.	Besonderheiten von PON gegenüber VDSL oder Kabel.....	5
1.	Unterschiede von PON zu VDSL-Netzen	5
a.	Unterschiede in der Funktionsweise	6
b.	Unterschiede in den Sicherheitsaspekten.....	8
c.	Unterschiede bei der Zugangsgewährung.....	12
2.	Unterschiede von PON zu Kabelnetzen	13
III.	Fallbeispiele für Störungen.....	15
IV.	Einzelne Aspekte aus der Stellungnahme des VTKE	17
1.	Standardisierung.....	18
2.	Auf dem Markt erhältliche Geräte.....	20
3.	Störungsfreiheit und Netzstörungen	22
V.	Schlechterbringung von Diensten (QoS-Verluste)	22
1.	QoS-Sicherung	23
a.	QoS-Sicherung im Upstream	24
b.	QoS-Sicherung im Vorleistungsverhältnis	25
2.	Behebung von QoS-Verlusten.....	26
3.	Folgen von QoS-Verlusten	26
a.	Leistungsstörung beim Endnutzer selbst.....	26
b.	Leistungsstörung bei anderen Endnutzern.....	29
VI.	Folgen der beantragten Festlegung des Netzabschlusspunkts.....	31
1.	Den Endkunden verbleibende Funktionalitäten.....	31
2.	Auswirkungen auf den Innovationsdruck	33

I. Absicherung gegen Störungen

Die PON-Standards sehen eine Möglichkeit der Absicherung gegen Störungen grundsätzlich vor, wobei darauf hinzuweisen ist, dass die Abschaltung eines ganzen OLT kaum wahrscheinlich erscheint, da hierfür direkt auf die Systemebene des OLT Zugriff genommen werden müsste. Von störenden ONT geht jedoch – wie unten näher erläutert wird – die Gefahr der Abschaltung eines OLT-Ports und damit eines Kundensektors aus.

In der Praxis können verschiedene OLT-Varianten denn auch unter gewissen Umständen störende ONT (z. B. Rogue ONT) erkennen. Hierfür ist es jedoch Bedingung, dass die Störung so früh erkannt wird, dass eine Abschaltung überhaupt noch möglich oder sinnvoll ist. Eine Störung, die so weit fortgeschritten ist, dass sie keinerlei Übermittlung von Signalen mehr erlaubt, wird auch das Anbringen von Steuersignalen zum Trennen der Verbindung oder Abschalten (Herunterfahren) des ONT verhindern.

Das heißt insbesondere, dass der betreffende ONT-Hersteller sowie dessen Firmware-Version bekannt sein müssen, um anhand von bekannten Mustern rechtzeitig Gegenmaßnahmen einzuleiten. Die Implementierung entsprechender Störungsmuster ist indes nichts, was einfach zu erreichen wäre. Selbst wenn ein bestimmtes Fehlermuster für einen bestimmten Störfall bekannt ist, werden bereits ein anderer Chipsatz, eine andere Firmwareversion oder ein anderes OLT mit hoher Wahrscheinlichkeit ein völlig anderes Störungsmuster erzeugen. Demzufolge können entsprechende Muster nur im Rahmen der sog. Interoperabilitätstests (s. dazu detaillierter unten) aufgeklärt und zur Störungserkennung hinterlegt werden und müssen dann im praktischen Einsatz weiter ausgebaut und verfeinert werden. Aber auch dies geschieht nur im Rahmen eines fortschreitenden Prozesses, da ein solcher definierter Test Fehlerfälle simulieren muss, die eigentlich nicht auftreten sollten. Künstlich geeignete Fehler herbeizuführen ist zwar möglich, wenn man zu den theoretischen Fehlerszenarien noch grundlegende praktische Erfahrungen gesammelt hat; dennoch darf man zum heutigen Zeitpunkt davon ausgehen, dass noch lange nicht genügend Fehlerfälle bekannt sind, um simuliert zu werden und entsprechende Fehlermuster erstellen zu können.

Wenn eine Störung auf diese Weise rechtzeitig erkannt ist, besteht eine hohe Chance, dass eine Trennung oder Abschaltung eines ONT vom OLT herbeigeführt werden kann – vorausgesetzt natürlich, dass die entsprechende Funktion im ONT ordnungsgemäß implementiert ist und das ONT für den Netzbetreiber mit einem steuernden Zugriff erreichbar ist (was eine entsprechende Rechtevergabe durch den Endnutzer bedingt).

Ohne die entsprechenden Informationen oder bei falschen Informationen zu Hard- und Software, wie sie durch fehlerhafte Konfiguration oder Firmware von Drittanbietern ("custom firmware") durchaus übermittelt werden können, kann der Mechanismus nicht alle Störungen erkennen. Auch dann ist eine Trennung oder Abschaltung zwar grundsätzlich möglich, jedoch müssen die entsprechenden Steuersignale auch zum ONT gelangen und dort richtig

interpretiert und ausgeführt werden. Die Wahrscheinlichkeit für Letzteres ist bei Geräten, für die keine Interoperabilitätstests durchgeführt wurden, indes als gering einzustufen.

II. Besonderheiten von PON gegenüber VDSL oder Kabel

Die von der BNetzA aufgeworfene Frage nach den für die vorliegende Frage relevanten Unterschieden zwischen PON auf der einen Seite und VDSL- und Kabelnetzen auf der anderen Seite ist sowohl nach technisch-topologischen (und damit auch rechtlich bedeutsamen) Kriterien als auch nach praktischen Kriterien zu beantworten. Kurz gefasst besteht dabei der wesentliche Unterschied zu VDSL-Netzen darin, dass VDSL-Netze ausschließlich als Point-to-Point-Topologie betrieben werden, während PON wie Kabelnetze eine Point-to-Multipoint-Architektur aufweisen. Ein weiterer Unterschied zu PON besteht darin, dass DSL-Netze nie als Multi-Service-Access-Technologie definiert wurden, also weder besondere QoS-Features kennen noch auf Anbindung anderer Services (Backhauling) ausgelegt sind. Das wird insbesondere beim Einsatz der Vectoring-Technologie problematisch, wo eine individuelle Adressierung des einzelnen Endkunden weiterhin den typischen Mechanismen der Point-to-Point-Netze unterliegt, die QoS-Absicherung aber ein enges Zusammenwirken mehrerer Endkunden erfordert, wie es für Point-to-Multipoint-Netze typisch ist.

Der wesentliche Unterschied zu den Kabelnetzen hingegen fließt aus den praktischen Gegebenheiten, dass für letztere eingespielte und weltweit akzeptierte Mechanismen sowie in langjähriger Arbeit entwickelte Standards eine Interoperabilität und Fehlerabsicherung ermöglichen, was für PON in der Praxis nicht gegeben ist. Eine aktuelle Änderung der Situation ist auch nicht zu erwarten, da der GPON-Standard in absehbarer Zeit das Ende seines Lebenszyklus erreicht hat und nach dem derzeitigen Stand vom XGSPON Standard abgelöst wird.

1. Unterschiede von PON zu VDSL-Netzen

Der zentrale Unterschied zwischen PON und VDSL-Netzen besteht in deren Topologie.

PON-Topologien setzen definitionsgemäß eine Point-to-Multipoint-Architektur voraus. Das bedeutet, dass sich alle Endkunden, die am OLT über einen Port angebunden sind, dieses Anschlussnetz teilen (shared medium). Das bedeutet zugleich, dass im Downstream alle Endkunden eines Segmentes die gleichen Signale erhalten und die Endgeräte entscheiden, welche Signale bei den jeweiligen Endkunden sichtbar werden, während im Upstream eine ausgehandelte Ressourcenaufteilung (zeitliche Aufteilung) für die Inanspruchnahme der Transportkapazitäten erfolgen muss. Dies lässt sich grafisch wie folgt verdeutlichen:



Abb. 1: Grundlegende Struktur eines Point-to-Multipoint-Netzwerkes [Bild: J. Dombrowski]

Demgegenüber erfordern VDSL-Netze eine Point-to-Point-Struktur, d. h. dort besteht im Anschlussnetz immer eine 1:1-Beziehung zwischen dem Anschluss des Endkunden und dem nächsten Netzelement (DSLAM). Jeder Endkunde hat also eine eigene, exklusive Leitung. Grafisch lässt sich dies wie folgt darstellen:

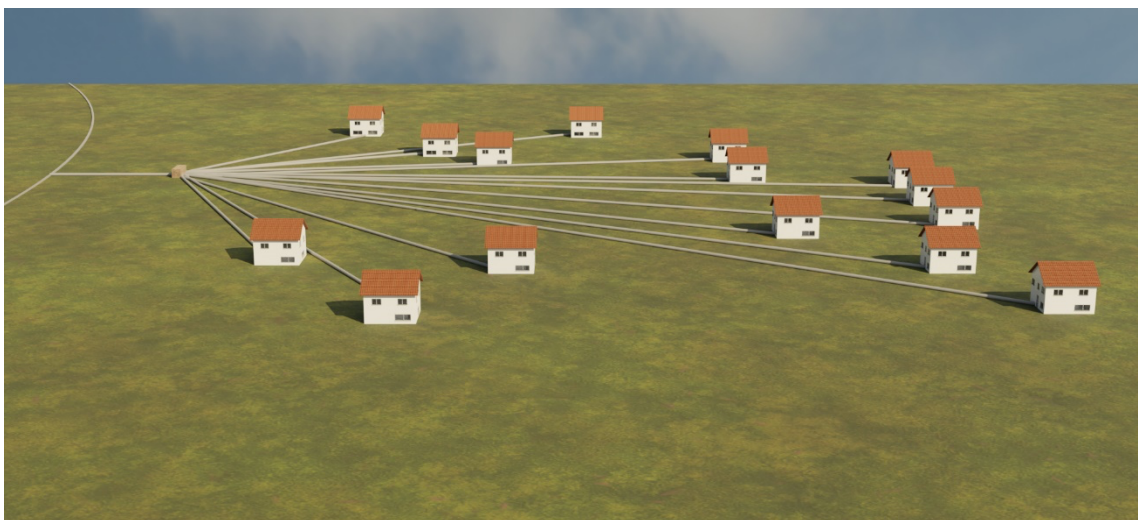


Abb. 2: Grundlegende Struktur eines Point-to-Point-Netzwerkes [Bild: J. Dombrowski]

Dieses zentrale Kriterium ist Grundlage für mehrere bedeutsame Folgerungen, die sowohl die Funktionsweise als auch Sicherheitsaspekte betreffen.

a. Unterschiede in der Funktionsweise

Richtet man den Blick auf den Downstream in beiden Netzwerktopologien, wird deutlich, dass in Point-to-Point-Netzen die Bestimmung des Adressaten und damit die Zuordnung der für ihn

bestimmten Daten trivial ist. Aufgrund der exklusiven Leitungsnutzung ist zwingend von der Signalisierung eines Datums auf der Leitung auf dessen Zuordnung zum Endnutzer dieser Leitung zu schließen. Eine individuelle Kommunikationsbeziehung und Adressierung lässt sich hier also durch die physische-passive Existenz der Leitung herstellen.

Da sich in Point-to-Multipoint-Netzen mehrere Endnutzer eine Leitung teilen und die gleichen Signale erhalten, liegt auf der Hand, dass die Herstellung einer individuellen Kommunikationsbeziehung und Adressierung nicht auf die gleiche physisch-passive Weise erreicht werden kann, wie bei Point to Point Netzen. Vielmehr muss eine Logik hinzutreten, welche für einen letzten, Endnutzer-exklusiven Leitungsabschnitt eine Filterung eingehender Signale vornimmt. Diese Aufgabe übernehmen in PON die adressierbaren ONT. Die ONT sind aus Sicht des Netzbetreibers die letzten (netzintern) adressierbaren Netzelemente und die einzigen, an denen sich die individuelle Kommunikationsbeziehung des Netzbetreibers zu einem Endkunden festmachen lässt.

Umgekehrt bekommt in PON nur der Router eine eigene IP-Adresse zugewiesen, während das ONT keine erhält. Aus Sicht des Internetdienstes bleibt das ONT mangels IP-Adresse damit „unsichtbar“ und wird nur vom Netz selbst über seine Seriennummer adressiert. Es ist damit Bestandteil des „Weges zum Endkunden“ – also Netzbestandteil – und liegt nicht im Heimnetz (also im Machtbereich des Endkunden).

Legt man zugrunde, dass zu den Aufgaben eines TK-Netzwerks immer auch die Adressierung des Endnutzers und damit die Herstellung der individuellen Kommunikationsbeziehung gehört¹, lässt sich der wesentliche Unterschied in der Funktionsweise also dahingehend umschreiben, dass die netzwerkspezifische Aufgabe der Adressierung individueller Endkunden in Point-to-Multipoint-Netzen nicht am Beginn des Anschlussnetzes, sondern in größtmöglicher Nähe zum Endkunden durch aktive Zuordnung der eingehenden Signale eines Netzabschlussgeräts erbracht werden muss. Es ist hier also nicht das Anschlussnetz – bzw. das davor geschaltete Netzelement (DSLAM etc.) –, das die Daten anschlusspezifisch verteilt, sondern ein nach dem Anschlussnetz gelagertes Netzelement (ONT etc.).

Auch für die umgekehrte Verkehrsrichtung, also den Upstream, ergibt sich aus den Netztopologien ein bedeutender funktioneller Unterschied. In einem Point-to-Point lässt sich eine ungestörte Übertragung ohne Weiteres auf der zeitlich durchgängig verfügbaren Ressource abbilden. Elektrische Medien wie VDSL-Netze verwenden hierzu dedizierte Frequenzbereiche; aktive Glasfasernetze (AON) nutzen eigene Wellenlängen.

Für Point-to-Multipoint-Netze ist solch ein Mechanismus ungeeignet, da der Vorteil dieser Netze gerade darin liegt, physische Ressourcen nicht-exklusiv zu nutzen, um so die statistische Auslastung zu erhöhen und damit die Wirtschaftlichkeit zu optimieren. Daher muss ein Mechanismus implementiert werden, der bei größtmöglicher Sicherheit eine gemeinsame Nutzung der physischen Ressource ermöglicht, was zu einem Zeitmultiplex führt. Praktisch

¹ Vgl. Art. 2 Nr. 9 EKEK, § 3 Nr. 32 TKG.

bedeutet das, dass jedem Endkunden für seine Senderichtung dezidierte Zeitschlitzte zur Verfügung stehen, die zwar flexibel ausgehandelt werden, naturgemäß aber peinlich genau einzuhalten sind, um keine gegenseitige Beeinflussung der Kundengeräte (CPE) zu verursachen. Insofern müssen Point-to-Multipoint-Netzwerke mit der Aushandlung der Zeitschlitzte auch für den Upstream eine zusätzliche, aktive Aufgabe und einen entsprechenden Kommunikationskanal implementieren. Auch diese Tätigkeit muss nutzerindividuell natürlich dort erbracht werden, wo ein physischer Leitungsabschnitt exklusiv einem Endnutzer zugeordnet werden kann. Sie ist dementsprechend in den ONT verortet.

b. Unterschiede in den Sicherheitsaspekten

Diese wesentlichen funktionalen Unterschiede haben verschiedene Implikationen für die Sicherheit und Stabilität der Netzwerke.

