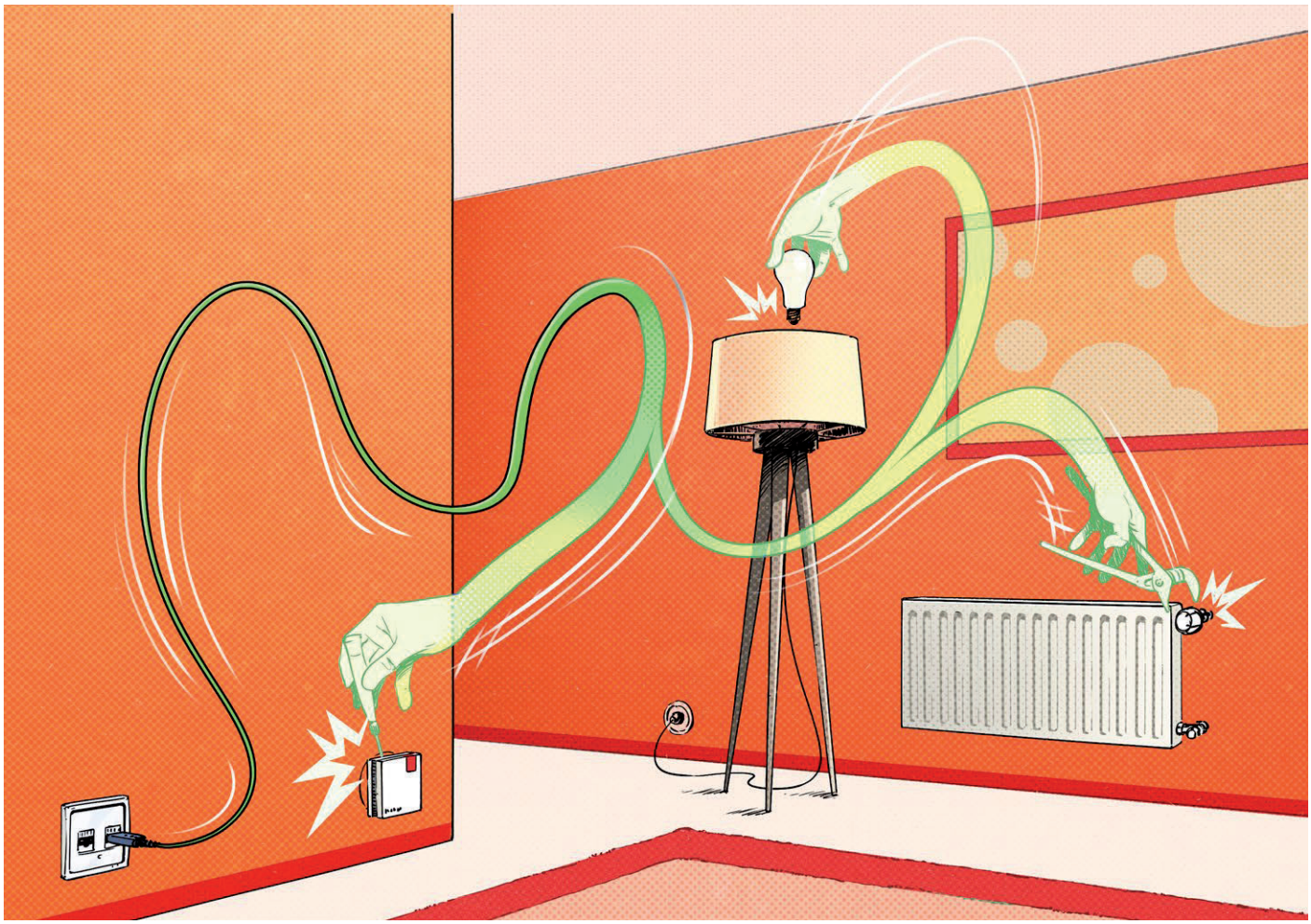


Bild: Albert Hulm

Stille Hilfsmission

Wie Provider Heimnetze und Router fernwarten

Wenn das Netzwerk lahmt, sind sachkundige Helfer selten unmittelbar zur Stelle, sodass sich IT-ferne Nutzer normalerweise gedulden müssen. Doch seit einer Weile springen Provider als Instant-Retter in die Bresche. Der Schlüssel dafür ist das Fernwartungsprotokoll TR-369.

Von Roland Riedel und Dušan Živadinović

Ob mangels Zeit, Lust oder Know-how: So wie nur wenige Nutzer ihr Auto selbst reparieren, so überlässt es auch die Mehrzahl der Internetnutzer lieber Fachleuten oder Tüftlern, Netzwerkprobleme zu lösen. Doch bis der beauftragte Experte vor Ort erscheint, kann es Tage dauern.

Daher bieten manche Internet-Provider ihren Kunden an, bestimmte Netzwerk- oder WLAN-Wehwehchen per Fernwartung zu beseitigen, denn schließlich sitzen sie netzwerktechnisch unmittelbar am Kundenanschluss und können die zur Analyse erforderlichen Statusmeldungen auf Kundenwunsch sogar rund um die Uhr abrufen.

