2020

c't ADMIN

IT-Praxis für Heim- und Büronetzwerke

So läuft alles rund

Windows-Netzwerke tunen
Netzwerk-Bremsklötze finden und beseitigen

Helfen ohne Hinfahren
PCs und Mobilgeräte fernwarten

VPN modernisieren
IPSec-Altlasten raus, WireGuard rein

Nextcloud optimieren
Tipps für die Gruppenarbeit in der Cloud

Funknetze erweitern
Mächtige WLAN-Controller
Privates LTE ergänzt WLAN

Traffic analysieren
Netzverkehr live beobachten, Störer finden,
Netzwerkmitschnitte richtig lesen

Fritzbox optimal

IPv6-Vorteile mit DynDNS nutzen, TK-Anlage erweitern

Telefonie verschlüsseln, VPN und SMB-Freigaben beschleunigen

www.ctspecial.de

c't ADMIN

Heise

Editorial

Liebe Leserinnen und Leser,

Netzwerke und Computer zu administrieren, ist ein bisschen wie Schneeschippen am Nordpol: Egal, wie sehr Sie sich ins Zeug legen, es fällt immerzu neue Arbeit vom Himmel. Mal braucht ein Update-verunfalltes NAS-Gerät Ihre heilenden Hände, mal müssen Sie den Router schlaumachen, damit Videokonferenzen glattlaufen, dann wieder das Einmaleins der WPS-Kopplung zusammen mit IT-abstinenten Familienmitgliedern herbeten oder dem Chef in den VPN-Sattel helfen.

Weil jeder Tag überraschen kann, haben wir diese c't-Sonderausgabe so zusammengestellt, dass Sie mit alltäglichen Anforderungen Schritt halten und zugleich den Blick für aktuelle Entwicklungen schärfen können.

Falls ein Windows-PC lahmt, gönnen Sie ihm eine gründliche Inspektion: Mit unseren Tipps finden und beseitigen Sie leistungsmindernde Flaschenhälse. Bei der täglichen Administration helfen wir mit fundierten Beschreibungen neuer PowerShell-7-Funktionen und einem kompakten Überblick über zeitsparende NetCmdlets für fast 40 Netzwerkprotokolle. Spürbare Entlastung bringt auch unsere Rubrik zur Fernwartung von PCs und insbesondere Mobilgeräten – damit kleine Probleme gleich beseitigt werden können und nicht bloß wegen des Fahrtaufwands vor sich hingären.

Wenn das WLAN nicht in alle Ecken reicht, überlegen Sie vielleicht, neue Access-Points aufzustellen. Wir haben einige WLAN-Controller auf den Prüfstand gebeten, die bei der Verwaltung der Access-Points helfen. Und falls Sie als Firmen-Admin mit der WLAN-Leistung hadern: Lesen Sie, woran WLAN grundsätzlich krankt und wie private LTE-Netze helfen können.

In vielen Netzen bauen Fritzbox-Router die Verbindung zum Internet auf. Mit dem neuen FritzOS 7.2 hat der Hersteller AVM hohe Erwartungen geweckt. Wir prüfen, ob die bemängelten NAS- und VPN-Zugriffe tatsächlich besser geworden sind, und klären, was Sie von verschlüsselter Telefonie und WPA3 erwarten können. Doch das IPSec-basierte VPN der Fritzboxen schmeckt nicht jedem. Mit unseren kompakten Anleitungen holen Sie sich die moderne WireGuard-VPN-Technik ins Haus.

Die vielleicht reizvollste Admin-Kunst besteht darin, in einem laufenden Netzwerk die Kontrolle zu behalten. Unsere Beiträge zum Live-Monitoring führen Sie an das Thema heran. Sie können sicher sein: Mit dem Tool ntopng werden Sie Dinge in Ihrem Netz sehen, die Sie nicht erwartet haben.

Herzlichst, Ihr

Dušan Živadinović

Inhalt

WINDOWS-NETZWERK-TUNING

Ein unerwünschtes Nebenprodukt der Windows- und PC-Entwicklung ist die kontinuierlich wachsende Zahl an Mauselöchern, die für heutige Datenströme zu eng sind. Mit strukturiertem Vorgehen lassen sie sich finden und weiten.