So führt die Exklusivität der Leitungsressource in Point-to-Point-Netzwerken dazu, dass eine Fehlfunktion von endkundenseitigen Geräten praktisch immer auf diese individuelle Kommunikationsbeziehung beschränkt bleibt. Es kann also durchaus vorkommen, dass ein defektes oder ungeeignetes Gerät verhindert, dass der individuelle Dienst erbracht wird. Solange das korrespondierende Netzelement (DSLAM etc.) aber nicht beeinträchtigt wird, was mit geringem Aufwand sicherzustellen ist, bleibt die Störung auf die betroffene Leitung und damit den betroffenen Endkunden beschränkt. Dieser Endkunde ist zudem einfach anhand der gestörten Leitung ermittel- und entstörbar. Wie oben bereits angeklungen, gibt es hier indes eine Ausnahme bei der Vectoring-Technologie, welche ein intensives Zusammenwirken einer bestimmten Menge von Endkunden – bzw. ihrer Modems – erfordert. Ein einzelnes Modem, welche die Mechanismen zur Ermittlung der auftretenden Störsignale nicht, unzureichend oder falsch unterstützt, wird unweigerlich dazu führen, dass die Dienstqualität für alle diese Endkunden sinkt. Dass es insoweit zum Diensteausfall für diese Endkunden kommt, ist indes eher unwahrscheinlich, sodass die Verfügbarkeit als Sicherheitsaspekt nicht unmittelbar bedroht erscheint.

Ganz anders hingegen in Point-to-Multipoint-Netzwerken, wo sich die Probleme praktisch in der Upstream-Verkehrsrichtung manifestieren, also bei den angesprochenen Zeitschlitzten. Bereits eine geringfügige Missachtung der ausgehandelten Zeiten für das eigene Senden von Signalen oder Fehler bei der Aushandlung führen zu gleichzeitigem Senden durch unterschiedliche Endkunden. Die dabei entstehenden Überlagerungen der Signale verhindern nicht nur die Signalzuordnung zum richtigen Endkunden, sondern auch die richtige Signalinterpretation am OLT. Es kommt in der Folge zu Fehlern im Upstream mehrerer Kunden, die grundsätzlich alle Endkunden an einem gemeinsamen Port betreffen können; je nach Netzwerkkonfiguration können dies mehrere Hundert Kunden sein, wobei sich die Zahl jedoch praktisch im Bereich von 32 bis 128 Endkunden bewegen wird. Solche Beeinträchtigungen verbleiben jedoch wegen der Natur des Datenverkehrs nicht im Upstream, sondern erfassen unmittelbar auch den Downstream, da die zuständigen Protokolle (in der Regel TCP/IP) Empfangsbestätigungen (Acknowledge - ACK) erwarten und bei deren Ausbleiben die Sendung der IP-Pakete sukzessive

drosseln bzw. im Extremfall sogar das Senden von Daten einstellen. Ist letzterer Effekt eingetreten, kann das störende Gerät auch nicht mehr zwecks Trennung oder Abschaltung kontaktiert werden, da Datenpakete nicht mehr zu dem betroffenen Endgerät durchdringen. In schweren Fällen, insbesondere bei wiederholten Problemen, kann es jedoch auch nötig sein, die betreffende Karte insgesamt zwecks Fehleranalyse herunterzufahren, was bei Karten aktueller Generation 32 Ports x 64 Nutzer, mithin bis zu 2048 Kunden, erfassen kann.

Es handelt sich hier auch nicht etwa um ein unrealistisches Szenario. Da die zum Senden verfügbaren Zeitschlitze nur wenige Millisekunden groß sind und wegen der Dynamik der Bedarfe bei den Endkunden praktisch in Echtzeit auszuhandeln sind, können solche fatalen Fehler schon bei unsauberer Programmierung der Firmware auftreten – ganz zu schweigen von „custom firmware“, die aus zumeist dubiosen Quellen im Internet bezogen werden kann, für die niemand die Verantwortung übernimmt und die auch keinerlei Interoperabilitätstest unterzogen wird. Angemerkt sei dabei, dass sich diese Aufgabe nicht etwa an die verwendeten Chipsätze delegieren lässt, da die Mechanismen ständigen Weiterentwicklungen unterliegen und auch in einzelnen Netzen unterschiedlich implementiert sein können. Vielmehr ist herauszustellen, dass diesen diffizilen Anforderungen nur durch eine aktuelle und fehlerfreie Programmierung der Firmware sowie entsprechende Tests wirksam begegnet werden kann.

Eine weitere Fehlerquelle für Upstream-Störungen ergibt sich daraus, dass auch Glasfasernetze in Point-to-Point-Architektur (also aktive Glasfasernetze – AON) errichtet werden und daher (insbesondere im Onlinehandel) auch dafür gedachte Geräte auf dem Markt sind. Daneben gibt es auch Geräte mit mehreren Konfigurationsprofilen, welche sowohl mit PON als auch mit AON-Netzen oder anderen Standards wie 10G-EPON zusammenarbeiten können. Schließt man ein für AON-Netze gedachtes Gerät – oder ein auf AON bzw. einen anderen Glasfaserstandard konfiguriertes Gerät – an ein PON an, so würde das Gerät naturgemäß die in der Erwartung einer exklusiven Ressource keine Aushandlung von Zeitschlitzten vornehmen, sondern die gesamte Senderichtung in Anspruch nehmen – was dann ebenfalls zur vollständigen Blockade aller am gleichen Port hängenden Endkunden führen würde. Ähnliches passiert beim Anschluss von Geräten, die auf andere Glasfaserstandards konfiguriert sind. Hier werden weitgehend identische Wellenlängen auf unterschiedliche Weise beansprucht, was zu einer spektralen Überlagerung und damit zu einer Blockade führt. Hiergegen gibt es zwar Sicherungsmechanismen, etwa „listen before talk“, welches die Erkennung z. B. einer AON-Konfiguration ermöglicht, oder durch Steuerbefehle, welche vom OLT an diese ONT gesendet werden und sie zum Abbrechen ihrer Sendetätigkeit veranlassen – dies aber setzt natürlich voraus, dass die ONT diese Mechanismen sauber implementiert haben und Befehle erkennen und umsetzen. Eine Garantie dafür gibt es natürlich nicht, was unterstreicht, dass an dieser Stelle eine umfangreiche Testung (Interoperabilitätstests) zwingend nötig ist. Dies ist umso wichtiger, als die einzig verbleibende Methode zur Störungseingrenzung und -behebung darin besteht, dass das Gerät manuell vom Netz getrennt wird – oder idealerweise gar nicht erst an das Netz angeschlossen wird. Das aber setzt zwei Dinge voraus, die schlechterdings nicht zu erwarten sind: Entweder der Endkunde ist in der Lage, das richtige Gerät bzw. die richtige

Konfiguration zu verwenden oder aber der Netzbetreiber hat einen physischen Zugriff auf den ONT und kann ihn – physisch – abschalten bzw. konfigurieren.

Gerade Letzteres zeigt auch die für Point-to-Multipoint-Netzwerke spezifische Problematik bei der Störungsbehebung. Zwar ist eine Identifizierung des störenden Gerätes etwa durch vorherige Registrierungsmechanismen zu ermöglichen. Es ist aber praktisch unmöglich, die Störeinflüsse defekter oder fehlerhaft programmierter Geräte netzseitig zu begrenzen oder gar zu beenden. Es bedarf in solchen Fällen eigentlich immer eines physischen Zugriffs auf ein Gerät (insbesondere ONT), welches sich in aller Regel in einem persönlichen und geschützten Bereich des Endkunden (zumeist eine Wohnung) befindet, sodass eine Abschaltung praktisch nur unter Mitwirkung dieses Endkunden erfolgen kann. Ist diese Kunde verreist, sonst verhindert oder unwillig, verbleibt zwar immer noch die Möglichkeit, die physische Leitung zu kapfen. Aber während dies etwa in Mehrparteienanlagen – den Zugang vorausgesetzt – verhältnismäßig einfach zu realisieren ist, steht bei einzeln versorgten Objekten auch diese Lösung nicht zur Verfügung, sodass in letzter Instanz dann nur ein Aufbruch der öffentlichen Verkehrswege zwecks Leitungstrennung verbleibt.

Ein weiteres topologiespezifisches Problem ist, dass Point-to-Multipoint-Netzwerke aufgrund ihrer Funktionsweise eine erhöhte Anfälligkeit für Identitätsfälschungen aufweisen.

Wie oben ausgeführt, wird in Point-to-Point-Netzen die individuelle Kommunikationsbeziehung zum Endnutzer durch dessen exklusive Leitungsnutzung auf physische Weise hergestellt. Daher ist es auch einfach, die Identität des Endnutzers durch Identifizierung der genutzten Leitung abzusichern. Eine Fälschung bedürfte eines physischen Leitungszugriffes, was einen ganz erheblichen Aufwand verursacht. Darüber hinaus müsste zusätzlich das Endgerät des Endnutzers eine andere Identität vorspiegeln, was eine weitere Hürde aufbaut und in Summe kaum zu realisieren ist. Die Absicherung der Identität erfolgt also sowohl netzseitig als auch endnutzerseitig.

In Point-to-Multipoint-Netzen hingegen ist es wie ausgeführt nicht möglich, die individuelle Kommunikationsbeziehung mit einem Endnutzer durch das physische Netz herzustellen. Ein Aufbau einer Kommunikationsbeziehung kann nur auf höherer Ebene (PPPoE IA bzw. DHCP Option 82) erfolgen und muss dafür an ein Netzabschlussgerät (ONT etc.) anknüpfen, das für die Authentifizierung des Endnutzers die relevante Instanz ist. Die Identität des Endnutzers kann hingegen nicht durch ein Netzelement (OLT etc.) abgesichert werden, sondern basiert allein auf dem Vertrauen in ein Gerät, welches sich im alleinigen physischen Zugriff des Endnutzers befindet.

Konkrete Missbrauchsmöglichkeiten tun sich in Point-to-Multipoint-Netzen also dort auf, wo das verwendete Netzabschlussgerät (ONT etc.) so manipuliert wird, dass es wirksam vertäuscht, ein anderes Gerät – insbesondere das eines anderen Nutzers im gleichen Segment (im gleichen PON-Port) – zu sein. Damit lassen sich dann nicht nur fremde Leistungen nutzen, sondern auch Straftaten unter Verschleierung der eigenen Identität begehen. Zugleich

besteht die Gefahr, dass Notrufe falsch zugeordnet werden und lebensrettende Hilfe unterbleibt.

Das Mittel der Wahl für Gegenmaßnahmen besteht offenkundig darin, den Netzabschlussgeräten unveränderliche und eindeutige Kennungen zuzuordnen. Naheliegend sind insofern Verknüpfungen mit Seriennummern und MAC-Adressen, die jedoch durch geschickte Hardwariemanipulationen oder durch Eingriffe in die Kommunikation (genauer: in die zur Authentifizierung übermittelten Daten) zu umgehen sind (sog. Spoofing). Daher bestehen modernere Lösungen darin, Zertifikate auszutauschen, die durch eine asymmetrische Verschlüsselung sichere Kommunikation und Identifikation ermöglichen. Bei genügender Schlüssellänge sind solche Zertifikate weitgehend fälschungssicher, können aber trotzdem – durch andere Techniken – ihren Weg in unberechtigte Hände finden. Hier sind Methoden des Social Engineering oder aber auch Fehler in der Programmierung der Firmware die wichtigsten Einfallstore.

Dass diese Szenarien auch nicht nur theoretischer Natur sind, zeigen die Erfahrungen in Kabelnetzen, wo das Problem seit Längerem bekannt ist und technisch durch zertifikatbasierte Mechanismen zumindest eingedämmt werden kann.

Der sicherlich prominenteste Fall datiert hier aus dem Jahr 2016, als bekannt wurde, dass die für die Absicherung der Identität von Kabelmodems nötigen Zertifikate von AVM-FritzBoxen mit integrierten Kabelmodems im großen Stile kompromittiert waren, nachdem der geheime Schlüssel dieser Zertifikate in der Firmware der Boxen abgelegt wurde und ausgelesen werden konnte. In der Folgezeit wurden von verschiedenen Netzbetreibern etliche Versuche detektiert, Geräte mit solchen Zertifikaten ans Netz zu bringen. In welchem Umfang seinerzeit Zertifikate gefälscht und missbräuchlich verwendet wurden, bevor das Problem enthüllt wurde, ist nicht bekannt. Zur Behebung der Probleme mussten jedenfalls durch Firmwareupdates neue Zertifikate auf alle entsprechenden Geräte aufgespielt werden, was nicht nur einen erheblichen Aufwand aufseiten der Netzbetreiber verursachte, sondern infolge mangelnder Mitwirkung von Nutzern auch bis in das Jahr 2018 hinein andauerte. Selbst Zwangsabschaltungen von Modems, deren Aktualisierung verweigert wurde, mussten durchgeführt werden.² Noch heute muss auf den Netzsteuersegmenten ein Widerruf der Zertifikate händisch eingetragen und vom Netzbetreiber bei jedem Firmwareupdate geprüft werden.

Vergleichbare Fälle sind in allen Point-to-Multipoint-Netzen denkbar, auch in PON. Es bleibt immer die Unsicherheit, dass die Authentifizierung auf einem nicht vollständig technisch zu schützenden Vertrauen in die Integrität eines (Netzabschluss-)Gerätes, das sich im exklusiven physischen Machtbereich des Endnutzers befindet, beruht. Dieses latente Risiko wird dabei natürlich desto größer, je mehr Verfügungsgewalt der Endnutzer über das Gerät hat bzw. je weniger Einfluss der Netzbetreiber auf dieses hat. Insbesondere Geräte, welche ein Endnutzer aus womöglich dubiosen Quellen bezieht, haben eine erhöhte Anfälligkeit für krasse Programmierfehler wie im vorstehend geschilderten Fall. Hinzu kommt, dass – wie auch der vorstehende Fall zeigt – Sicherheitslücken nur auf anbietereigenen Geräten rasch zu

² Verwaltungsverfahren der BNetzA Az. 416a (18-12).

schließen sind, da die Mitwirkungsbereitschaft von Endnutzern – sei es aus Bequemlichkeit, aus Unwissen oder gar in Missbrauchsabsicht – gering ist.

c. Unterschiede bei der Zugangsgewährung

Ein spezifischer Unterschied zwischen PON und VDSL-Netzen tut sich wegen der praktisch fehlenden Interoperabilität von ONT mit unterschiedlichen Netzen bei den Bemühungen um die Einführung eines Open-Access-Regimes auf.

Hier besteht die zentrale technische Herausforderung darin, den durch Netzbetreiber A an Netzbetreiber B gewährten Zugang möglich zu machen, was den Einsatz geeigneter Netzabschlussgeräte voraussetzt. Ausgangssituation ist jedoch, dass Netzbetreiber B über ONT verfügt, die indes mit an Sicherheit grenzender Wahrscheinlichkeit nicht mit Netz A ordnungsgemäß zusammenarbeiten werden. Eine individuelle Anpassung von Netz A an die Geräte von Netzbetreiber B ist ersichtlich unsinnig, da dies übermäßige Kosten verursachen, eigene Kunden in Gefahr bringen und den Zugang anderer Nachfrager hindern würde. Auch der umgekehrte Weg, die Geräte von Netzbetreiber B durch entsprechende Firmwareupdates interoperabel zu machen, ist nicht gangbar. Er löst nämlich ebenso enorme Kosten für langwierige Tests aus, welche insbesondere bei kleinen Zugangsnachfragern prohibitiv wirken, weil sie – umgelegt auf eine geringe Kundenzahl – die Preise in Höhen weit jenseits jeder Wettbewerbsfähigkeit treiben. Da es aber auch keine den Kunden vermittelbare Option ist, ihnen die Beschaffung eines passenden Gerätes auf eigenes Risiko zu überlassen, sind Zugangsnachfrager darauf beschränkt, die gleichen ONT zu beschaffen, welche vom Netzbetreiber A verwendet werden. Das hat jedoch zwei gewichtige Nachteile: Bei integrierten Geräten, also solchen mit integrierten Endgeräten (Routern), geht damit eine Vorprägung auf ein bestimmtes Funktionalitätsangebot (das im Router abgebildet wird) einher und behindert die wettbewerbliche Differenzierung. Außerdem ist die Beschaffung von Klein- und Kleinstmengen nur zu deutlich höheren Stückpreisen möglich, was insbesondere bei kleinen Zugangsnachfragern einen gewichtigen Einfluss auf den Endkundenpreis und damit die Wettbewerbsfähigkeit hat. Einzig sinnvoll ist daher im Ergebnis der Einsatz von nicht-integrierten ONT, welche durch Netzbetreiber A gestellt werden – und zwar ungeachtet der Vorstellungen der Endkunden von Netzbetreiber B.