Die Rechnung dahinter ist einfach: Schnell abgestellte Netzwerkmissstände verbessern die Kundenzufriedenheit und erhöhen die Kundenbindung. Wenn zumindest ein Teil der Wartungsarbeiten automatisch abläuft, entlastet das zudem die Hotline.

Erste Anläufe dazu unternahmen einzelne Netzbetreiber schon vor Jahrzehnten, etwa indem Fachleute von der Netzwerkseite aus den Leitungsdurchgang und die Übertragungsgüte gemessen haben und auf dieser Basis das weitere Vorgehen veranlassten. Im Jahr 2004 definierte dann das Broadband Forum mit TR-069 ein Fernwartungsprotokoll, mit dem sich viele Überwachungs- und Wartungstätigkeiten automatisieren lassen, darunter etwa die Anschluss- und Diensteeinrichtung. Im

c't Hardcore

Broadband Forum entwickeln Netzbetreiber, Internet Service Provider und Endgerätehersteller eine Vielzahl an Protokollen für den eigenen Bedarf.

Aber so sehr manche Provider heute noch für TR-069 dankbar sind, den aktuellen Szenarien und Anforderungen ist es mit seinem langsamen Verbindungsaufbau und den schwerfälligen XML-SOAP-Konstrukten nicht gewachsen.

Mehr Probleme im Heimnetz

Hinzu kommt: Wenn Kunden dem Support melden, dass beispielsweise „MagentaTV ruckelt“, genügt es nicht, wie bei TR-069 üblich, nur die Leitung bis zum Router zu prüfen. Provider berichten, dass sogar die Mehrzahl der gemeldeten Internetprobleme letztlich gar nicht dem Internet, sondern einem der vielen Details im Heimnetz des Kunden geschuldet ist. Deshalb wollen Provider die gesamte Strecke vom Streamingserver bis zum Wiedergabegerät im Heimnetz untersuchen.

Als weiteren Antrieb für ihre Fernwartungsambitionen sehen die Provider die rasant zunehmende Zahl an vernetzten Geräten in den Haushalten. Da können sich leicht 20 und mehr tummeln, beispielsweise Computer, Notebooks, Smartphones, Telefone, Smart-TVs, Staubsauger, Steckdosen, Schalter, Lampen, Türschlösser oder Thermostate und zur Reichweitenvergrößerung auch Access-Points, WLAN-Repeater oder Powerline-Brücken. Bei Netzwerkstörungen ist es für Personen ohne Netzwerk-Know-how nahezu unmöglich, die Ursache allein herauszufinden: Liegt es am Internetanschluss, am Heimnetz oder am Dienstanbieter?

c't kompakt

- Dem 2004 entwickelten TR-069-Protokoll zur Router-Fernkonfiguration fehlen Echtzeitmerkmale, um moderne Netze zu warten.
- Der schlanke Nachfolger TR-369 steckt sowohl in Provider- als auch in manchen Anwender-Apps.
- Provider wie die Deutsche Telekom verwalten darüber das WLAN ihrer Kunden.
- Das Broadband Forum fördert die Verbreitung mit quelloffenen Implementierungen.

Beispiele gibt es zuhauf: Das WLAN reagiert empfindlich auf Störungen von Nachbarnetzen und Radarsignalen, Billigprodukte aus Fernost funken in Masse, besitzen aber selten Steering- und Kanalalgorithmen, um sich veränderten Bedingungen anzupassen. Mesh-Systeme verhalten sich zwar deutlich robuster, verhindern aber auch nicht, dass WLAN-Repeater ungünstig platziert werden.

Für solche und viele weitere Fernwartungszwecke hat das Broadband Forum sein ursprüngliches Fernwartungskonzept 2018 gründlich reformiert und unter dem Namen TR-369 veröffentlicht [1]. Die feine Kunst liegt nun darin, sich möglichst umgehend über markante Netzwerkparameter zu informieren und nur die Dinge anzufassen, die der Wartung oder Optimierung bedürfen, die Privatsphäre der Kunden aber nicht anzutasten. Wir erklären, wie das funktionieren kann.

Vorweg kann man aber schon sagen: TR-369 deckt sogar Probleme auf, die User aus Unerfahrenheit nicht einmal melden würden.

Gemessen daran, was alles an PCs und Netzwerken kaputtgehen kann, widmen sich Provider per Fernwartung nur einem kleinen Teil der potenziellen Fehler. Bei Hardware- oder Softwareproblemen wie defekten Netzteilen oder vermurksten Betriebssysteminstallationen hilft TR-369 nicht; wie man dabei vorgeht, haben wir umfassend in der c’t-Ausgabe 21/2024 ab Seite 16 beschrieben.