6 Flaschenhälse beseitigen
12 Netzprobleme unter Windows finden
18 PowerShell 7: Das ist neu
24 NetCmdlets: 40 Netzprotokolle

FERNWARTUNG

Kein Admin kann überall vor Ort sein, wo es gerade brennt. Mit etwas Know-how lassen sich viele IT-Verknotungen aber auch aus dem Büro lösen.

26 Probleme aus der Ferne lösen
32 Fernwartung (nicht nur) für den PC
38 Mobilgeräte aus der Ferne warten
42 Redfish löst IPMI ab
48 HPE ProLiant Micro Server Gen10 Plus
52 Netzwerkzentrale für kleine Firmen

NEXTCLOUD UND NAS

Moderne NAS-Geräte treiben mit immer größeren Kapazitäten die Verbreitung von 10-Gigabit-Anschlüssen voran. Wie Gruppen davon Gebrauch machen können, zeigt unser Nextcloud-Special.

56 Nextcloud: Tipps für die Gruppenarbeit
62 NAS mit 10-Gigabit-Port
63 NAS-Festplatte mit 14 TByte
64 NAS für Express-Netze
65 Cache-SSD für NAS-Systeme

FRITZBOX OPTIMAL

Mit FritzOS 7.2 verbessert AVM seine Fritzboxen entscheidend. Aber es geht noch mehr: mehr Privatsphäre, besseres DynDNS, günstigere Telefonie mit Raspi und Android-Smartphone.

66 FritzOS 7.2 im Labortest
70 Was für Ihre neue Fritzbox wichtig ist
76 FritzOS 7.2 schützt die Privatsphäre
78 Testlabor: Wireguard-VPN und Fritzboxen
82 Fritzbox 6660 mit Wi-Fi-6-WLAN
84 DynDNS mit IPv6 leicht gemacht
88 Fritzbox als Mobilfunk-Gateway
96 Fritzbox: Internet-Fallback optimieren
100 FAQ Fritzbox
102 VoIP-Telefone zum Sparpreis

WLAN & DSL-KNOW-HOW

Wenn eine WLAN-Zelle zu klein ist, spannt man mehrere auf. Wir stellen leistungsfähige Controller vor, die mehrere Zellen steuern.

108 HPE-Aruba Instant On
110 WLAN-Steuerung für Access-Points
118 Power-over-Ethernet-Wandler
120 Was Router-Wizards übersehen

MODERNES VPN MIT WIREGUARD

Ob Vernetzung von Filialen oder Anbindung von Homeoffice-Mitarbeitern: VPN-Techniken sind unverzichtbar. Für das moderne WireGuard spricht, dass es sich leicht und sogar auf Klein-Computern wie dem Raspi einrichten lässt.

124 VPN-Server mit dem Raspi
134 VPN mit WireGuard und OpenWrt
138 FAQ VPNs mit WireGuard

SICHERHEIT UND MONITORING

Jedem Netzwerk-Admin stellt sich früher oder später die Frage: Was geht da gerade in meinem Netz vor? Wir zeigen, wie Sie den Verkehr live entschlüsseln.

142 Netzwerk-Live-Diagnose
150 PC zum Capture-Device machen
156 Spiegelports von Switches nutzen
162 TCP-Reassembly in WireShark
170 USB-Festplatte mit Fingerabdruckleser
172 Mobilspeicher mit Sicherheit
173 Backups im Schlaf

CAMPUSNETZE STATT WLAN

Keine Funktechnik hat sich auf der Welt so schnell verbreitet wie WLAN. Doch WLAN stößt zunehmend an Grenzen. 4G- und 5G-Mobilfunk versprechen Abhilfe.

174 Warum VW ein 5G-Netz plant
178 Campusnetz-Planung
186 Privater LTE-Mobilfunk
192 Testbetrieb für Campusnetze beantragen

ZUM HEFT

3 Editorial
191 Impressum

Flaschenhälse beseitigen

Wenn Windows lahmt, kann die Ursache bei der Hardware liegen – vielleicht ist der Arbeitsspeicher überfüllt oder der Prozessor am Anschlag. Windows-Bordmittel liefern viele Hinweise zur Diagnose.