Hinzu kommt, dass zwar Router als Endgeräte im Rahmen des Internetdienstes durch die ihnen zugewiesene IP-Adresse adressier- und identifizierbar und damit für Eingriffe des Vorleistungsnachfragers/Diensteanbieters im Störfall oder für Firmware-Updates offen stehen. Allerdings hat der Vorleistungsnachfrager keine Möglichkeit, für solche Maßnahmen auf den ONT des Endkunden zuzugreifen: Er ist via IP nicht adressierbar, sondern muss durch den OLT direkt angesprochen werden, auf den für ihn kein Zugriff besteht. Sinnvollerweise muss das ONT also als Bestandteil der Vorleistung (und damit des vorleistenden Netzes) gesehen werden und nicht als Teil des Heimnetzwerks.

2. Unterschiede von PON zu Kabelnetzen

Der zentrale Unterschied zwischen PON und Kabelnetzen ist kein topologischer, da beide eine Point-to-Multipoint-Architektur aufweisen und folglich ihre dienstespezifischen Adressierungsaufgaben durch aktive Geräte im Bereich des Endkunden erfüllen müssen. Diese Aufgabe wird dabei in Kabelnetzen durch sog. Kabelmodems übernommen, die insoweit das Gegenstück zu den ONT darstellen.

Der dennoch deutlich wahrnehmbare praktische Unterschied im Betrieb ist historisch begründet. Zum einen dauert die Entwicklung und Fortschreibung des DOCSIS-Standards für Kabelnetze schon deutlich länger an und erfolgt auch heute noch. Zum anderen werden Sicherheitsaspekte nicht nur in den Standards, sondern auch in den eingeübten Prozessen (dazu unten) deutlich stärker berücksichtigt. Insbesondere erweist es sich zunehmend als Vorteil, dass sich eine unabhängige Stelle für den Standard und die Interoperabilitätstests verantwortlich zeigt und von einer solchen Stelle auch Zertifikate erstellt werden, auf die keine weitere Partei einen Einfluss hat..

Die grundsätzlichen Störungsszenarien für Point-to-Multipoint-Netze, die im vorstehenden Unterpunkt dargelegt wurden, sind dennoch in beiden Technologien denkbar. Lediglich das Szenario eines für aktive Netze (Point-to-Point) gedachten Netzabschlussgeräts existiert in Kabelnetzen nicht, da es diese Topologie dort gar nicht erst nicht gibt.

Für Kabelnetze existieren konkret seit Jahren eingeübte Prozesse, in denen Kabelmodems und ihre Firmware in allen ihren Entwicklungsständen wohldefinierten und stetig fortentwickelten Interoperabilitätstests unterzogen werden. Die notwendige Testinfrastruktur aus Labors und hoch qualifizierten Fachleuten ist über Jahre hinweg durch CableLabs aufgebaut worden und steht allen Herstellern offen. Die Testszenarien sind aus den Anforderungen der jeweiligen DOCSIS-Standards entwickelt und können auch Spezifika für einzelne große TK-Provider adressieren, da die Standards einzelne Abweichungen zulassen bzw. Optionen enthalten. Mit dem Bestehen eines solchen Tests kann in der Praxis quasi lückenlos sichergestellt werden, dass die Geräte bzw. ihre Firmware mit allen wichtigen Netzen zusammenarbeiten – da kleinere Betreiber den Netzwerkanforderungen der großen Provider üblicherweise folgen, kommt es auch dort in der Praxis zu keinen Interoperabilitätsstörungen.

Solche Tests sind indes aufwendig, da nicht nur die Laborinfrastruktur vorgehalten werden, sondern das Verhalten der Geräte bzw. ihrer Software tief greifend analysiert werden muss. Für die von den Herstellern zu tragenden Kosten ist eine Größenordnung von 100.000 US\$ für einen vollständigen Test üblich. Allerdings ist aufgrund der – gegenüber PON – vergleichsweise geringen Zahl von Permutationen an Herstellern/Chipsätzen/Firmwareversionen eine deutlich geringere Komplexität der Tests nötig.

Für Glasfasernetze, insbesondere PON, hat sich bisher keine ernsthaft vergleichbare Teststruktur herausgebildet, was aber auch dem Umstand geschuldet ist, dass durch den fortlaufenden Ausbau und die gestiegene Bedeutung von Glasfaser derzeit sehr viele Hersteller den

Markt der Herstellung von OLT und ONT bedienen. Eine Marktkonsolidierung ist derzeit noch nicht absehbar.

Hersteller versuchen vor allem, durch bilaterale Kooperationen mit Netzbetreibern individuelle Tests und Anpassungen vorzunehmen, um die Kosten ganz oder zumindest teilweise auf die Netzbetreiber zu verlagern. Das sichert indes – wie auf der Hand liegt – lediglich die Interoperabilität mit dem spezifisch getesteten Netz; für andere Netze gibt es keine auch nur im Ansatz belastbare Aussage über eine Interoperabilität. Daneben gibt es zwar auch Testmöglichkeiten innerhalb des Broadband Forums (BBF.247 Certification³). Diese Tests sind jedoch nur lückenhaft standardisiert und keineswegs auf konkrete Netzbetreiber und deren Service Modelle abgestimmt; vielmehr können Hersteller ihre Testszenarien mehr oder weniger umfangreich ohne die Mitwirkung von Netzbetreibern selbst ausgestalten. Darüber hinaus erfolgt die Testung gegen ein (simuliertes) OLT, welches mit den im praktischen Einsatz befindlichen Geräten nur wenig zu tun hat, sondern seine eigene Interpretation der Standards mitbringt. In der Praxis zeigt sich zudem, dass schon aus Kostengründen nur wenige für eine Interoperabilität aussagekräftige Tests durchgeführt werden. Ein Testsiegel enthält in der Folge keinerlei Aussage über die störungsfreie Kommunikation mit einem bestimmten Netz – geschweige denn mit mehr als einem Netz.

Im Allgemeinen wird die BBF.247-Zertifizierung im Markt höchstens als grundlegende Interoperabilität angesehen.

Eine der Testkultur für Kabelnetze vergleichbare Infrastruktur herauszubilden, erscheint zwar allenthalben erstrebenswert, ist aber auch auf lange Sicht ein schwieriges Unterfangen. Allein der Aufbau der nötigen Testkapazitäten wird erhebliche Zeit und die Einbindung von einer Vielzahl an hoch qualifizierten Experten in Anspruch nehmen und daher Jahre dauern. Außerdem müssen Testszenarien entwickelt werden, was mehrere Monate und erhebliche Summen beanspruchen dürfte. Schließlich ist noch der Unwille der Hersteller zu überwinden, sich an den Kosten sinnvoller Tests zu beteiligen.

Letztlich aber müssen sich solche Tests aus rein praktischen Gründen – d. h. wegen ihres schieren Umfangs und Aufwands – auf 2-3 Referenznetze konzentrieren, was ein eigenes Problem darstellt: In den Gesprächen, welche die Verfasser mit US-amerikanischen Experten geführt haben, hat sich jedenfalls sehr schnell gezeigt, dass Letztere aus ihrer Erfahrung in Kabelnetzen, aber auch in US-amerikanischen Glasfasernetzen, keine realistische Möglichkeit sehen, die erforderlichen Tests auf mehr als 2-3 Netzwerke und ihre Spezifika auszurichten. Für Deutschland/Europa ist dies aktuell ein kaum zu überwindendes Problem. Hierzulande errichten ungefähr 170 Anbieter Glasfasernetze in PON-Architektur und es gibt wahrscheinlich genauso viele spezifische Netzwerkanforderungen, gegen die getestet werden müsste, zumal die am Markt verfügbaren Netzelemente Teil von proprietären Lösungen des jeweiligen Herstellers und alle unterschiedliche Anforderungen mit sich bringen.

³ <https://www.broadband-forum.org/wp-content/uploads/2023/04/BBF.247-GPON-ONU-Products-2023-04-21.pdf>.

Ist in der Praxis daher mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen, dass Geräte, die mit einem Netz A – auch mit einem „großen“ Netz – zusammenarbeiten, mit einem Netz B zusammenarbeiten werden, heißt dies für die Mehrzahl der Anbieter in Deutschland, dass eine Interoperabilität nur dann sicherzustellen sein wird, wenn diese ihre Netze an diejenigen der „großen“ Betreiber anpassen. Voraussichtlich wird dieser Zustand von selbst im Laufe der Zeit eintreten, nämlich als Nebeneffekt fortschreitender Konsolidierung sowohl auf Hersteller- als auch auf Netzbetreiberseite. Er wird jedoch nach allem, was abzusehen ist, mehrere Jahrzehnte in Anspruch nehmen und erhebliche Aufwände erfordern, die im Ausbau von Glasfasernetzen sicherlich besser allokiert wären als im Umbau bestehender Glasfasernetze.

Um die Dimension der Unterschiede in den Testaufwänden zwischen PON und Kabelnetzen etwas deutlicher zu machen, verweisen wir hier auf die **Anlage 1**, welche allerdings aus Platzgründen auch nur die wesentlichen Aspekte behandeln kann.

III. Fallbeispiele für Störungen

Zu der Frage nach konkreten Fallbeispielen und dazugehörigen Details verweisen wir hier auf eine separat übersendete **Anlage**. Darüber hinaus sind indes einige Anmerkungen angebracht:

Wir haben vorstehend eingehend und anhand konkreter Szenarien aufgezeigt, welche Störungen und Sicherheitsprobleme zur Rede stehen und welche Mechanismen für deren Auftreten verantwortlich sein können. Die Ursachen können zwar mannigfaltig sein, lassen sich aber im Wesentlichen auf drei Felder einengen:

- (ungetestete) inkompatible Implementationen
- Firmwaremanipulationen
- Programmierfehler

Abgesehen letzterer Fehlerursache (Programmierfehler), die in allen Konstellationen auftreten kann und auch durch ausgiebige Tests nicht vollständig auszuschließen ist, sind alle diese Szenarien nur dann relevant, wenn Kunden ein eigenes ONT an das jeweilige Netz anschließen. Geräte, welche die Netzbetreiber ihren Kunden überlassen, sind – wie oben beschrieben – bilateral ausgiebig getestet und werden mit jedem relevanten Firmware-Update neu getestet. Außerdem verhindern Netzbetreiber das Aufspielen potenziell gefährlicher Firmware aus Drittquellen in sehr effektiver Weise.

Hier aber zeigen Rückmeldungen aus den Mitgliedsunternehmen der unterzeichnenden Verbände, dass bei den meisten Netzbetreibern derzeit lediglich etwa 0,1 % der Kunden ein eigenes ONT anzuschließen suchen. Von diesen wiederum nutzt der allergrößte Teil (ca. 98 %) ein ONT, welches ihm auch von seinem Netzbetreiber zur Verfügung gestellt werden könnte, da diese auf dem Markt am ehesten erhältlich sind und in der Regel eine gewisse Kundenreputation besitzen. Damit sind in der heutigen Situation praktisch alle zum Anschluss gelangenden ONT auf Interoperabilität getestet und lassen Firmwaremanipulationen nur mit sehr hohem Aufwand zu.

Vor diesem Hintergrund erschließt sich denn auch, warum konkrete Praxisfälle nur schwer zu finden sind. Die beschriebenen und auch realistisch zu befürchtenden Fälle sind nicht etwa deswegen nicht in größeren Mengen aufgetreten, weil die Szenarien an den Haaren herbeigezogen wären. Sie werden lediglich sehr effektiv dadurch verhindert, dass die Netzbetreiber ihren Kunden nur sichere Geräte überlassen und diese (noch) kein Interesse daran zeigen, sich fragwürdige Geräte aus fragwürdigen Quellen zu besorgen. Gerade die Auflistung, welche der VTKE vornimmt (dazu ausführlicher unten) zeigt bei näherem Hinsehen, dass es keineswegs einfach und naheliegend ist, ein unproblematisches ONT "im Vorübergehen" zu beschaffen.

Genau in diese Richtung zielt denn auch der hier hilfsweise gestellte Antrag. Er soll verhindern, dass durch plakative Freigabe kundeneigener ONT das Interesse der Endkunden befeuert und damit auch zunehmend auf problematische Geräte gelenkt wird. Damit würden einer Fehlerquelle gleich zwei hinzugefügt, von denen eine – die fehlende Interoperabilitätstestung – auch das weitaus größte Problem darstellt. Die heute noch überschaubare Gefahr für die Netze würde signifikant steigen – aber es wäre natürlich auch deutlich schneller möglich, eine Vielzahl von Sicherheitsvorfällen zu dokumentieren.

Ein weiteres Hindernis, konkrete Vorfälle zu benennen, übrigens liegt auch in der Fragestellung selbst: Hier wird nicht etwa nur nach Details wie Ort, Art und Anzahl betroffener Kunden gefragt. Vielmehr sollen viele weitere Details beigebracht werden, nämlich insgesamt

- Art des OLT
- Chipsatz des OLT
- Anzahl der betroffenen Nutzer
- Art des Ausfalls (Totalausfall oder Reduzierung der Bandbreiten Dritter)
- Dauer des Ausfalls
- Behandlung der Störungen im Rahmen etwaiger Minderungs- und Entschädigungsansprüche nach § 57 bzw. § 58 TKG

Dies sind Daten, die für zurückliegende Vorgänge aus verschiedenen Quellen zusammengestellt werden müssen. Insbesondere die rechtliche Behandlung im Nachgang muss aufwendig manuell nachvollzogen werden. Aber auch die technischen Details zu den OLT müssen einzeln zusammengetragen werden. Dies alles nimmt erhebliche Kapazitäten bei Mitarbeitenden in Netzbetrieb und Kundenservice in Anspruch, die sich üblicher Weise um aktuelle Themen zu kümmern haben.

Dennoch ist es unser Anspruch, die entsprechenden Fälle so genau wie möglich zusammenzutragen und nachvollziehbar darzustellen. Wir halten es jedoch nicht für zielführend, ein so komplexes und wichtiges Thema durch oberflächliche und lückenhafte Darstellungen ungeprüfter Sachverhalte zu belasten und Zeitdruck aufzubauen.

Den in diesem Zusammenhang auch bilateral geäußerten Vorwurf, dass seitens der Antragsteller Zeit gewonnen werden sollte, weisen wir jedenfalls zurück. Es ist noch nicht einmal ersichtlich, welche Vorteile erreicht oder welche Weichenstellungen in der gewonnenen Zeit vorgenommen werden könnten. Entgegen einer immer wieder – natürlich ohne jeden Beleg – geäußerten Vermutung verdienen die Netzbetreiber und Diensteanbieter nicht an der

Überlassung der Geräte an ihre Kunden. Die Kosten für Beschaffung, Verwaltung, Lagerung und Logistik übersteigen bei Weitem die Zahlungen, welche Endnutzer bei Vertragsschluss leisten.