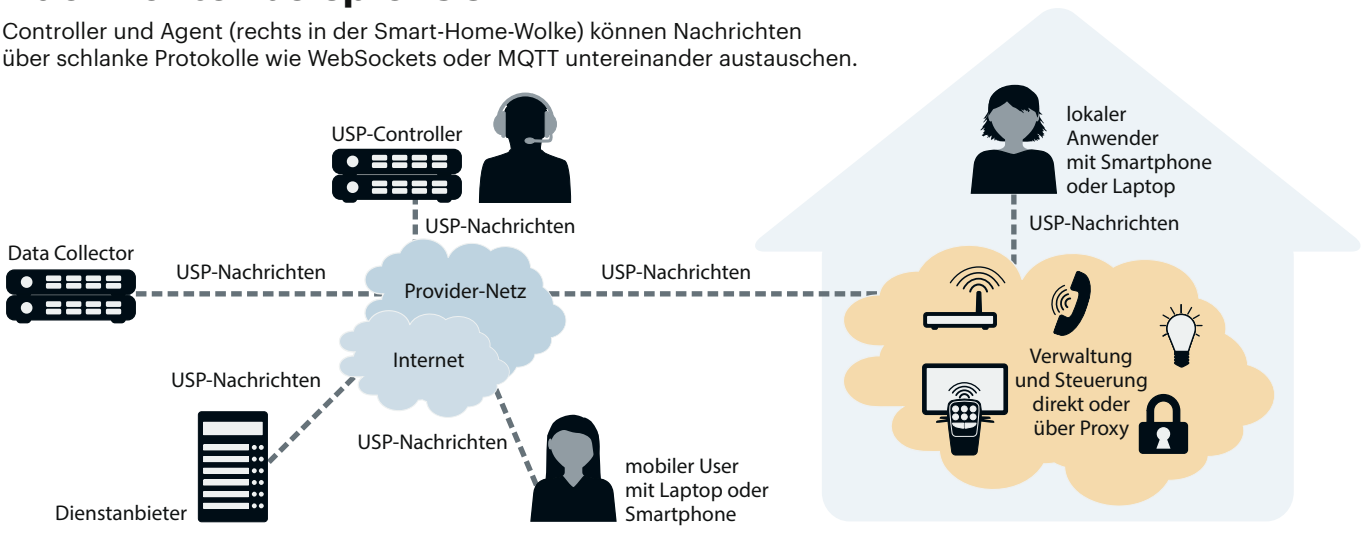
Dieser Beitrag ist in zwei Teile gegliedert. Zunächst erklären wir ausführlich das Fernwartungskonzept und die Bausteine, dann als Anwendungsbeispiel das Zusammenspiel zweier Vorreiter: die Hotline der Deutschen Telekom und der verbreitete Fritzbox-Router von AVM. Einige andere Routerhersteller implementieren TR-369 ebenfalls, sodass grundlegende Dinge beispielsweise auch auf Geräte von TP-Link oder Zyxel zutreffen. Die Mehrzahl der Routerhersteller stützt sich aber noch auf TR-069.

Von TR-369 zu USP

Bei TR-369 liegt der Fokus auf Echtzeitfunktionen: Die integrierten Transportprotokolle gründen auf einer persistenten IP-Verbindung zwischen dem Kundengerät (Customer Premises Equipment,

Nachrichtenbeispiel USP

Controller und Agent (rechts in der Smart-Home-Wolke) können Nachrichten über schlanke Protokolle wie WebSockets oder MQTT untereinander austauschen.



CPE) und der Managementinstanz. Weil der Kommunikationskanal nicht immer wieder neu aufgebaut wird, sondern einfach schon da ist, läuft der IP-Verkehr zwischen den Endpunkten deutlich schneller als bei TR-069. Er eignet sich daher auch für echtzeitnahe Anwendungen, beispielsweise um Mesh- und Smart-Home-Umgebungen zu überwachen. Zudem sind die Nachrichten binär kodiert und grundsätzlich schlanker als die schwafeligen SOAP-XML-Klartextkonstrukte von TR-069.

Das komplette System aus TR-369-Architektur, Protokollen, Datenmodellen, Open-Source-Implementierungen und Testplänen fasst man unter dem Begriff „User Services Plattform“ zusammen, kurz USP, und um diese Gesamtheit geht es im Weiteren.

Die Netzwerkprotokolle und die Messages (Nachrichten) für den Datenzugriff und die Konfiguration, also das Datenmodell des CPE, wurden radikal überarbeitet und optimiert. Um den Migrationsaufwand vom etablierten TR-069 zum besseren USP zu begrenzen, nutzt man nur die Datenmodelle von TR-069 weiter. Diese sind standardisiert, gründen auf der Spezifikation TR-181 Device:2 und adressieren praktisch alle Anwendungen für das Management von Netzkomponenten, Geräte- und Serviceklassen.

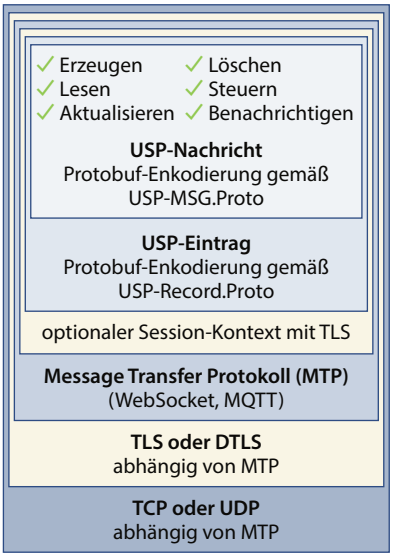
Als Einstieg in das USP-Universum empfiehlt sich die vom Broadband Forum verwaltete Webseite usp.technology. Neben der fast 300-seitigen technischen Spezifikation [2] sind dort alle erforderlichen Informationen über Protokolle, Datenmodelle, Ressourcen und Testpläne zentral verfügbar.