Von **Christof Windeck**

Am Anfang steht der Task-Manager: Wann immer Windows holprig läuft und ein Verdacht auf die Hardware fällt, ist er die erste Anlaufstation. Und obwohl er auf den ersten Blick ganz simpel aussieht, verrät der Task-Manager eine Fülle an wichtigen Details [1]. Ist noch Platz im RAM? Frisst ein Hintergrundprozess übermäßig viel Prozessorleistung? Nutzt die lahmende Software nur einen CPU-Kern?

Falls der Task-Manager das Rätsel nicht löst, hat Windows noch mächtigere Werkzeuge unter der Haube: den Ressourcenmonitor und die Leistungsüberwachung. Für Spezialfälle wie lahme USB-Sticks nimmt man WinSAT, manchmal aber lieber externe Soft-Werkzeuge wie LatencyMon – aber der Reihe nach.

Task-Manager

Alte Windows-Hasen öffnen den Task-Manager mit der Tastenkombination Strg + Umschalt + Esc (Ctrl + Shift + Esc); man findet ihn aber auch nach einem Rechtsklick auf die Taskleiste. Drei Klicks sind beim Task-Manager wichtig, um Bremsklötze rascher zu entdecken. Bei einem frisch installierten Windows zeigt der Task-Manager zunächst fast nichts an, was

sich jedoch mit einem Klick auf „Mehr Details“ unten links schlagartig ändert. Nun taucht auf dem Reiter „Prozesse“ eine lange Liste laufender Programme und Dienste auf, in der man zunächst den Wald vor lauter Bäumen nicht sieht. Doch klicken Sie probeweise mal auf einen der Spaltenköpfe wie „CPU“ oder „Arbeitsspeicher“: Schwupps, sortiert der Task-Manager die Liste um und der Prozess mit dem jeweils höchsten Bedarf der angeklickten Ressource steht oben. So bekommt man rasch heraus, welches laufende Programm die CPU am stärksten belastet. Als zusätzliche Hilfe verfärben sich die jeweils höchsten Werte in den Spalten.

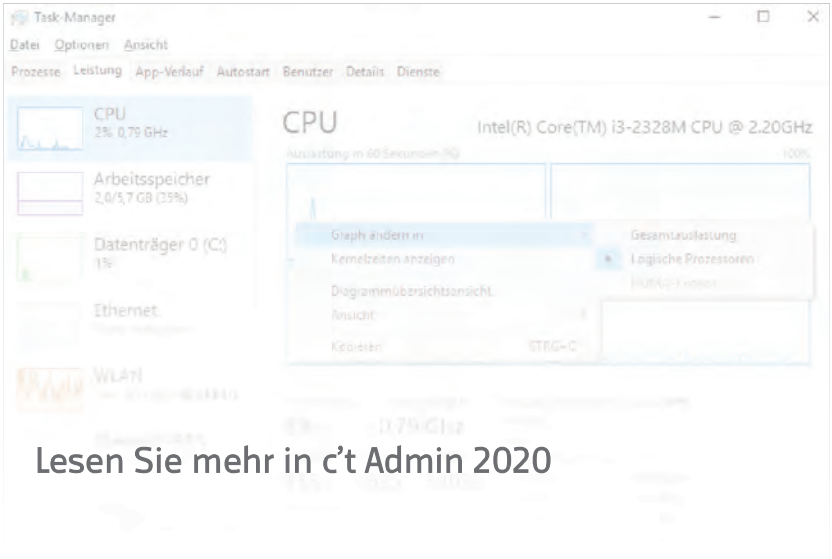
Manche Software lahmt, weil sie nicht schnell genug an Daten kommt: Das kann die Spalte „Datenträger“ verraten. Wenn im Spaltenkopf „100%“ steht, sind SSD oder Festplatte möglicherweise am Anschlag. Nach einem Rechtsklick auf die Spaltenköpfe lassen sich Spalten hinzu- oder abwählen, in aktuellen Windows-10-Versionen etwa auch zur Belastung des Grafikprozessors (GPU). So finden Sie beispielsweise heraus, ob der Browser bei der Videowiedergabe die GPU einspannt oder nicht. Die Spalte „GPU-Modul“ zeigt das direkt an (Video Decode). Moderne Video-Codecs wie VP9 (YouTube) oder HEVC (H.265, etwa für DVB-T2) fressen viel Rechenleistung, wenn sie als Software auf den CPU-Kernen laufen – dann ruckelt es womöglich.