Letztlich erstaunt uns aber auch die Äußerung, dass aufseiten der BNetzA keine Kenntnis über Sicherheitsvorkommnisse vorläge. Wie der **Anlage** zu entnehmen ist, gibt es eine Vielzahl von Sachverhalten, die sehr wohl detailliert besprochen wurden. Auch sei hier auf das oben erwähnte ein Verwaltungsverfahren zu Zertifikatschlüsseln in FritzBoxen hingewiesen, wo die Notwendigkeit einer Kontrolle über die Firmware – mithin über den Netzabschlusspunkt – deutlich erkennbar wurde. Das Verfahren selbst wurde in verschiedenen Abteilungen und Ebenen der BNetzA intensiv diskutiert.

IV. Einzelne Aspekte aus der Stellungnahme des VTKE

Hinsichtlich der Stellungnahme des VTKE ist zunächst in aller Deutlichkeit klarzustellen, dass die Antragsteller zu keiner Zeit das Ziel verfolgt haben – und dies auch weiterhin nicht tun –, die Endgerätewahlfreiheit zu beschneiden oder abzuschaffen. Die Antragsteller erkennen wie der seinerzeitige Richtliniengeber und ihm folgend BEREK in den Richtlinien⁴ den Wert eines freien Marktes für Endgeräte, insbesondere weil dessen Innovationskraft und Wettbewerbsfähigkeit den Endnutzern zugutekommen. Sie treten jedoch dem Bestreben entgegen, den Endgerätebegriff so weit zu überdehnen, dass die fehlende Hoheit der Netzbetreiber über ihr eigenes Netz zu ernsthaften Problemen hinsichtlich Sicherheit und Dienste-Qualität (QoS, QoE) der Netze führt. Dies gilt umso mehr, als der VTKE zwar für eine freie ONT-Wahl einen Vorteil für Endnutzer hinsichtlich Innovationskraft und Wettbewerbsfähigkeit insinuiert aber nirgends zu belegen vermag. Hierzu ist bereits im Antrag ausgeführt worden, dass alle für Endnutzer relevanten Funktionalitäten, hinsichtlich derer ein Innovationswettbewerb gewährleistet sein soll und muss, im Router und nicht im ONT implementiert werden. Der Router stellt unstreitig ein Endgerät dar, welches der Endnutzer nach seinem Belieben wählen kann.

Die Innovativität bei der ONT-Entwicklung ist hingegen im Wesentlichen auf die von den Technologiestandards vorgegebenen Funktionalitäten begrenzt. Die Innovativität wird maßgeblich durch die Entwicklungen des Netzes und die Erkenntnisse aus den durchgeführten Interoperabilitätstests getrieben. Lediglich bei Geschwindigkeit und Effizienz mögen sich unabhängig von Fortentwicklungen in der Standardisierung einzelne Gewinne erzielen lassen. Jedoch sind dies Eigenschaften, welche für die Netzbetreiber eine genauso große (wenn nicht gar eine größere) Rolle wie für Endkunden spielt, sodass auch insoweit ein ausreichender Innovationsdruck gewährleistet ist. Für weitere Ausführungen hierzu verweisen wir auf die Darlegungen unten unter VI.

Entgegentreten ist auch dem Vorwurf, dass durch die gestellten Anträge bestehende Lösungen für vor dem ONT liegende Netzabschlusspunkte aus dem Markt gedrängt würden. Durch

⁴ BEREK Guidelines on Common Approaches to the Identification of the Network Termination Point in different Network Topologies, BoR (20) 46.

die Festlegung des Netzabschlusspunktes kann allenfalls bestimmt werden, wo das jeweilige Netz spätestens endet. Welche Funktionen in diesem Netz implementiert werden und welche Freiheiten Endnutzer auf diesem Netz genießen, ist der Entscheidung des jeweiligen Netzbetreibers überlassen. Es ist nach unserem Dafürhalten zu erwarten, dass durchaus einige Netzbetreiber einen einmal eingeführten Umgang mit diesen Fragen nicht ohne Weiteres wieder abschaffen werden. Im Übrigen können solche Lösungen sehr wohl noch vertrieben werden. Es ist allerdings zuzugeben, dass es schwieriger wird, sie mit plakativen Werbeaussagen und bunten Verpackungen auf dem Markt zu etablieren, da die Netzbetreiber und Diensteanbieter ihre Auswahl eher auf die Funktionalitäten und Leistungen stützen werden.

Wir sehen auch nicht, dass sich eine solche Entscheidung in unzulässiger Weise negativ auf die Endgerätehersteller auswirken würde. Diese können weiterhin Endgeräte, also Router vertreiben. Auch steht es ihnen selbstredend frei, ONT zu entwickeln und zu vertreiben. Dass sich der Kundenkreis einengt, hat dabei sicherlich Auswirkungen, jedoch sind wirtschaftliche Partikularinteressen kein Argument bei der Beurteilung rechtlicher und technischer Sachverhalte.

Schließlich widersprechen wir auch dem Vortrag, dass Endkunden die Verweigerung eines Anschlusses droht. Die Netzbetreiber haben ein intrinsisches Interesse, allen Endkunden einen Anschluss zu ermöglichen. Es sollte indes gesichert sein, dass dieser Anschluss nicht nur funktioniert – was aufgrund der technischen Realität für vom Endnutzer beschaffte Geräte gerade nicht zu gewährleisten ist –, sondern auch keine nachteiligen Auswirkungen auf die Sicherheit der Netze und somit auf andere Endkunden hat. Auch dies ist ein intrinsisches Interesse der Netzbetreiber, das sehr wohl eine rechtliche Bedeutung hat.

Zu den einzelnen Aspekten des VTKE-Schreibens darüber hinaus wie folgt:

1. Standardisierung

Hinsichtlich der Standards führt der VTKE richtigerweise aus, dass derzeit im wesentlichen drei Standards – IEEE-PON, IEEE-Active-Ethernet und ITU-PON – bestehen, wobei unterschlagen wird, dass diese Standards untereinander nicht kompatibel sind und eine unübersehbare Vielfalt an optionalen Features und möglichen Implementationen vorsehen. Ebenso wird unterschlagen, dass selbst für eigentlich zwingende Vorgaben eine enorme Vielzahl an Umsetzungen in OLT und ONT besteht, die untereinander eher zufällig kompatibel sind.

Daher ist die Tatsache, dass in Europa der ITU-Standard vorrangig genutzt wird, wenig informativ. Die Aussage, Produkte könnten weltweit mit den bestehenden Standards weltweit problemlos designet werden, erscheint noch nicht einmal in Europa sinnvoll. Die Realität ist vielmehr deutlich kleinteiliger: Konformität wird bestenfalls national, in der Praxis aber

tatsächlich netzwerkweit hergestellt. Realistische Zahlen können übrigens einer WIK-Studie⁵ entnommen werden.

Vor diesem Hintergrund stellt sich die unbestritten richtige Aussage, dass Endkunden CPE weltweit beziehen können, ganz anders dar: Gerade aufgrund der unzähligen Permutationen an Anforderungen, welche das OLT an das ONT stellt und welche Umsetzungen das ONT und dessen Firmware zu bieten hat, ist die Chance, ein solches Gerät auch nur an einem Netz eines deutschen PON-Betreibers arbeitsfähig – und bestenfalls auch noch störungsfrei – ohne Interoperabilitätstest zu Laufen zu bringen, geradezu verschwindend gering.

Diese Probleme beginnen aus technischer Sicht mit den verschiedenen Chipsätzen, welchen der VTKE indes fälschlich die größte Bedeutung beimisst. Die ONT-Kompatibilität und Funktionsmöglichkeit hängen nur teilweise von den Chipsätzen ab, da diese nicht in ihrem Design genormt sind, sondern in ihrer Funktionalität und wenige Abweichungen zulassen. Der Wert eines Chipherstellers ist in seinem Technologiefiler begründet, mit dem er die entsprechenden Wafer für die Chipsets erstellt. Die Möglichkeiten eines ONT hängen vielmehr ganz weit überwiegend von der Prozessorleistung, Speichergroße, den mit dem Chipsatz verbundenen SDKs (Software Development Kit) ab. Damit eine Interoperabilität und Kommunikation mit dem OLT aufgebaut werden kann, müssen alle Komponenten entsprechend konfiguriert sein. Allerdings unterscheiden sich Chipsätze in ihren Baureihen, also in ihren Fortentwicklungen. Nimmt man hinzu, dass es deutlich mehr Chipsatzhersteller für OLT als für CMTS und deutlich mehr Hersteller von OLT als von CMTS gibt, so ergibt sich allein auf der Hardwareseite, dass es für PON mindestens 40 Permutationen von OLT-ONT-Konfigurationen gibt, während in Kabelnetzen gerade einmal 8 Permutationen von CMTS-CM-Konfigurationen bestehen (zu Details s. hier die **Anlage 1**).

Letztlich aber entscheidet der CPE-Hersteller, welche Funktionen und Aufgaben das Gerät überhaupt übernehmen kann und welche Aufgaben ggfs. zukünftig implementiert werden mit dem Design der Firmware, die mit den Chipsätzen interagiert. Die Netzbetreiber haben auf deren Entwicklung allenfalls einen sehr entfernten Einfluss, sind also den CPE-Herstellern insoweit ausgeliefert. Diese Software setzt die in den Chipsätzen fest hinterlegten grundsätzlichen Funktionalitäten um und passt sie den sich entwickelnden Anforderungen der Netze an. Die Chipsätze selbst werden nach den einigermaßen klaren und eindeutigen Designregeln der IEEE/ITU/BBF-Standards erstellt und sind somit im Wesentlichen gleich. Diese Anforderung wird von entsprechenden Gremien geprüft. Nicht umsonst werden Interoperabilitätstests in anderen Technologien (namentlich im DOCSIS-Bereich) für einzelne Firmwarestände durchgeführt. Hierzu kann beispielhaft auf die Einführung der AVM-Firmware FritzOS 7.26 (Releasedatum 01.09.2022) verwiesen werden, die nach den Release-Notes zur Verbesserung der Interoperabilität diente. Mit welchen Netzen oder welchen Netztopologien damit zusätzlich eine Zusammenarbeit hergestellt und welchen Qualitäts- und/oder Sicherheitsproblemen

⁵ <https://www.wik.org/veroeffentlichungen/veroeffentlichung/studie-zur-umsetzung-der-bestimmungen-zum-offenen-internetzugang-der-verordnung-2015-2120>.

begegnet wurde, ist den Notes zwar nicht zu entnehmen, dürfte angesichts des Umfangs aber eine erhebliche Reichweite gehabt haben.⁶

Unter dem Strich muss hier von einer mindestens dreistelligen Anzahl an Permutationen für

Konfiguration ONT und physische Anbindung <-> Konfiguration OLT

ausgegangen werden, die insbesondere durch die vielen Optionen und Interpretationsspielräume der Standards getrieben wird, sodass die Chance, ein ungetestetes, arbeitsfähiges und nicht-störendes Gerät auf dem Weltmarkt zu erwerben, selbst bei großzügigen Annahmen bei deutlich unter 1 % liegt. Da hilft auch die Veröffentlichung von Schnittstellenbeschreibungen nicht weiter, da es praktisch ausgeschlossen ist, derartig viele Varianten in einer Firmware zu berücksichtigen und Faktoren wie (Virtual) OMCI ebenfalls die Kompatibilität beeinflussen.

Aus diesem Grund bedürfte es für jedes Endgerät zumindest der Durchführung geeigneter Konformitäts- und Interoperabilitätstests. Wie aber oben bereits ausgeführt, ist auch dies illusorisch, weil die nötige Vielzahl an Testszenarien nicht zu leisten ist. Welche Testszenarien dem VTKE in diesem Zusammenhang bekannt und in seiner Anlage 2 näher dargelegt werden, wäre an dieser Stelle sicherlich interessant zu erfahren. Leider existiert die Anlage 2 – zumindest nicht in dem den Verbänden zugänglich gemachten Dokument – genauso wenig wie herstellerübergreifende Interoperabilitätstests. Richtig ist hier lediglich die Darlegung, dass Endgerätehersteller dazu übergegangen sind, ihre Geräte bilateral mit Netzbetreibern zu testen, um die Testkosten abzuwälzen. Dass dies indes nicht dazu führt, dass Geräte an mehr als den konkret getesteten Netzen funktionieren, ist oben bereits näher ausgeführt worden.

2. Auf dem Markt erhältliche Geräte

Der VTKE listet in seiner Stellungnahme etliche Geräte auf, die vorgeblich bezogen und an praktisch jedem deutschen Glasfasernetz betrieben werden können. Eine nähere Recherche zu diesen Geräten zeigt, dass diese Aussage an der Wahrheit ausgesprochen weit vorbeigeht. Außerdem wird der völlig irreführende Eindruck erweckt, diese Geräte hätten irgendetwas mit den Tests im Rahmen des ‚BBF.247 Certificate‘ zu tun.

Zu den einzelnen Geräten verweisen wir auf die **Anlage**, in welcher wir die Liste inhaltlich repliziert und kommentiert haben.

Zunächst fällt auf, dass sich in der Liste verschiedene Geräte des Herstellers Mikrotik finden. Deren Vertrieb ist soweit ersichtlich von der BNetzA im Amtsblatt 18/2022 für 3 Geräte untersagt worden, da eine nicht behobene Inkompatibilität zu den Anforderungen der Funkanlagenrichtlinie⁷ sowie den einschlägigen ETSI-Standards⁸ bestand.

Sodann lassen sich die eigentlich namhaften globalen Hersteller auf der Liste nicht finden. Stattdessen werden in großer Zahl Geräte gelistet, die sich an Businesskunden richten und für

⁶ <https://winfuture.de/news,122439.html>.

⁷ Richtlinie 2014/53/EU.

⁸ ETSI EN 301893 v 2.1.1 (2017-05).

den normalen Endkunden ohne Belang sind. Selbst aber bei diesen Businessgeräten fällt auf, dass sie sich von Geräten für Verbraucher nur in den Routerfunktionalitäten unterscheiden – sofern sie denn überhaupt ein ONT enthalten. Etliche Geräte in der Liste sind nämlich **keineswegs funktionelle ONT**, sondern auf Ethernet-Basis anzuschließen bzw. benötigen ein zuge-schaltetes Modul (SFP).

Andere Geräte sich nicht mehr aufzufinden oder sind gar nicht verfügbar. Abgesehen davon, dass auch bei diesen Geräten einiges dafür spricht, dass sie keineswegs über ONT-Funktiona-litäten verfügen, sind die Geräte praktisch eben nicht – zumindest nicht über die angegebenen Quellen – erhältlich.

Interessanterweise lässt sich beim Gerät „Halny ONT Client Terminal“ noch eine Kundenbe-merkung finden, dass das Gerät als ONT an seinem Anschluss gerade nicht lief.