Managementseitig könnten bereits heute alle TR-069-Anwendungen auch über USP abgewickelt werden. Die Migration zu USP verläuft aber nur schrittweise. Wegen ihrer großen Verbreitung wird die TR-069-Technik noch lange der Standard für die Anschlusseinrichtung und andere Anwendungen sein, bei denen es nicht auf Echtzeitfunktionen ankommt.

Immerhin haben Hersteller wie AVM Wege geschaffen, TR-369 in geeigneten Routern aus der Ferne per TR-069 zu aktivieren, also ohne Firmware-Updates oder manuelle Benutzereingriffe. Zudem sehen die Konzepte der beiden Fernwartungen einen Parallelbetrieb vor, was auch erklärt, weshalb auf manchen Routern beide Protokolle implementiert sind. Beispielsweise können Fritzbox-Router zur Laufzeit gleichzeitig über TR-069 und USP kommunizieren und das sogar mit verschiedenen Diensteanbietern.

Protokollstapel TR-369

USP-Nachrichten können je nach Message Transfer Protokoll verschlüsselt oder im Klartext übertragen werden. Wenn sie übers Internet gesendet werden, ist die TLS-Verschlüsselung Pflicht.



Agent und Controller

In der USP-Terminologie ist das CPE der Agent [3]. Dabei spielt es keine Rolle, ob das CPE ein Router, ein Smart-Home-Sensor, ein NAS-Gerät oder ein sonstiges Netzwerkgerät mit IP-Stack ist. Der Agent bildet die steuerbaren Funktionen in seinem Datenmodell ab, auf welches der USP-Controller zugreift.

Im Datenmodell sind die Parameter, Attribute und Operationen definiert, für die sich ein CPE eignet, sowie die Anweisungen und Datenstrukturen, mittels denen der Controller das CPE konfiguriert, überwacht und verwaltet.

Das Datenmodell ist im Standard TR-181 spezifiziert und trägt den Namen „Device:2“ [4]. Es stellt sicher, dass CPE und Controller unabhängig vom Hersteller oder Gerätemodell miteinander kommunizieren können und umfasst `Parameter`, `Commands` und `Events`. Parameter sind Schlüssel-Wert-Paare zur Konfiguration, Commands sind Befehle, die der Agent ausführt, zum Beispiel `reboot`, und bei Events handelt es sich um Ereignisse auf dem Agenten, über die der Controller informiert werden will.

Der Controller liest und schreibt im Datenmodell über verschiedene Operationen. Dazu gehören `Get` zum Abfragen von Parameterwerten, `Set` zum Setzen von Werten und `Operate` zum Ausführen von Commands. Zusätzlich kann sich der Controller mittels `Subscriptions` über Ereignisse und Zustandsänderungen im Gerät informieren lassen (`Notification`).

Insgesamt sind im Datenmodell TR-181 Device:2 für das CPE-Management mehrere tausend Parameter definiert. Sollte dies nicht genügen, kann ein Hersteller für seinen speziellen Bedarf weitere hinzufügen. Für VoIP-Telefonie, Settop-Boxen und NAS-Geräte gibt es separate Datenmodelle.

Ein Datenmodell besteht aus Name- und Wert-Paaren, die einem Objekt als Parameter zugeordnet sind. Das Root-Objekt heißt `Device`.

Die darunterliegenden Objekte sind in einer hierarchischen Struktur angeordnet, in der einzelne Objektebenen durch Punkte getrennt sind. Das erinnert an den Aufbau hierarchischer Dateisysteme. Folgendes Beispiel verdeutlicht die Struktur anhand einiger Objekte und Parameternamen:

```
Device.DeviceInfo.
Manufacturer: AVM
SerialNumber: 00040E112233
Device.LANDevice.1.LANHostConfig↵
↳Management.
DHCPServerEnable: 1
DNSServers: 192.168.178.1
Device.LANDevice.1.LANHostConfig↵
↳Management.IPInterface.IPAddress:↵
↳ 192.168.178.1
SubnetMask: 255.255.255.0
```

Die Struktur enthält unter anderem die Seriennummer, die IP-Adresse und Netzwerkmaske einer Fritzbox; der DHCP-Server ist aktiviert. Der Controller kann Informationen mittels Such-Expressions sehr effizient anfordern (USP-Spezifikation, Abschnitt 2.5.3). So kommt TR-369 gegenüber TR-069 mit weniger Requests aus, was den Netzwerkverkehr reduziert.

Beispiel: Mit dem `Get`-Befehl für den folgenden Pfad fordert der Controller die IPv4-Adressen aller aktiven Interfaces des CPE an:

```
Device.IP.Interface.*.IPv4Address.↵
[Status==„Enabled“].IPAddress
```

Für das IoT-Management sieht das USP-Datenmodell ein „Proxied Device“ vor. Eigenschaften von angekoppelten IoT-Devices bildet das Datenmodell des vorgeschalteten USP-Agents ab. In der Fritzbox sind im USP-Datenmodell die angeschlossenen Smart-Home-Devices des Fritz-Ökosystems als Proxied Device abgebildet; das ist üblich, wenn einem Zielgerät der IP-Stack und somit auch TR-369 fehlt.

So lassen sich Lampen, Taster, Sensoren, schaltbare Steckdosen und Heizkörperregler auch über USP steuern. Das können beispielsweise Unternehmen nutzen, um die Gebäudesteuerung einem Dienstleister zu übertragen, der dann nach Feierabend etwa Lampen oder Heizkörperregler aus der Ferne abschaltet. Und da ein Agent in jeder Art Internet-Host sitzen kann, können Anwender ihre Heimnetzgeräte per USP auch per Smartphone schalten und zwar auch aus der Ferne.

Über die persistente IP-Verbindung können Agent und Controller unmittelbar auf ihre gegenseitigen Ressourcen zugreifen, was der Schlüssel für Echtzeitfähigkeit ist. Den Verbindungsaufbau initiiert üblicherweise der Agent. So überwindet er auch eine etwaige Provider-NAT selbstständig und kommt anders als bei TR-069 ohne offenen Port aus. Das reduziert die Angriffsfläche des CPE.

Auf dem USP-Controller setzen Management-Applikationen des Service-Anbieters auf, beispielsweise für die Ersteinrichtung, das Firmware-Management oder Anwendungen für den Kundensupport eines Providers. Und weil USP echtzeitnah arbeitet, eignet es sich sogar für die Verarbeitung zeitkritischer Sensor- und Messzustände von Smart-Home-Applikationen. Dabei kann die USP-Controller-Anwendung als App auf einem Smartphone laufen und etwa einen Selfcare- oder Smart-Home-Service für Kunden enthalten.

Ein USP-Agent lässt sich von mehreren USP-Controllern mit unterschiedlichen Berechtigungen steuern (Multi-Stakeholder-Fähigkeit). Ein Beispiel: Der USP-Controller des Providers hat Schreib- und Leserechte für die Konfiguration von Internet- und Telefoniediensten und Leserechte für Mesh-Einstellungen, während jener eines anderen Service-Anbieters auf die Konfiguration von Smart-Home-Diensten zugreifen darf.

Die Controller-Anwendungen für Internet, Telefonie und Mesh hostet der Provider, der USP-Controller für das Smart Home läuft als App auf dem Smartphone des Kunden. Beide haben nur Zugriffsrechte auf eine Teilmenge des Datenmodells und wissen nichts voneinander. Der USP-Agent unterhält zu beiden Controllern je eine IP-Verbindung mit unterschiedlichen Message-Transport-Protokollen (MTP).

Bei Fritzboxen können Nutzer auf Wunsch zusätzlich eine Direktverbindung zum MyFritz-USP-Controller für das Firmware-Management nutzen und Informationen über gekoppelte Smart-Home-Geräte in Echtzeit ablesen. Weitere Beispiele:

– Provider-Controller: Schreib- und Leserechte für Internet und VoIP-Konten, Leserechte für WLAN und Mesh im Heimnetz
– Vendor-Controller, zum Beispiel MyFritz: Firmware-Management und Smart-Home-Energiemessung
– Benutzer-Controller, zum Beispiel eine App: Rechte für die Konfiguration des Smart Home.

WebSockets und MQTT

USP nutzt zur Übertragung im Allgemeinen das Transport Control Protocol (TCP); wenn Nachrichten über das Internet gehen, müssen sie außerdem per Transport Layer Security (TLS) verschlüsselt werden. Gebräuchliche Message-Transport-Protokolle sind Websockets [5] und Message Queuing Telemetry Transport (MQTT) [6]. Über WebSockets kommunizieren der USP-Agent und der USP-Controller bidirektional miteinander.

Da WebSockets die IP-Verbindung permanent aufrechterhalten, bieten sie gegenüber traditionellen HTTP-Verbindungen den Vorteil, dass sowohl der Server als auch der Client Nachrichten ohne vorherige Anfragen senden und empfangen können. Weil bestimmte Headerinformationen nur einmal und nicht immer wieder aufs Neue übertragen werden, schrumpft gegenüber TR-069 der Overhead, was die Kommunikation beschleunigt und die Latenz verkürzt.

WebSockets kommen mit wenigen Ressourcen aus, sind deshalb gut skalierbar und Server können viele parallele Verbindungen gleichzeitig aufrechterhalten. Das kommt besonders Anwendungen mit vielen Benutzern oder Geräten zugute, die gleichzeitig mit dem Server kommunizieren, also genau dem Fernwartungsprofil von Providern.