Interoperabilitätstests können lediglich für die Geräte von AVM sowie für die Telekom Deutschland GmbH, die Deutsche Glasfaser und teilweise für die Vodafone angenommen wer-den. Hierbei ist herauszustellen, dass die Interoperabilitätstests aber lediglich die Konformität im jeweiligen Netz der Netzbetreiber prüfen. Eine generelle Akzeptanz über alle Netze hinweg kann nicht angenommen werden. Für alle weiteren Endgeräte ist nicht bekannt, dass In-teroperabilitätstests durchgeführt wurden. Wie der VTKE selbst ausführt, ist eine Verifizierung der Interoperabilität notwendig und eine gängige Praxis im Austausch mit den Netzbetreibern. Aus diesem Grund ist es umso mehr verwunderlich, wenn hier Endgeräte benannt werden, welche in Deutschland praktisch nicht im Einsatz sind und dort auch nur über Umwege zu beziehen sind. Die Chance, dass solche Geräte auch nur in einem Szenario zum störungsfreien Betrieb zu bringen sind, dürfte verschwindend gering ausfallen.

Auch die Kundenrezensionen sind wohl kaum geeignet, eine Interoperabilität der Geräte zu belegen. Was die Kunden in welchem technischen Umfeld bewertet haben, ist keiner der Be-wertungen zu entnehmen. Dass die Geräte diejenigen (Router-)Funktionen bieten, die auch angepriesen werden, mag man gern glauben. Es ist auch gut möglich, dass ein Telekom-Gerät an einem Telekom-Netz funktioniert. Darüber hinaus bedürfen die Ausführungen des VTKE an dieser Stelle aber keiner weitergehenden Kommentierung.

Letztlich muss an dieser Stelle auch noch einmal ausdrücklich klargestellt werden, dass gerade Geräte, welche über ausländische Onlineshops bezogen werden, ein hohes Potenzial für Stör-verhalten aufweisen. Hinzu kommt noch, dass bei solchen Shops – wie die wenigen auffind-baren Links eindrucksvoll zeigen – die Beschreibungen der Funktionen gelinde gesagt zu wün-schen übrig lassen, was bei den Bedienungsanleitungen mit Sicherheit ähnlich sein wird und damit Fehlkonfigurationen Vorschub leistet. Hinsichtlich der Gefahr, die für den Endnutzer und den Netzbetreiber wegen der praktischen Nicht-Durchsetzbarkeit von Gewährleistungs-ansprüchen bei Störungen hinzukommt, führen wir unten noch näher aus.

3. Störungsfreiheit und Netzstörungen

Die Darstellung des VTKE, dass von Endkunden beschaffte ONT bisher keine Schwierigkeiten bereitet hätten, können wir nicht nachvollziehen. Dass es diese Schwierigkeiten bei den Netzbetreibern gab, ist dokumentiert und zum Teil auch öffentlich geworden. Dass dies seitens des VTKE nicht wahrgenommen wurde, mag sicherlich möglich sein, erscheint aber doch eher unwahrscheinlich.

Zu den konkreten Fällen haben wir oben bereits näher ausgeführt. Alle diese Fälle sind der Bundesnetzagentur als Aufsichtsbehörde bekannt gemacht worden.

V. Schlechterbringung von Diensten (QoS-Verluste)

Wie oben bereits ausführlich dargestellt, ist bereits das bloße Funktionieren von ONT – also die Erbringung irgendeines Dienstes – nur mittels Interoperabilitätstests sicherzustellen und ohne diese Tests eher Glückssache. Daneben aber wirkt sich die Verwendung ungeeigneter Geräte natürlich auch auf die Qualität der Dienste (QoS) aus. Schon eine fehlerhafte Interpretation von Einstellungen sich kann etwa bei der Telefonie durch Knacken oder Gesprächsfetzen bemerkbar machen. Eine fehlerhafte Kommunikation kann sich im Extremfall wie geschildert aber auch auf andere Endkunden und den Dienst als Ganzes auswirken.

Es ist der Netztopologie von PON nun einmal immanent, dass verschiedene Instanzen Einfluss auf die Netzqualität und damit die verfügbaren QoS-Parameter haben. Neben dem Netzbetreiber und dem Diensteanbieter können auch der Endkunde und – im Extremfall – andere Endkunden innerhalb eines Netzsegments einen positiven wie negativen Einfluss auf die Netz- und Dienstqualität (QoS) nehmen, diese wiederum essenziell ist, um ein optimales Kundenerlebnis (Quality of Experience – QoE) zu erreichen. Grundvoraussetzung und von überragender Bedeutung bei der Sicherung der nötigen QoS ist es daher, für eine optimale und reibungslose Zusammenarbeit von Software- und Hardware-Komponenten bei allen diesen Instanzen unter Berücksichtigung der jeweiligen Dienste zu sorgen.

Dies wird vor allem dort zu einer besonderen Herausforderung, wo – wie heute üblich aber in der Technologie hinter den DSL-Netzen noch nicht berücksichtigt – sich die Dienstqualität nach der Art des Endkunden (Privat- und Geschäftskunde) und Netztechnologie (Mobilfunk und Festnetz) unterscheidet. So haben Geschäftskunden in der Regel Service Level Agreements (SLAs), welche bestimmte QoS-Parameter garantieren und bei Unterschreitung eine priorisierte Entstörung des Anschlusses vorsehen. Kommen Endkunden mit verschiedenen QoS-Levels in einem Segment zusammen, ist es Aufgabe des gesamten Netzes, diese Qualität in einem austarierten, echtzeitbasierten System abzusichern. Jede kleine Störung durch eine Instanz kann wie beschrieben die Qualität der Dienstleistung anderer Endkunden unmittelbar negativ beeinflussen – bis hin zum kompletten Dienstaussfall. Zu den Mechanismen, welche diese Probleme minimieren sollen, geben wir nähere Details unten unter 1.

Dem eng verwandt ist die Herausforderung, eine rasche wirksame Entstörung zu ermöglichen, bei der Netzbetreiber und Diensteanbieter vor weiteren Problemen stehen, wozu wir im Folgenden ebenfalls weitere Details geben (unten 2.)

Eine weitere Frage ist schließlich die nach den rechtlichen Auswirkungen von QoS-Verlusten (3.). Hier liegt auf der Hand, dass sie von sehr großer Bedeutung ist, da mit dem aktuellen TKG umfangreiche Rechte der Endnutzer geschaffen wurden, mit denen qualitätsgerechte Leistungen durchgesetzt werden sollen.

1. QoS-Sicherung

Um der gesteigerten Bedeutung der Interoperabilität aller Instanzen, insbesondere von OLT und ONT, gerecht zu werden, unternehmen PON-Betreiber große Anstrengungen. Die wichtigste davon sind vom OLT ausgehende, an das ONT gerichtete Konfigurationsbefehle. Werden diese nicht oder unzureichend umgesetzt, hat dies unmittelbare Auswirkungen auf die Qualität der Dienstleistung zwischen diesen beiden Geräten, mithin zwischen Netzbetreiber/Diensteanbieter und Endkunden, aber auch über die oben beschriebenen Mechanismen auf andere Endkunden.

Der grundlegende Mechanismus besteht darin, dass das OLT jedes angeschlossene Gerät kontrolliert und organisiert. Hierbei werden verschiedene Aufgaben und Kontrollen, wie Systemkonfiguration, Fehleranalyse, Performance-Überwachung, Durchsetzung von Sicherheitsregeln, Sender- und Empfänger-Kommunikation sowie Softwarebereitstellung übernommen. Dies erfolgt auf Basis der im PON-Standard definierten Control Channel (OMCC) und dem ONT-Management. Die nachfolgende Abbildung 3 zeigt den vorgesehenen Kommunikations- und Kontrollpfad [Quelle: ITU-T G.988, Amendment 4, (09/2021) OMCI Managed Entities] als gestrichelte Linie:

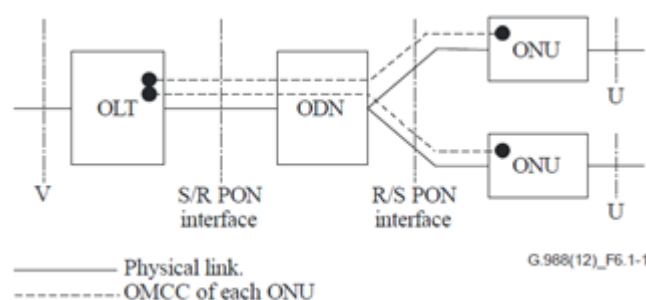


Abb. 3: Referenzmodell OMCI mit Kommunikationspfad

Hier wird deutlich, dass die Qualitätskonfiguration nicht auf das als passiver Netzabschlusspunkt vermeintlich in Betracht kommende R/S PON Interface (das in der Praxis als Anschlussdose in der Wand ausgeführt ist) zugreift. Dies ist auch nicht möglich, da ein passives Interface solche Aufgaben nicht ausführen kann, sondern eine eigene Logik nötig ist. Vielmehr werden QoS-Vereinbarungen, -Konfigurationen und -Absicherungen immer auch das ONT bzw. ONU

(so die Terminologie der IEEE bzw. ITU für das gleiche Netzelement, wobei das ONU eher eine ART multiples ONT meint) einbeziehen müssen.

Die PON-Standards definieren die OMCI dabei bewusst so, dass Anbieter modulare Dienste und SLA anbieten können, um die unterschiedlichen Anforderungen der Kunden (Privat, Geschäftskunden, Wholesale) zu erfüllen. Verschiedene Dienste haben unterschiedliche Anforderungen und Erfordernisse, welche auch in dem jeweiligen Netz funktionieren müssen. Aufgrund unterschiedlicher Parameter und verschiedener Aufbauweisen sowie technischer Ausstattungen entstehen für die Dienstbereitstellung allerdings eine Vielzahl an Permutationen, für die alle sichergestellt werden muss, dass die Dienste und Services jeweils kompatibel und interoperabel sind. Dazu muss ein Informationsaustausch über die OMCI erfolgen, für den sog. protokollabhängige MIBs genutzt werden, welche abstrakte Darstellungen der Ressourcen und Services im ONT darstellen. Die Nutzung der MIBs stellt sicher, dass das ONT durch das OLT genauso konfiguriert und überwacht wird, wie es für die Diensteebringung und die QoS-Anforderungen nötig ist, weswegen die einzelnen MIBs im Standard auch als ‚Managed Entities‘ (ME) bezeichnet werden. Allerdings ist nur ein geringer Teil dieser ME zwingend vorgeschrieben; das Einrichten und Umsetzen weiterer ME ist von der Netzarchitektur und dem Funktionsumfang, welchen die Hersteller (auf beiden Seiten) unterstützen bzw. implementieren, abhängig.

a. QoS-Sicherung im Upstream

Wie oben dargelegt, ist die Störung des Upstreams das augenfälligste Problem, das es nicht nur den störenden Endkunden selbst, sondern darüber hinaus auch andere Endkunden betreffen kann. Hier ist eine direkte Absicherung nur mit den in den Standards für genau diese Zwecke vorgesehenen Methoden möglich. Das bedeutet, dass konkrete Konfigurationen in einem wohldefinierten Format dem ONT durch das OLT per OMCI ME vorgegeben werden. Ob diese indes vom ONT richtig interpretiert und umgesetzt werden, kann nicht mehr verifiziert werden. Hier muss sich der jeweilige Netzbetreiber darauf verlassen, dass die Umsetzung der Vorgaben des Standards, aber auch die spezifischen Abweichungen vom ONT richtig verstanden und beachtet werden. Einzig Interoperabilitätstests bieten hier eine mittelbare Absicherung, weswegen genau diese Mechanismen einen zentralen Baustein dieser Tests darstellen.

Um einen Eindruck der Komplexität einer QoS-Absicherung zu erhalten, mag beispielhaft die Konfigurationsmatrix für einen Aspekt der Upload-QoS herhalten:

Betrachtet wird die Funktionalität DBA – Dynamic Bandwidth Assignment

Gemäß PON-Standard wird die Upstream-Bandbreite vom OLT jedem einzelnen ONT dynamisch vorgegeben. Dabei werden verschiedene Parameter genutzt, von denen hier nur eine Auswahl wiedergegeben werden kann:

VLAN:	1:1 oder N:1, tagged oder untagged, VLAN per Service, VLAN per UNI
pbit:	1–7

Die Zuweisung und Gruppierung ist anbieterspezifisch, z. B. Beispiel: Voice (pbit 5, 6), Data (pbit 0, 1, 2, 3, 4, 7) [Referenz: L2BSA II Technische Spezifikation V2.1 2014]

TCONT: Typ 1 -4

Anzahl der TCONTs pro TCONT Typ

Gesamtanzahl der TCONT (abhängig von Chipsatz OLT, ONU, Chipsatz SDK und welche Funktion implementiert wird)

GEM: <Nummer>

Anzahl der GEM Ports pro TCONT (z. B. 1-8)

Gesamtanzahl der GEM Ports (abhängig von Chipsatz OLT, ONU, Chipsatz SDK und welche Funktion implementiert wird)

Scheduler: Single oder hierarchischer Scheduler, Typ des Schedulers SP, WRR, Mischung der Scheduler nach Dienstklassen z. B. 1SP-6WRR, 8WRR

Die jeweiligen Werte können sich bei Netzbetreibern regional (zumeist aus historischen Gründen) unterscheiden. Jede Fehlbehandlung wird mindestens dazu führen, dass die zugewiesene Bandbreite falsch allokiert wird. Im ungünstigsten Fall kann eine Fehlbehandlung dazu führen, dass falsche Zeitschlitze genutzt und so andere Endkunden gestört werden.

b. QoS-Sicherung im Vorleistungsverhältnis

Im Vorleistungsverhältnis wird ein Kunde, welcher zum Beispiel einen Layer 2-Zugang nachfragt, auf dem BNG des Netzbetreibers terminiert. Dem Nachfrager wird am BNG der Datenstrom übergeben. Neben der korrekten Adressierung („Tagging“) und Priorisierung („pbit“) ist es im Interesse des Nachfragers, dass die vereinbarten Bandbreiten und Telefoniekanäle zwischen dem Netzbetreiber und dem Nachfrager eingehalten werden. Die hierfür notwendige Limitierung der Datenrate kann durch den Nachfrager selbst vorgenommen werden. Allerdings müssen die Einstellungen hinsichtlich der Datenrate spätestens am OLT-Port erfolgen, anderenfalls besteht die Gefahr, dass das endkundeneigene Endgerät zu viel Bandbreite anfordert und somit im Frequenzband andere Endgeräte stört. Eine übermäßige dauerhafte Beleuchtung der Leitung bedeutet, dass in der PON-Architektur andere Endkunden mittels ihrer Endgeräte gar nicht mehr senden können, was einer Störung des Anschlusses gleichkommt.

Für einen reibungslosen Ablauf sowie für die Kontrolle der Kommunikation benötigt ein Nachfrager also Kontrolle über das Endgerät und somit den (bis dahin aktiven) Netzabschlusspunkt. Anderenfalls hat er keine Möglichkeit des Zugriffs auf das Endgerät, da der OLT unter der Kontrolle des Netzbetreibers steht. Liegt eine Störung in diesem Fall vor und ein Endkunde meldet dies, hat der Nachfrager keinerlei Möglichkeit, Abhilfe zu schaffen. Bei getrennten Endgeräten

ist es dem Nachfrager nicht einmal möglich Software- und Sicherheitsupdates einzuspielen, da er weder über den OLT noch den Endkunden Zugriff erhält.

2. Behebung von QoS-Verlusten

Kommt es hingegen zu Qualitätsbeeinträchtigungen durch Fehler in der Zusammenarbeit aller Instanzen, so müssen der Netzbetreiber und der Diensteanbieter in der Lage sein, die Beeinträchtigungen zu beheben. Dazu gehört es insbesondere, störende Geräte zu identifizieren und deren Verhalten zu korrigieren. Ein solcher Eingriff sollte aufgrund des Zeitfaktors in der Regel automatisiert erfolgen, wird aber in vielen Fällen auch manuelles Vorgehen erfordern. Vor allem aber liegt es auf der Hand, dass ein zwingender Bedarf daran besteht, auf störende Geräte zugreifen zu dürfen.

Das bedeutet zunächst, dass Eigentumsrechte kein Hindernis für den nötigen Zugriff darstellen dürfen. Es wäre auch – abgesehen von der rechtlichen Möglichkeit – unzureichend, Zugriffsrechte in AGB zu vereinbaren. Wegen der durchaus sinnhaften technischen Restriktionen müssen entsprechende Rechte vom Kunden aktiv eingeräumt werden, was eine Bereitschaft und technisches Know-how beim Kunden voraussetzt, die beide in der Praxis nicht bestehen.

Ein weiteres Hindernis bei der Störungsbehebung stellen Firmwareversionen aus Drittquellen dar, da die Zugriffe zumeist über andere Kanäle und Methoden implementiert sind, die manuell aufzuklären wären. Zu Aufwand und Zeitverlust kommt hier noch das Risiko hinzu, das Problem mangels entsprechender Kenntnisse der Firmware nicht beheben zu können. Und nicht zuletzt bedeutet der Eingriff in eine nicht oder wenig bekannte Umgebung auch immer ein hohes Risiko, dass das entsprechende Gerät anschließend nicht mehr oder nur nach weiteren aufwendigen Eingriffen verwendbar ist.

3. Folgen von QoS-Verlusten

Hinsichtlich der Folgen fehlender QoS sind zwei große Fallkonstellationen zu unterscheiden: Zum einen ist dies die Konstellation, in der eine Schlecht- oder Nichtleistung beim betreffenden Endnutzer eintritt; zum anderen ist die Konstellation zu bedenken, in welcher andere Endnutzer durch ein untaugliches ONT von einer Nicht- oder Schlechtleistung betroffen sind (hierunter fallen insbesondere die oben dargelegten Uploadstörungen, die ganze OLT-Ports stören). In beiden Konstellationen ergibt sich sowohl rechtlich als auch tatsächlich ein ausgesprochen hohes wirtschaftliches Risiko aus dem Anschluss ungeeigneter ONT.

a. Leistungsstörung beim Endnutzer selbst

Setzt ein Endnutzer ein von ihm beschafftes ONT ein und dieses ist nicht in der Lage, einen Service herzustellen oder lediglich in der Lage, einen unter den angegebenen Leistungsparametern bleibenden Dienst herzustellen, liegt es zwar prinzipiell auf der Hand, dass Gewährleistungsrechte aus den §§ 57 Abs. 4, 58 Abs. 1+3 TKG, 314 Abs. 2 BGB nicht in Betracht kommen (sollten).

In der Praxis sieht dies indes anders aus. Hier kommen nämlich die gesetzlichen Formulierungen zum Tragen, die erhebliche und in der Praxis kaum zu überwindende Beweiserleichterungen bzw. Beweislastumkehrungen vorsehen.

i. Minderung

Stellt ein Endnutzer – Verbraucher – mittels des von der BNetzA gestellten (oder sonst eines zertifizierten) Mechanismus fest, dass er eine zu geringe Leistung erhält, besteht zu seinen Gunsten eine gesetzliche Vermutung, dass der Tatbestand einer Minderung im Sinne des § 57 Abs. 4 TKG eröffnet ist. Dies folgt nicht nur aus dem Wortlaut der genannten Vorschrift, sondern insbesondere aus Art. 4 Abs. 4 TSM-VO⁹. Dieser fordert, dass ein Rechtsverstoß bereits mit der Feststellung der Minderleistung durch einen entsprechenden Überwachungsmechanismus feststünde. Das enthält eine gesetzliche Vermutung, die sich auf den Gedanken gründet, dass mit dem Bereitstellen eines entsprechenden Überwachungsmechanismus auch der Einfluss von Fehlerquellen außerhalb des Machtbereichs der Diensteanbieter ausgeschlossen sein würde. Ob dies tatsächlich der Fall ist, sei hier dahingestellt; jedenfalls muss eine solche Vermutung in jedem Einzelfall widerlegt werden, um eine Minderung auszuschließen.

Für den hier skizzierten Fall heißt dies, dass dem Diensteanbieter die Aufgabe zufällt, die Ungeeignetheit des angeschlossenen ONT festzustellen, geltend zu machen und im Streitfalle auch nachzuweisen. Für einen solchen Gegenbeweis dürfte nicht zu erwarten sein, dass Gerichte fehlende Interoperabilitätstests bereits ausreichen lassen, sondern eine konkrete Beweisführung in Bezug auf das konkrete Gerät fordern werden. Es verbleibt also für diese Fälle ein ganz erhebliches Minderungsrisiko, das nur mit technischer Expertise und voraussichtlich hohen Kostenrisiken (namentlich für gerichtliche Sachverständige) aus der Welt zu schaffen ist. Aber auch in den Fällen erfolgreicher Verteidigung gegen unberechtigte Minderungsbegehren verbleiben immer ein unzufriedener Kunde und ein hoher interner Aufwand für die Fallbearbeitung und Störungssuche.

Faktisch werden Diensteanbieter dem wirtschaftlich nur damit begegnen können, dass sie Minderungsrisiken durch kulante Handhabung von Minderungsbegehren – auch den hier thematisierten unberechtigten – abfangen.

ii. Außerordentliche Kündigung

Analog zum vorstehend dargelegten Minderungsrisiko entsteht unter identischen Voraussetzungen (abgesehen von der Notwendigkeit einer Fristsetzung) die Möglichkeit des Endnutzers, den Vertrag wegen der Schlechtleistung außerordentlich zu kündigen. Gerade in Fällen, in denen das vom Endnutzer eingesetzte ONT zu einer sehr deutlichen Leistungseinschränkung

⁹ Verordnung (EU) 2015/2120 des Europäischen Parlaments und des Rates vom 25. November 2015 über Maßnahmen zum Zugang zum offenen Internet und zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten sowie der Verordnung (EU) Nr. 531/2012 über das Roaming in öffentlichen Mobilfunknetzen in der Union.

oder gar zu temporären Ausfällen führt, dürfte dieser Weg für den Endnutzer naheliegen. Abgesehen davon, dass ein Wechsel des Diensteanbieters unter Beibehaltung des ungeeigneten ONT allenfalls zufällig eine Verbesserung bringen wird, entstehen auch hier wieder enorme Aufwände und Einbußen aufseiten der Diensteanbieter, die durch die bloße gesetzliche Vermutung einer Schlechtleistung herbeigeführt werden.

iii. Entstörung

Im Falle eines Ausbleibens der Dienste zeigt ein Blick auf § 58 Abs. 1+3 TKG, dass auch hier eine gesetzliche Vermutung besteht, dass dies auf den Diensteanbieter zurückzuführen sei. Insofern ist der Wortlaut des § 58 Abs. 1 S. 1 2. HS TKG eindeutig, der durch eine „... es sei denn“-Konstruktion ein Regel-Ausnahme-Verhältnis kennzeichnet.

Auch hier gilt also im Wesentlichen das Gleiche, was bereits zu Minderung und Außerordentlicher Kündigung ausgeführt wurde: Für den Diensteanbieter verbleibt ein hohes Risiko, dass die Verwendung eines ungeeigneten ONT, auf den er keinen Zugriff hat und dessen Zustand im Fall der Störung, ihm angelastet wird, weil der Nachweis der wirklichen Störungsursache entweder nicht oder nur unter unwirtschaftlichen Aufwendungen zu führen sein wird.

Dieses Risiko ist insofern jedoch besonders hervorzuheben, als die möglichen Rechtsfolgen im Gegensatz zur Minderung vom Äquivalenzinteresse entkoppelt sind. Insbesondere können die vom Gesetz angeordneten Entschädigungen nicht nur die vereinbarten vertraglichen Entgelte deutlich übersteigen, sie liegen auch deutlich höher als vernünftigerweise zu antizipierende Schäden. Insbesondere die Regelung, dass eine Entschädigung für jeden betroffenen Dienst zu leisten ist, kann enorme Forderungen nach sich ziehen, deren Abwehr in den hier in Rede stehenden Fällen immer mit einem hohen Ungewissheitsfaktor versehen bleibt.

iv. Vertragliche Ansprüche

Zusätzliche Risiken entstehen mit Blick auf die üblichen vertraglichen Ansprüche bei Verträgen mit Geschäftskunden und Vorleistungsnachfragern. Dort besteht zumeist der Bedarf, Service Level Agreements (SLAs) zu vereinbaren, welche dann bei Nutzung kundeneigener ONT nicht garantiert werden können. Hier sind zwar die gesetzlichen Vorgaben, insbesondere die zur Beweislast, nicht einschlägig. Ob von diesen indes AGB-mäßig abgewichen werden darf oder ob insofern ein gesetzliches Leitbild verletzt würde (§ 307 Abs. 2 Nr. 1 BGB), ist zumindest diskutabel. Nichtsdestotrotz verbleibt aber auch bei diesen Kunden ein hohes Maß an Unzufriedenheit, wenn die vereinbarte kurze Entstörungsfrist nicht garantiert werden kann, wenn bei einer Störung ein Zugriff auf das jeweilige kundeneigene ONT nicht durchgeführt werden kann oder ähnliche SLA-Forderung nicht erfüllt werden können, weil der Kunde auf ein vermeintliches Recht zum Anschluss eigener ONT pocht. Wenn dann noch aufgrund fehlender rechtlicher Befugnis ein Zugriff auf den kundeneigenen ONT nicht möglich ist, unterbleibt eine Behebung des Fehlers aus der Ferne und ein Techniker muss vor Ort zum Einsatz kommen. Dabei vergeht

eben nicht nur mehr Zeit, sondern es entstehen auch unvorhergesehene hohe Kosten, deren Liquidierung beim Kunden selten zu realisieren sein wird.

b. Leistungsstörung bei anderen Endnutzern

Auch für den Fall, dass ein Endnutzer durch den Anschluss eines ungeeigneten ONT für eine Störung bei anderen Endnutzern sorgt (vgl. zu den Mechanismen die Ausführungen oben), sollte rechtlich einfach dahingehend zu beantworten sein, dass dieser Endnutzer für entstandene Schäden haftbar zu machen sein wird. Die Realität – auch die rechtliche – sieht indes anders aus.

Tatsache ist nämlich, dass für gegenüber den betroffenen (anderen) Endnutzern zunächst der Diensteanbieter als Vertragspartner für entsprechende Gewährleistungsansprüche einzustehen hat, ohne auf das Fremdverschulden verweisen zu können. Dem Diensteanbieter steht allenfalls die Möglichkeit offen, etwaige Ansprüche beim betreffenden Endnutzer zu liquidieren, was indes auch rechtlichen und tatsächlichen Schwierigkeiten begegnet.

i. Keine Exkulpation

Für keines der infrage kommenden Gewährleistungsrechte der betroffenen Endnutzer besteht für den Diensteanbieter eine Möglichkeit, diese unter Verweis auf das Verschulden des den störenden ONT anschließenden Endnutzers abzuwehren.

Für Minderung und Außerordentliche Kündigung folgt dies schon unmittelbar aus der gesetzlichen Regelung in § 57 Abs. 4 TKG. Dort ist Voraussetzung für die entsprechenden Rechtsfolgen, dass die versprochene Leistung nicht in der erforderlichen Qualität zur Verfügung gestellt wird. Ein Verschulden des Diensteanbieters ist dafür nicht erforderlich, wie auch der Grund der Minderleistung insgesamt unbeachtlich ist.

Für die Störungsentschädigung hingegen ist grundsätzlich zwar ein Verschulden des Diensteanbieters zu fordern, jedoch wird dieses angesichts des Kanons an Ausnahmetatbeständen in § 58 Abs. 3 S. 1 2. HS. TKG gesetzlich fingiert. Hier eröffnet der Gesetzgeber eine Exkulpation nämlich nicht generalklauselartig, sondern nur für enumerativ aufgezählte Fälle, von denen lediglich der Fall Höherer Gewalt in Betracht kommt. Der Diensteanbieter wird also lediglich dann nicht haften, wenn die Störungsursache nicht seinem typischen Betriebsrisiko zuzurechnen ist. Ob in dem hier in Rede stehenden Fall von Höherer Gewalt auszugehen ist, ist zwar aufgrund des geringen Alters der Vorschrift nicht abschließend geklärt. Es dürfte aber eine deutliche Wahrscheinlichkeit bestehen, dass die Rechtsprechung eine Zuordnung zum typischen Betriebsrisiko vornimmt.

ii. Geringe Regresschancen

Geht man mit dem Vorstehenden davon aus, dass die Gewährleistungsansprüche der betroffenen Endnutzer – insbesondere auch die tendenziell enormen Ansprüche nach § 58

Abs. 3 TKG – durch den Diensteanbieter zu erfüllen sein werden, stellt sich die Frage, ob ein Regress beim verursachenden Endnutzer rechtlich und tatsächlich Aussicht auf Erfolg bietet. Ein solches Vorgehen ist indes realistisch betrachtet nur wenig aussichtsreich, da sowohl rechtlich bedeutende Hürden bestehen als auch eine tatsächliche Durchsetzung nur selten erfolgreich sein wird.

In rechtlicher Hinsicht wird ein Regress nur unter dem Gesichtspunkt der Vertragsverletzung, §§ 241 Abs. 2, 280 Abs. 1 S. 1 BGB, in Betracht kommen. Auch ohne Verankerung eines „Störungsverbots“ in den AGB sollte jedenfalls davon auszugehen sein, dass eine entsprechende Nebenpflicht auch ungeschrieben besteht. Das dabei notwendige Verschulden des betreffenden Endnutzers wird nach § 280 Abs. 1 S. 2 BGB zwar vermutet, dennoch dürfte für ihn durchaus eine realistische Aussicht auf Exkulpation bestehen. Hierbei ist insbesondere in Betracht zu ziehen, dass dem Recht zur freien Wahl eines (vermeintlichen) Endgerätes ein politisch hoher Stellenwert eingeräumt wird und für Endnutzer praktisch keine Möglichkeit besteht, die tatsächliche Kompatibilität eines Geräts im Vorfeld zu eruieren. Schenkt man zudem den Einlassungen des VTKE, dass Störungen praktisch nie aufträten, Interoperabilitätsprobleme durch die Hersteller im Vorfeld ausgeräumt würden und allumfassend kompatible Geräte auf einfachem Wege für jedermann zu beschaffen seien, Glauben, so führt die insgesamt komplexe Problematik dazu, dass selbst ein höchst sorgfältig vorgehender Kunde nicht in der Lage sein wird, einen ungeeigneten ONT vor dem Anschluss zu erkennen. Es besteht also durchaus die Erwartung, dass Rechtsprechung zu der Auffassung gelangen wird, dass ein Regress mangels Verschuldens ausscheidet.

Selbst aber dann, wenn ein Regressanspruch nicht am fehlenden Verschulden scheitern sollte, stellt sich immer noch die Frage nach der Wahrscheinlichkeit seiner praktischen Durchsetzung.

Dies beginnt bereits bei der Frage nach dem Schadensumfang. Ist diese bei den Störungsschädigungen und Minderungsfolgen noch einfach zu beantworten, handelt es sich bei den Folgen Außerordentlicher Kündigungen um entgangene Gewinne, die nach dem Maßstab des § 252 BGB zwar ersatzfähig sind, aber einen hohen Begründungsaufwand erfordern und in der Praxis von den Gerichten nach § 278 Abs. 1 ZPO nur geschätzt werden.