Speziell für die IoT-Kommunikation steht mit MQTT ein leichtgewichtiges, offenes Protokoll zur Verfügung. MQTT setzt als zentralen Bestandteil einen Broker voraus, der zwischen den Kommunikationspartnern vermittelt. MQTT-Broker wie Mosquitto sind für verschiedene Plattformen gratis erhältlich.

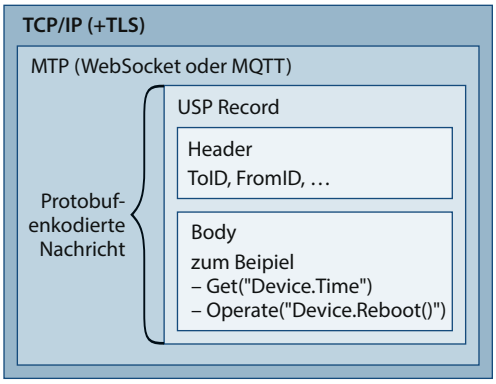
MQTT lässt sich wie WebSockets gut skalieren; es funktioniert selbst bei einer großen Anzahl gleichzeitiger Verbindungen effizient. Seine Mechanismen stellen Nachrichten zuverlässig zu oder wieder her, was bei Verbindungsabbrüchen und Netzwerkstörungen hilft und besonders dem Betrieb mit mobilen Geräten zugutekommt.

Protobuf statt XML-Spaghetti

Ein USP-Eintrag (Record) besteht aus einem Header mit Metainformationen wie Absender und Empfänger sowie der USP-

TR-369-Architektur

An der Fernwartung per TR-369 beziehungsweise USP können mehrere Controller an beliebiger Stelle beteiligt sein, je nach Protokollen der unteren Schicht, zwischengeschalteten Brokern oder Proxys. USP-Controller können im Rechenzentrum, Back-Office, auf dem Smartphone oder dem Notebook installiert sein.



Die Fernwartung per USP ist auf manchen Routern bereits aktiviert. Im obigen Beispiel dürfen der MyFritz-Dienst und die Deutsche Telekom mit Einverständnis des Nutzers einige Einstellungskategorien auslesen und setzen.

Message. Sie enthält ebenfalls einen Header. Dieser beschreibt hauptsächlich den Befehlsstyp (engl. Operation). Im Body sind dann Details zu den auszuführenden Operations beziehungsweise den angeforderten Antworten aufgeführt. Die Übertragung der USP-Records und -Messages erfolgt über das binäre Datenformat Protocol Buffers.

Protocol Buffers, oder kurz Protobuf, ist eine von Google entwickelte, plattformübergreifende und sprachunabhängige Methode zur Serialisierung strukturierter Daten [7]. Sie gilt als leistungsfähige Technik zur Kommunikation zwischen verschiedenen Systemen und Programmen. Im Vergleich zu textbasierten Datenstrukturen wie JSON oder XML sind die Datenmengen weit kleiner, was den Bedarf an Speicherplatz und Übertragungsgeschwindigkeit deutlich senkt.

Die erforderlichen Datenstrukturen sind als .proto-Dateien usp-record.proto und usp-msg.proto veröffentlicht [8, 9]. Daraus baut der Protobuf-Compiler Quellcode für die gewünschte Zielsprache. Das reduziert den Entwicklungsaufwand aufs Minimum und vereinfacht künftige Änderungen und Erweiterungen im USP-Nachrichtenformat.

Sicherheit

Im WebSocket-Protokoll ist der Datenverkehr per TLS abhörsicher verschlüsselt, was Unbefugten Einblicke verwehrt. Digitale Zertifikate bestätigen die Authentizität (Echtheit) der Kommunikationspartner, was das Fälschen, Mitlesen und Verändern von Transaktionen verhindert.

Selbiges gilt für MQTT. Der MQTT-Broker muss vertrauenswürdig sein, wenn der Netzwerkverkehr im Broker terminiert oder von dort weitergeleitet wird. Setzt man einen MQTT-Broker eines Drittanbieters ein, zum Beispiel aus der Amazon-Cloud, möchte man den Inhalt von USP-Messages vertraulich halten. Dafür sieht USP die Verschlüsselung der Nutzdaten vor.

Grundsätzlich hat der USP-Controller für benutzereigene Passwörter des Geräts nur Schreib-, aber keine Leserechte. Er kann also einen WLAN-Schlüssel setzen, was für die Ersteinrichtung erforderlich sein kann. Aber wenn der Anwender den WLAN-Schlüssel ändert, kann ihn der Controller nicht auslesen. Selbiges gilt für Passwörter von VoIP-Konten, die Nutzer manuell hinzufügen.

Privatsphäre

Controller haben zwar keine allumfassenden Rechte, sondern genau besehen nur wenige, für ganz spezielle Konfigurationen. Doch wenn der Benutzer die Verantwortung abgibt, kann es erforderlich sein, dass Diensteanbieter unbemerkt vom Nutzer Einstellungen auslesen und optimieren. Wer sich um die Gerätekonfiguration nicht kümmern will, wird das als Vorteil werten.