Viel bedeutsamer aber dürfte die Tatsache sein, dass insbesondere umfangreiche Regressforderungen, wie sie aus Störungsschädigungen nach § 58 Abs. 3 TKG sehr leicht entstehen können, nur schwer einzutreiben sind. Der weit überwiegende Teil betroffener Endkunden wird mangels Liquidität kaum in der Lage sein, diese Forderungen zu erfüllen. Ob dem Endkunden hier eigene Regressforderungen – etwa gegen den Verkäufer/Hersteller – oder eine Versicherung zur Seite stehen, erscheint in diesem Kontext eher fraglich, sodass dies einen praktisch zu vernachlässigenden Faktor darstellt.

Insgesamt ist zudem noch nicht in Rechnung gestellt, dass die Durchsetzung derartiger Forderungen insbesondere vor dem Hintergrund der nahe liegenden Exkulpationsmöglichkeit der Endnutzer auch ein unmittelbares (Rechtsverfolgungskosten) und mittelbares

unternehmerisches Risiko darstellt. Entsprechende Presseberichte mögen zwar eine gewisse erzieherische Wirkung haben und andere Kunden bei der Auswahl von Geräten beeinflussen; in erster Linie aber haben sie eine negative Imagewirkung, die erheblichen wirtschaftlichen Schaden mit sich bringen kann.

VI. Folgen der beantragten Festlegung des Netzabschlusspunkts

Die unterzeichnenden Verbände respektieren, wie bereits mehrfach und auch in diesem Schreiben ausgeführt, dass der Innovationswettbewerb ein zentrales und hohes Schutzgut ist, welches der sog. Endgerätewahlfreiheit zugrunde liegt. Wir teilen die Auffassung, dass ein stetiger Innovationsdruck unerlässlich ist, um technischen Fortschritt und neue Ideen zum gesamtwirtschaftlichen Nutzen aber auch zum Nutzen des Endkunden fruchtbar zu machen.

Wir betonen aber erneut, dass dieses wichtige Schutzgut nicht dazu führen darf, technische Realitäten und rechtliche Vorgaben zu ignorieren. Hier hatten wir zuletzt in unserem verbändeübergreifenden Antrag vom 09.06.2022 dargelegt, warum wir der Auffassung sind, dass für PON bereits aus rechtlichen Gründen – eben wegen des zwingenden technischen Umstands, dass eine Adressierung des Endkunden erst im ONT möglich ist und nicht vorgelagert erfolgen kann – der Netzabschlusspunkt nur an der Ethernet-Schnittstelle des ONT liegen kann.

Dessen ungeachtet erscheint es uns aber weiterhin wichtig, auch die Frage der Folgen einer solchen Festlegung für die Endkunden und den Innovationswettbewerb noch einmal ausführlich darzustellen.

1. Den Endkunden verbleibende Funktionalitäten

Grundlegend und wesentlich ist hier zunächst die Tatsache, dass die Festlegung auf einen Netzabschlusspunkt hinter dem ONT diesen zwar der Wahlfreiheit des Endkunden entzieht, ihm aber immer noch die Freiheit bei der Auswahl des Routers belässt. Dies gilt auch für den Fall integrierter Geräte, deren Routerkomponente jederzeit zugunsten des vom Endkunden präferierten Routers abgeschaltet werden kann.

Ausgehend hiervon kapriziert sich die Frage also auf die Funktionalitäten, welche ONT und Router dem Endkunden zur Verfügung stellen und deren Bedeutung.

Ein ONT hat folgende Funktionalitäten:

- (1) Es übersetzt die optischen Signale aus dem Glasfasernetz in eine für den Router verständliche Form und umgekehrt.
- (2) Es wickelt die Kommunikation mit dem OLT ab, wobei die Aushandlung der Zeitschlitzes für den Upload und die Absicherung der QoS-Parameter im Fokus stehen.
- (3) Es filtert eingehenden Verkehr nach einem endkundenindividuellen Parameter, um so eine individuelle Adressierung des Verkehrs zu ermöglichen.

- (4) Es stellt geeignete Informationen zur Sicherung des Netzes, wie die Alarmierung (z. B. Dying GASP) und Health Parameter (z.B. Optische Werte) im Fehlerfall

Alle diesen Funktionalitäten sind natürlich für den Kunden wichtig. Sie haben aber ein hervorstechendes gemeinsames Merkmal: Alle Funktionen sind für die Erbringung der mit dem Anbieter vereinbarten Dienste essenziell. Ihre ordnungsgemäße Arbeit ist also in beiderseitigem Interesse, wobei das Erfüllungsrisiko beim Diensteanbieter liegt, er also das deutlich höhere Interesse am Funktionieren haben muss. Indes sind diese Funktionen nur bei einer vollständigen Interoperabilität gewährleistet.

Ein Router hat mehrere Kernfunktionalitäten.

- (1) Er ist der Punkt, an dem die Dienste seitens des Internet Service Providers (z. B. PPPoE Einwahl, IP Adresse des ISP) erbracht werden.
- (2) Er vernetzt andere Endgeräte (Laptops, Desktop-Rechner, Tablets etc.) miteinander in einem Heimnetz, steuert dafür deren Adressierung.
- (3) Er stellt den im Heimnetz angeschlossenen Endgeräten als Gateway den Zugang zum Internetdienst zur Verfügung.
- (4) Er bietet Sicherheitsfunktionen wie Paketfilter, Portblocking u. ä. zur Verfügung.

Er hat darüber hinaus je nach Ausstattung weitere Funktionalitäten, die indes so vielfältig sind, dass ihre Aufzählung hier unvollständig bleiben muss.

- (1) Er stellt Telefoniefunktionen für angeschlossene Telefoniegeräte zur Verfügung.
- (2) Er stellt Medienstreaming im Heimnetz zur Verfügung.
- (3) Er stellt Verwaltungsfunktionen für IoT-Geräte zur Verfügung.
- (4) Er stellt die Möglichkeit für Fernzugriffe zur Verfügung.
- (5) Er stellt Zugriffsbeschränkungen (Kindersicherungen, Zeitbeschränkungen, Blacklists/Whitelists) zur Verfügung.
- (6) Er stellt Gastzugänge zur Verfügung.

Auf der anderen Seite kommuniziert der Router nicht mit dem OLT selbst – er hat eine Verbindung mit dem ONT, welches die Kommunikation im Zugangsnetz abwickelt.

Augenfällig ist insoweit zunächst, dass die Kernfunktionen sich erneut auf die Erbringung der mit dem Anbieter vereinbarten Dienste beziehen, wobei sie ihren Fokus jedoch nicht auf die Kommunikation mit anderen Netzelementen richten, sondern – quasi in die „Gegenrichtung“ – auf das Heimnetzwerk abzielen. Dessen Funktionieren liegt aber wie bereits der Name Heimnetz suggeriert im alleinigen Interessen- und Risikobereich des Endkunden.

Die zusätzlichen Funktionalitäten, welche ein Router zu erbringen vermag, haben mit der Erbringung der TK-Dienste denn auch nur insoweit zu tun, als sie häufig dessen Funktionieren voraussetzen. Umgekehrt sind sie für die Dienstleistung komplett irrelevant, sie haben also lediglich für den Endkunden eine Bedeutung, für diesen indes häufig eine große.

Die alles äußert sich denn auch darin, dass ONT und Router völlig unterschiedliche Lebenszyklen haben. Während bei Routern von einem Generationswechsel – also der Markteinführung einer Version mit völlig neuen Funktionalitäten - innerhalb von 2 Jahren zu rechnen ist, ist bei ONT mit Zyklen von 10 Jahren – bei XGSPON sogar deutlich mehr – zu rechnen. Dies liegt vor allem darin begründet, dass Routerfunktionalitäten unmittelbar nachgefragt werden und diese Nachfrage durch den Hersteller rasch zu befriedigen ist.

Als Beispiel kann hier die Ausgestaltung des WLAN-Standards herangezogen werden, welcher sich binnen kurzer Zeit mehrfach fortentwickelt(e). Ein Endkunde, der sein Endgerät für 10 Jahre nutzt, würde damit mehrere WLAN-Generationen „verpassen“ und etwa heute anstelle des derzeitigen aktuellen WLAN-Standards 6 ggfs. nur WLAN Version 3 nutzen. Ihm würde damit insbesondere bei einer gebuchten Gigabitgeschwindigkeit ein Großteil der gebuchten Geschwindigkeit verloren gehen.

Gegenüber Routern werden ONT nicht dadurch im Sinne eines Generationensprungs fortentwickelt, dass Kunden nach besserer Leistung verlangen und der Gerätehersteller eine Lösung entwickelt. Vielmehr entwickeln Netzausrüster und Netzbetreiber solche Innovationen in Standardisierungsgremien wie ITU und IEEE, woraufhin zunächst die Netzausrüster entsprechende Netzelemente (etwa OLT) in den Markt bringen und Netzbetreiber sie in ihre Netze integrieren. Erst danach folgen die CPE-Hersteller diesen Vorgaben, sodass deutlich mehr Zeit vergeht.

2. Auswirkungen auf den Innovationsdruck

Um die Frage nach einem wirksamen Innovationsdruck zu beantworten, ist zunächst festzuhalten, dass dieser dort am größten ist, wo Entwicklung und Bedarf – also Angebot und Nachfrage – unmittelbar aufeinandertreffen. Der höchste Druck geht folglich von dem Marktteilnehmer aus, welcher das größte Interesse an einer konkreten Innovation hat. Daneben ist jedoch auch ein weniger wirksamer mittelbarer Innovationsdruck in Szenarien möglich, in denen unmittelbare Nachfrage gestuft weitergereicht wird.

Geht man mit dem vorstehenden Abschnitt davon aus, dass insbesondere die zusätzlichen Routerfunktionalitäten für den Endkunden wichtig sind, wird klar, dass diesbezüglich ein Innovationsdruck in allererster Linie von den Endkunden kommen wird. Fragen diese bestimmte Features nach – etwa die Automatisierung und Fernsteuerung von Heimgeräten –, wird deren Entwicklung vorangetrieben. Diensteanbieter, die solche Features ihren Kunden zur Verfügung stellen, weil sie einen solchen Bedarf vermuten oder vernehmen, können aber eine ebenfalls wichtige Rolle – gerade als Multiplikator der Einzelinteressen spielen.

Ähnliches gilt für die Kernfunktionalitäten der Router, bei denen indes schon seit langem wenig Bedarf an Innovationen zu verzeichnen ist.

Für die vom ONT gestellten Features hingegen ist der größte Bedarf an Innovationen bei den Diensteanbietern zu erkennen, welche von besseren Leistungsparametern profitieren können

und umgekehrt das Risiko schlechter Leistungen tragen. Natürlich haben auch Endkunden ein Interesse an einer guten Leistung, sie können jedoch nur sehr bedingt von Leistungsverbesserungen profitieren (etwa bei energetischen Verbesserungen). Damit lassen sich die Interessen der Beteiligten und ihre Wertigkeiten sehr plastisch mit einem Restaurantbesuch umschreiben: Sowohl der Restaurantbesitzer als auch der Besucher haben ein intrinsisches Interesse daran, dass das angebotene Essen möglichst gut ist. Allerdings würde keiner von beiden auf die Idee kommen, dass es irgendwie sinnvoll wäre, dass der Kunde mit eigenem Herd und Kochgeschirr erscheint und lediglich nach Rezept und Zutaten verlangt. Augenscheinlich würden alle Beteiligten sich hier von vornherein einig sein, dass jeder davon profitiert, wenn jeder seinen Teil beiträgt – der Koch mit dem fertigen Essen und der Gast mit dem Entgelt. Dass diese Wertigkeit bei Telekommunikationsleistungen eine andere sein sollte, leuchtet hingegen nicht ein. Auch der TK-Endkunde erwartet einen möglichst guten Dienst und würde widerigfalls seinen Anbieter wechseln, warum es für ihn oder sonst wen sinnvoll sein sollte, dass der Endkunde diese Aufgabe teilweise an sich nimmt, leuchtet nicht ein.

Hinzu kommt zudem, dass die Endkunden ihre Nachfrage nicht so effektiv äußern können wie bei den Routerfunktionalitäten. Während interessierte Kunden mit den oben beschriebenen Features gewiss etwas verbinden und auch gezielt danach fragen, sind technische Innovationen in ONT komplex und für Laien völlig unverständlich. Nur extrem wenige Kunden würden verstehen, was hinter bestimmten Techniken (etwa einer aktiven Pufferoptimierung) steht, geschweige denn danach suchen. Außerdem sind alle Innovationen, die in ONT implementiert werden könnten, nur dann überhaupt sinnvoll, wenn sie ein Gegenstück in den Netzen haben, also dort unterstützt werden. Dazu bedarf es wie oben dargelegt einer Standardisierung, welche dann von den Herstellern der OLT umzusetzen und von den Netzbetreibern in ihre Netze zu integrieren ist, bevor sie sinnvoll in den ONT implementiert werden kann. Auch hier kann ein innovationstreibender Nachfragedruck durch Endkunden allenfalls mittelbar über deren Diensteanbieter an die Standardisierungsorganisationen und von dort an die Hersteller der OLT und im Weiteren an die Hersteller der ONT weitergereicht werden.

Wird damit klar, dass für ONT unmittelbarer und wirksamer Innovationsdruck nur von den Diensteanbietern ausgehen kann, so wird auch deutlich, welchen Effekt die Vermarktung von ONT an Endkunden hat: Diese richten ihr Augenmerk lediglich auf die Routerfunktionalitäten und stehen Innovationen bei den ONT bestenfalls gleichgültig gegenüber. Dies führt also nicht zu einer Steigerung der Innovativität, sondern zu einem Nachlassen des Innovationsdrucks, da der wirksamere unmittelbare Druck der Diensteanbieter zurückgedrängt wird. Dies ist das Gegenteil des Effekts, den man mit der Endgerätewahlfreiheit erreichen möchte! Deutlich sinnvoller und auch nachhaltiger ist da eine Trennung von ONT und Router, zumal die unterschiedlichen Entwicklungszyklen (s. o.) eine solche Trennung (auch physisch) nahelegen. Legt man nämlich für den Routeranteil eines integrierten Gerätes einen 2-jährigen Generationswechsel zugrunde, würde der typischerweise an genau diesen Funktionen interessierte Endkunde das Gerät 4 Mal durch ein neueres ersetzen, bevor ein Generationswechsel einen ONT-Tausch erfordern würde. Außer für die wirtschaftlichen Belange der CPE-Hersteller erscheint dies für niemanden sinnvoll. Den Endkunden kostet es deutlich mehr Geld als nötig und die Umwelt

wird mit vorzeitig ausgesonderten Geräten und einer damit einhergehenden Ressourcenverschwendung belastet.

)

Anlage – Kommentierung zu

*“Examples of Fibre Telecommunication Terminal Equipment / Integrated Access Devices (IAD)
Available in Worldwide Retail Markets
(08/2022)”*

Hersteller	Technologie	Gerät	Link	Kommentar
EU/Deutschland				
Telekom	Fiber / GPON	Speedport Smart 4 Plus	https://www.telekom.de/zuhaus/geraete-undzubehoer/wlan-und-router/speedport-smart-4-pluskauf	ONT für Telekom-GPON, keine Interoperabilität in anderen PON
Sercom (Deutsche Telekom)	Fiber / GPON	Speedport Modem 2	https://www.amazon.de/-/en/Deutsche-Telekomflexible-connection-Speedport/dp/B09159SSJB	Lediglich ONT ohne Routerfunktion; Router muss separat angeschlossen werden.
Telekom	Fiber / GPON /DSL	Speedport Pro Plus	https://www.mediamarkt.de/de/product/_telekom-speedport-pro-plus-2721714.html?	Router, welcher in PON nur zusammen mit einem ONT zu nutzen ist
Telekom	Fiber / GPON	Digitalisierungsbox	https://www.telekom.de/hilfe/geraetezubehoer/router/digitalisierungsbox/premium-2 https://blog.jaseg.de/posts/telekom-gpon-sfp/	ONT für Telekom-GPON, keine Interoperabilität in anderen PON
Zyxel	Fiber / GPON	PMG3000-D20B	https://geschaeftskunden.telekom.de/internetdsl/produkt/digitalisierungsbox-glasfasermodemkaufen	SFP-Modul, welches im PON der Telekom genutzt werden kann; stellt für sich allein jedoch kein ONT dar

AVM	Fiber / GPON	FRITZ!Box 5590 Fiber	https://www.amazon.de/AVM-Glasfasermodem-DECT-Basis-5-Gigabit-Port-Deutschland/dp/B09ZD4LFR3	ONT mit Interoperabilitätstests in verschiedenen PON; keine Interoperabilität in allen PON
AVM	Fiber / GPON	FRITZ!Box 5530 Fiber	https://www.amazon.de/AVM-Glasfasermodem-2-5-Gigabit-LAN-Port-geeignet-Deutschland/dp/B08RB83RZ4/	ONT mit Interoperabilitätstests in verschiedenen PON; keine Interoperabilität in allen PON
AVM	Fiber / GPON	FRITZ!Box 5491 Fiber	https://www.notebooksbilliger.de/avm+fritz-box+5491+b+ware+663575	ONT mit Interoperabilitätstests in verschiedenen PON; keine Interoperabilität in allen PON
LANCOM	Fiber / GPON	LANCOM 1790EF	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1790ef	Link existiert nicht; nicht als ONT nicht einsetzbar ohne LANCOM SFP GPON1, für das weitere Kosten anfallen
LANCOM	Fiber / GPON	LANCOM 1800EF	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1800ef	Link existiert nicht; nicht als ONT nicht einsetzbar ohne LANCOM SFP GPON1, für das weitere Kosten anfallen
LANCOM	Fiber / GPON	LANCOM 1800EFW	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1800efw	Link existiert nicht; nicht als ONT nicht einsetzbar ohne LANCOM SFP GPON1, für das weitere Kosten anfallen
LANCOM	Fiber / GPON	LANCOM 1800EFW-5G	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1800ef-5g	Link existiert nicht; nicht als ONT nicht einsetzbar ohne LANCOM SFP GPON1, für das weitere Kosten anfallen
LANCOM	Fiber / GPON	LANCOM LANCOM 1900EF	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1900ef	Link existiert nicht (womöglich gemeint: https://www.lancom-systems.de/fileadmin/download/LC-1900EF/1900EF_DE.pdf)

				Gerät ist lediglich als Router ausgewiesen und wird per Ethernet angebunden; SFP-Modul ist jedoch mit weiteren Kosten möglich
LANCOM	Fiber / GPON	LANCOM 1900EF-5G	https://www.lancom-systems.de/produkte/routersdwan/vpn-router/lancom-1900ef-5g	Link existiert nicht Gerät ist lediglich als Router ausgewiesen und wird per Ethernet angebunden; SFP-Modul ist jedoch mit weiteren Kosten möglich
LANCOM	Fiber / GPON	LANCOM SFP-GPON-1	https://www.lancom-systems.de/produkte/optionenzubehoer/zubehoer/lancom-sfp-gpon-1	Kein ONT, sondern SFP-Modul, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
Draytek	Fiber / GPON	Vigor2925FVn	https://www.draytek.de/Glasfaser.html	Nicht als ONT nicht einsetzbar ohne SFP Modul, für das weitere Kosten anfallen
Draytek	Fiber / GPON	Vigor 2860FVn	https://www.draytek.de/Glasfaser.html	Nicht als ONT nicht einsetzbar ohne SFP Modul, für das weitere Kosten anfallen
Turris	Fiber / GPON	Omnia RTROM01-FCC	https://www.turris.com/en/omnia/overview/	Nicht als ONT nicht einsetzbar ohne SFP Modul, für das weitere Kosten anfallen
Ubiquiti	Fiber / GPON	UF-Nano	https://www.amazon.de/-/en/0810354025761-Ubiquiti-Uf-Nano/dp/B076KHSXTB	Kein ONT, sondern per Ethernet angebundener Router
Televes	Fiber / GPON	ONT Hospitality (769514)	https://www.televes.com/uk/769514-ont-hospitality-wifi-ac-module.html	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber / GPON	TX-VG1530	https://www.tp-link.com/baltic/homenetworking/pon-sfu-hgu/tx-vg1530/	Der Link existiert nicht (womöglich gemeint: https://www.tp-link.com/ae/service-provider/cable/tx-vg1530/#overview)

				ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber / GPON	N300	https://www.ebay.de/itm/265710040345	Kein ONT, sondern WLAN-Signalverstärker, vgl. Beschreibung unter https://www.tp-link.com/de/home-networking/range-extender/tl-wa850re/
Halny	Fiber / GPON	HL-1GE	https://www.amazon.de/-/en/terminal-downstreamupstream-gigabit-interface-White/dp/B09YD1XGD7	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
Elfcam	Fiber / GPON	Onu	https://www.amazon.de/-/en/Elfcam%C2%AEGPON-Ethernet-optical-interface/dp/B09LD3FGVN	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar Gerät selbst ist nicht verfügbar
Tenda	Fiber / GPON	HG7	https://www.tendacn.com/de/product/HG7.html	Kein ONT Beschreibung lässt zwar ONT vermuten, auf den Bildern aber lediglich 2 LAN-Ethernet-Anschlüsse zu erkennen
D-Link	Fiber / GPON	DPN-101G	https://www.dlink.lt/mn/products/1383/2624.html	Link führt nicht zum benannten Gerät; lediglich auf russischem Pendant abruf- und verfügbar keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar

D-Link	Fiber / GPON	DPN-144DG	https://www.dlink.lt/mn/products/1383/2176.html	<p>Link führt nicht zum benannten Gerät; lediglich auf russischem Pendant abruf- und verfügbar</p> <p>keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar</p>
D-Link	Fiber / GPON	DPN-124G	https://www.dlink.lt/mn/products/1383/2177.html	Gerät und Befund identisch mit vorstehendem Gerät DPN-144DG
D-Link	Fiber / GPON	DPN-1021G	https://www.dlink.lt/mn/products/1383/2175.html	<p>Link führt nicht zum benannten Endgerät; lediglich auf russischem Pendant abruf- und verfügbar</p> <p>keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar</p>
EchoLife	Fiber / GPON	EG8280P	https://www.router-switch.com/eg8280p.html	Ethernet-Switch, der nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar ist; keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
Comtrend	Fiber / GPON	GRG-4267uf	https://www.aleashop.es/gpon/ont/ont-gponcomtrend-grg-4267uf.html	<p>Link ist: https://www.comtrend.com/dbase/upload-img/download/DS_GRG-4267uf_R1.0_031921.pdf</p> <p>ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar</p>

Comtrend	Fiber / GPON	GRG-4260	https://www.aleashop.es/gpon/ont/ont-gponcomtrend-grg4260us.html	<p>Link ist: https://www.comtrend.com/dbase/upload-img/download/DS_GRG-4260us_R1%200_031821.pdf</p> <p>ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar</p>
Huawei	Fiber	EG8245Q	https://www.aleashop.es/ont-gpon-huawei-eg8245q.html	<p>Link ist: https://e.huawei.com/de/products/enterprise-transmission-access/access/onu/eg8245q</p> <p>ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar</p>
Huawei	Fiber	EG8245H5	https://www.aleashop.es/gpon/ont/ont-gponhuawei-eg8245h5.html	<p>Link ist: https://e.huawei.com/at/products/enterprise-transmission-access/access/onu/echolife-eg8245h5</p> <p>Beschreibung als ONT unzutreffend, da nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar</p>
Huawei	Fiber	EG8145v5	https://www.aleashop.es/gpon/ont/ont-gponhuawei-eg8145v5.html	<p>Link ist: https://e.huawei.com/za/products/optical-terminal/echolife-eg8145v5</p> <p>Beschreibung als ONT unzutreffend, da nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar</p>

Huawei	Fiber	EG8141A5	https://www.aleashop.es/gpon/ont/ont-gponhuawei-eg8141a5.html	<p>Link ist: https://e.huawei.com/de/products/enterprise-transmission-access/access/ont/eg8141a5</p> <p>Beschreibung als ONT unzutreffend, da nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar</p>
Mikrotik	Fiber	PowerBox Pro	https://mikrotik.com/product/RB960PGS-PB	Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar
Mikrotik	Fiber	hEX S	https://mikrotik.com/product/hex_s	Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar
Mikrotik	Fiber	hEX PoE	https://mikrotik.com/product/RB960PGS	Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar
Mikrotik	Fiber	RB4011iGS+RM	https://mikrotik.com/product/rb4011igs_rm	Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar
Mikrotik	Fiber	RB2011iLS-IN	https://mikrotik.com/product/RB2011iLS-IN	Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar
NuCom	Fiber / GPON	NC8800AC	https://www.aleashop.es/gpon/ont/ont-gponnucom-nc8800ac.html	<p>Link ist: https://www.myleashop.com/documentation/NC8800AC.pdf</p> <p>Nicht ohne SFP Modul, für das weitere Kosten anfallen, als ONT einsetzbar</p>
Optera	Fiber / GPON	i6405 FTU	<p>https://icotera.com/media/1475/icotera-ftth-cpe-iseries-product-catalogue-v52.pdf</p> <p>https://www.proshop.de/Datenelektronik/Icotera/i6405-00-with-ftu/2750164</p>	Kein ONT, sondern Router, da erkennbar nur LAN-Ethernet-Ports vorhanden

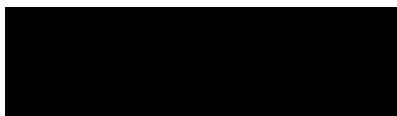
Televes	Fiber / GPON	ONT-Modul Home	https://www.televes.com/de/769502-ont-modul-home.html https://www.amazon.de/Televes-Modul-GPON-Ont-WLAN/dp/B01LCZQDRA/	Kein ONT, sondern Router, da erkennbar nur LAN-Ports vorhanden
TP-Link	Fiber / GPON	Archer CR500 XN020-G3v	https://service-provider.tp-link.com/gpon/xn020-g3v/	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber (GPON Modem, VoIP)	XR500v (Archer) TX-6610	https://service-provider.tp-link.com/gpon/archer-xr500v/	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber (GPON Modem)	FIBRA	https://www.amazon.de/TP-Link-WiFi-Router-Fibra-300mb/dp/B07G5JW9PP	Spezifikation nicht aufklärbar
TP-Link	Fiber / GPON	TX-6610	https://www.amazon.de/TP-Link-TX-6610-1-Port-Gigabit-GPON-Terminal/dp/B019M0IP2I	Spezifikation nicht aufklärbar
FS	Fiber / GPON	GPON SFP Transceiver Modul mit DDM - GPON SFP ONU Stick mit Mac	https://www.fs.com/de/products/133619.html	Kein ONT, sondern SFP-Modul, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
Televes	Fiber / GPON	Basic ONU module (769507)	https://www.televes.com/uk/769507-basic-onumodule.html	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
USA				

Ubiquity	Fiber	UF-Nano	https://www.amazon.com/dp/B077BFMJGL	Kein ONT, sondern Router, da erkennbar nur LAN-Ports vorhanden
CENTURY-LINK	Fiber	Greenwave C4000XG	https://www.amazon.com/-/de/dp/B08BHNWR34/r	Kein ONT, sondern Router, da erkennbar nur LAN-Ports vorhanden.
NBS	Fiber	BGW-320 500 802.11a	https://www.amazon.com/-/de/dp/B08PCRYJPW/	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber	TX-6610	https://www.tp-link.com/ae/serviceprovider/gpon/tx-6610/	Spezifikation nicht aufklärbar
Optera	Fiber	i6405 FTU	https://icotera.com/media/1475/icotera-ftth-cpe-iseries-product-catalogue-v52.pdf https://www.proshop.de/Datenelektronik/Icotera/i6405-00-with-ftu/2750164	Gerät mit unbekannter Spezifikation, soweit erkennbar aber kein ONT, sondern Router, da erkennbar nur LAN-Ports vorhanden
China				
Diverse	Fiber	Diverse	https://www.taobao.com/ Search: „GPON Router“	Website ohne vertiefte Mandarin-Kenntnisse nicht verwendbar; einige Endgeräte mit lediglich Ethernet-Anbindungsmöglichkeiten
Huawei	Fiber	HG8120C	https://www.a.ubuy.com.kw/en/product/5C6C6H0AI-hg8120c8321rhgu2-1dibili-hg8120c	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar
TP-Link	Fiber	Ep110	https://www.a.ubuy.com.kw/en/product/1HKT1LOIO-tp-link-tl-ep110-gigabit-cat-broadband-catepon-china-telecom-mobile-pon-terminal-tlgp110-gigafiber-broadband-gpon	Link ist: https://www.tp-link.com/latam/home-networking/pon-sfu-hgu/tl-ep110/ ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON

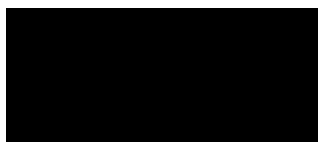
				oder BBF-Zertifizierung oder BBF-Zertifizierung verfügbar
Linkwell	Fiber	BT-762XR	https://de.aliexpress.com/item/1005001727917969.html	ONT, jedoch keine Informationen zur Interoperabilität mit verschiedenen PON oder BBF-Zertifizierung verfügbar

Wir gehen davon aus, dass im Rahmen dieser Stellungnahme alle im Termin vom 27. Februar 2023 angesprochenen Themen ausführlich erörtert worden sind und stehen für Rückfragen gerne zur Verfügung. Wir freuen uns auf die weitere Diskussion im Zuge einer Verfahrenseinleitung.

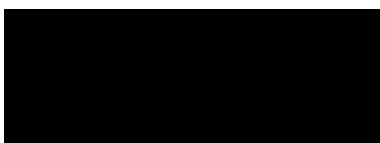
Mit freundlichen Grüßen



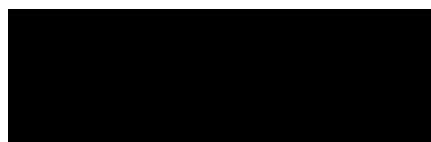
Dr. Andrea Huber
Geschäftsführerin ANGA e. V.



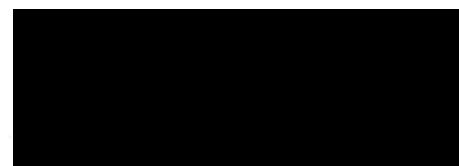
Dr. Heiko Schäffer
Geschäftsführer VKU-Zentralabteilung



Dr. Stephan Albers
Geschäftsführer BREKO e. V.



Wolfgang Heer
Geschäftsführer BUGLAS e. V.



Jürgen Grützner
Geschäftsführer VATM e.