Da die Daten aber oft private Dinge wie IP- und MAC-Adressen, Gerätenamen und Events enthalten, lassen sich daraus persönliche Präferenzen und Verhaltensmuster ableiten. Diensteanbieter sind zwar verpflichtet, solche Daten vertraulich zu behandeln. Doch in Szenarien mit hohen Sicherheitsanforderungen oder bei Anwendern, die ihren Gerätezoo lieber selbst verwalten, kann USP dennoch unerwünscht sein. Deshalb sollte man bei der Anschaffung von Routern darauf achten, dass USP möglichst einfach abschaltbar ist, etwa über das Webinterface des Routers.

Provider und Routerhersteller

USP setzen bereits einige Provider ein, darunter die Deutsche Telekom als kostenlosen Service „Heimnetz-Diagnose“ [10]. Auf dieser Basis sichert sie schnelle Hilfe zu, zum Beispiel um die WLAN-Reichweite zu optimieren oder die Verbindungsqualität zu verbessern. Sie bietet aber auch allgemein an, bei Fehlersuche und -behebung zu helfen.

Mit dem ausdrücklichen Einverständnis des Kunden kann die Telekom auf diese Weise relevante Performance-, Mess- und Statistikdaten erfassen, bis hinunter zu den vermeshten Komponenten. Die Daten hält das Unternehmen bis zu 14 Tage vor. Mittlerweile sind auf der Telekom-Plattform mehr als eine Million Fritzboxen mit USP verzeichnet [11]. Laut dem Konzern ist das die aktuell weltgrößte USP-Management-Plattform.

Bei Kundenzustimmung übermittelt die Fritzbox alle 20 Minuten einen „Bulk“ detaillierter Infos über den Status der DSL- beziehungsweise Glasfaserleitung. Dazu gehören die Anzahl der Sync-Abbrüche, Linkraten-Einbrüche und Fehlerzähler. Ferner sendet der Router die Heimnetz-Topologie, WLAN-Mesh-Metriken und angebundene Endgeräte. Damit liegen beim ISP alle für die Verwaltung und Pflege erforderlichen Daten vor.

Die Heimnetzanalyse legt Engpässe, Fehlkonfigurationen und Störungen in einem Heimnetz mit Fritz-Mesh offen. Konkret bedeutet das, die Telekom kann Flaschenhälse wie niedrige WLAN-Signalpegel, mangelhafte Link-Verfügbarkeit, verstopfte WLAN-Kanäle, hohe Latenzen, Paketverluste oder ungenügende Übertragungsgeschwindigkeiten im Mesh des Kunden analysieren und Ursachen aufspüren.

Das erfordert vom Mesh-Master und seinen Komponenten, alle Messdaten verlässlich und schnell zu ermitteln. Mit den aggregierten Daten lässt sich eine Mesh-Störung auch rückwirkend exakt lokalisieren. Analysen, etwa betreffs hakeliger Netflix-Streams, enden also nicht wie mit TR-069 am Router, sondern beziehen das Heimnetz ein.

Viele weitere Provider bereiten ähnliche Anwendungen vor. Supporter können im Servicefall in Sekundenschnelle sowohl auf historische als auch auf aktuelle Daten zugreifen, eine Analyse starten und im Idealfall das Problem beseitigen oder zumindest eine Lösung nennen.

Der nächste Schritt ist auch nicht mehr weit: Der Serviceanbieter kann mit einer echtzeitfähigen Architektur und geeigneten Applikationen präventiv eingreifen, falls er Fehlkonfigurationen und Störungen in der Infrastruktur ausmacht, die eine zugesicherte Qualität von abonnierten Diensten verhindern.

Deshalb sind Provider überzeugt, dass aktives Management „silent sufferer" verhindert, also Kunden, die ihren Frust über mangelnde Servicequalität mit sich selbst abmachen und ohne Angabe von Gründen kündigen. Über Selfcare-Apps können Provider ihre Kunden über den Zustand der Internetdienste informieren und Tipps zur Optimierung und Fehlerbehebung geben.

Einige Provider und Serviceanbieter praktizieren aktives WLAN-Management über USP oder ähnliche Protokolle, darunter die Thüringer NetKom in Zusammenarbeit mit dem Dienstleister Plume und die Firma Airties [12, 13, 14]. Oft sind solche Dienste an kostenpflichtige Abonnements gebunden. Sofern es die Endgeräte im Heimnetz erlauben, steuern die Provider Kanäle und Bandsteering von einem Clouddienst aus dynamisch und versprechen dem Benutzer eine verbesserte Servicequalität.

Allerdings können die Auswirkungen bei einem Ausfall der Management-Cloud sehr bunt sein, sofern lokal keine wirksamen Fallback-Mechanismen existieren.

Deshalb empfiehlt sich eher ein lokales Management, wie es auch AVM umgesetzt hat. Ausfälle der Cloud sind dann kein Thema. Im Fritz-Ökosystem liefern die vermeshten Komponenten, also Mesh-Repeater und Endgeräte dem Mesh-Master ihre Messdaten über schnelle Tunnelprotokolle. Dabei wird die Datenbasis nahezu in Echtzeit lokal aktualisiert. Auf diese Datenbasis greifen die Fritz-Kanal- und Steering-Algorithmen des Mesh-Masters zurück und reagieren sehr viel schneller als eine Management-Applikation in der Cloud.

Eine der ersten USP-Anwendungen für Endkunden findet man auf myfritz.net. Bei Aktivieren der „Direktverbindung" baut die Fritzbox eine verschlüsselte WebSocket-Verbindung zum MyFritz-USP-Controller auf. Dort findet man neben Statusinformationen wie der aktuellen Link-Geschwindigkeit auch die Option, Energiemesswerte der schaltbaren Steckdose DECT200 für Vergleiche und für eine Langzeitspeicherung feingranular aufzuzeichnen. Das dürfte für Betreiber von Balkonkraftwerken ein nützliches Tool sein. Weitere Anwendungen für das Smart Home und die Heimnetzoptimierung sind in Planung.

Fazit

Die Branche entwickelt USP laufend weiter, mittlerweile ist die Version 1.4 aktuell. Wer USP nicht wie etwa ein Routerhersteller für seine speziellen Bedürfnisse selbst implementiert, kann auf die offizielle Referenzimplementierung, den Open Broadband-User Services Platform-Agent zurückgreifen (OB-USP-Agent). Die in der Programmiersprache C geschriebenen Quellen sind veröffentlicht und ermöglichen eine rasche Integration in jede Embedded-Plattform.

Einige Provider stützen sich bereits umfassend auf USP. Der britische Netzbetreiber Vodafone etwa hat sich bei seinem Controller-Ansatz von der zentralistischen Anordnung verabschiedet und stattdessen die Technik eng mit den AWS-Cloud-Diensten von Amazon verzahnt [15].

Um die Verbreitung zu beschleunigen, veranstaltet das Broadband Forum schon seit Längerem regelmäßig USP-Summits und Plugfests zum Austausch und für Interoperabilitätsprüfungen der Produkte [16]. Diese Veranstaltungen nutzen zunehmend nicht nur Anbieter von Managementlösungen wie Axiros und Nokia, sondern auch Endgerätehersteller wie Zyxel, um ihre Implementierungen gegenseitig intensiv zu testen.

Das dürfte sich sowohl für Provider als auch für IT-ferne Nutzer bezahlt machen und vielleicht auch dem Support-Recken vor Ort gefallen, der sich etwa ums WLAN nur noch kümmern muss, wenn der Repeater seine letzte Grätsche gemacht hat. *(dz@ct.de)* c't

Roland Riedel arbeitet bei AVM in der Softwareentwicklung im Bereich Networking Provider.

Je nach Konzept können USP-Dienste über eine Cloud laufen oder lokal in einem Mesh-Master wie der Fritzbox implementiert sein.

Literatur

[1] Broadband Forum: Realizing the Promise of the Connected Home with User Services Platform (TR-369), https://www.broadband-forum.org/wp-content/uploads/2019/05/BBF-179-TR-369-MU-461-Marketing-Update-V6.pdf
[2] Broadband Forum: The User Services Plattform, https://usp.technology/specification/index.html
[3] Open Broadband-User Services Platform-Agent, https://github.com/BroadbandForum/obuspa
[4] Broadband Forum User Services Plattform (USP) Data Models, https://usp-data-models.broadband-forum.org/
[5] IETF: The WebSocket Protocol, https://datatracker.ietf.org/doc/html/rfc6455
[6] MQTT Specifications, https://mqtt.org/mqtt-specification/
[7] Google: protocolbuffers (GitHub), https://github.com/protocolbuffers/protobuf
[8] usp-record-1.3.proto, https://usp.technology/specification/usp-record-1-3.proto
[9] usp-msg-1-3.proto, https://usp.technology/specification/usp-msg-1-3.proto
[10] Deutsche Telekom, Heimnetz-Diagnose, https://www.telekom.de/zuhause/tarife-und-optionen/zubuchoptionen/heimnetz-diagnose
[11] USP Case Study: Scaling up at DT - #USPSummit 2024, https://www.youtube.com/watch?v=2Lnkpjj-9Hg10
[12] Thüringer NetKom kooperiert mit Plume, https://www.netkom.de/Privatkunden/Plume
[13] Plume HomePass, https://www.plume.com/homepass/blog/introducing-network-priority-boost-what-matters/
[14] Airties, Customer Care & Diagnostics, https://airties.com/broadband-operator-solutions/customer-care-diagnostics/
[15] How Vodafone is using AWS and Broadband Forum User Service Platform (USP) standard to re-architect the management of its Customer Premise Equipment (CPE) and become more adaptive to changes https://aws.amazon.com/de/blogs/industries/how-vodafone-is-using-aws-and-broadband-forum-user-service-platform-usp-standard-to-re-architect-the-management-of-its-customer-premise-equipment-cpe-and-become-more-adaptive-to-changes
[16] Beyond the Era of Speed to One of Experience - #USPSummit 2024 Highlights, https://www.youtube.com/watch?v=77Akxt495nQ&pp=ygUOdXNwc3VtbWl0IDIwMjQ%3D

USP-Infos: *ct.de/y2tq*