Der zweite Reiter „Leistung“ im Task-Manager summiert die Auslastung der jeweiligen Ressourcen und zeigt den Verlauf der letzten Sekunden grafisch an. Wichtig hier bei der CPU-Auslastung: Ein Rechtsklick und die Auswahl von „Graph ändern in/Logische Prozessoren“ zeigt die Auslastung der einzelnen CPU-Kerne; die Summe bleibt weiter im Mini-Diagramm in der linken Spalte sichtbar. Mit den logischen Prozessoren sind sowohl echte Kerne als auch virtuelle Hyper-Threading-(SMT-) Kerne gemeint, ein Ryzen 5 2600 mit sechs Kernen hat in dieser Logik also 12 Kerne. Freundlicherweise verrät der Task-Manager die Zahl der echten und logischen Kerne gleich selbst.

Ein Blick auf die Lastverteilung klärt jedenfalls schnell, ob ein Programm nur einen oder wenige CPU-Kerne nutzt. Bestimmte typische Werte in der Gesamtauslastung sollten Sie stutzig machen: 50, 25, 12,5 oder 6 Prozent deuten an, dass die aktuell laufende Software nur einen von zwei, vier, acht oder sechzehn Kernen auslastet. Falls Sie beispielsweise mit LibreOffice Präsentationen erstellen, lahmt „Impress“ schon bei wenigen grafischen Elementen pro Folie oder beim PDF-Export – weil die Software dabei bloß einen CPU-Kern nutzt.

Turbo-Diagnose

Wenn aber nur einer oder zwei Kerne unter Volldampf stehen, dann sollten sie bei modernen Prozessoren mit Turbo wenigstens ordentlich hochtakten. Achten Sie deshalb auf die Anzeige der CPU-Frequenz (Geschwindigkeit) daneben: Dort stehen Werte von 0,6 bis 1,5 GHz, wenn die CPU nichts



Der Task-Manager ist die erste Informationsquelle bei der Suche nach Hardware-Bremsen

Bild: Andreas Martini

Probleme aus der Ferne lösen

Ob die Chefin unterwegs nicht ins VPN kommt oder Papas Videochat mit den Freunden scheitert: Manchmal werden IT-Probleme anderer Leute zu den eigenen. Zur Herausforderung wird es, wenn man sich nicht vor Ort darum kümmern kann. Mit passendem Werkzeug und unseren Tipps helfen Sie trotzdem erfolgreich.

Von **Axel Vahldiek**

Das Lösen von Technikproblemen ist nicht immer trivial, doch wenn es um die Schwierigkeiten anderer Leute geht, die zudem aus der Ferne zu lösen sind, wird es noch kniffliger. Man kann sich ja dann zum Reparieren nicht vor das betroffene Gerät setzen. Man muss also nicht nur eine Lösung finden, sondern auch einen Weg, sie anzuwenden. Das läuft meist darauf hinaus, entweder das Gerät fernzusteuern oder – noch herausfordernder – dessen Besitzer. In dieser Ausgabe geht es gleich in mehreren Artikeln um diese zusätzlichen Herausforderungen.

Am bequemsten löst man Technikprobleme an anderen Orten, wenn man Fernwartungssoftware einsetzen kann. Anders als bei klassischer Fernsteuerung sehen bei der Fernwartung nicht nur Sie den Desktop des entfernten PCs, sondern auch der davorsitzende Besitzer. Beide können Maus und Tastatur steuern. Ihr Gegenüber kann live demonstrieren, was das Problem ist. Sie sehen Fehlermeldungen im Original und können zur weiteren Recherche beispielsweise direkt in Logs und Einstellungsdialoge schauen. Sie können selbst versuchen, das Problem zu lösen. Im nachfolgenden Beitrag auf Seite 32 finden Sie Tipps zu Auswahl und Einsatz solcher Fernwartungssoftware. Mit ihr können Sie aber nicht nur störrischen PCs und Notebooks wieder Beine machen, sondern auch Tablets und Smartphones. Mehr lesen Sie im Beitrag ab Seite 38.

Der Artikel, den Sie gerade lesen, widmet sich jenen Fällen, in denen der Einsatz von Fernwartungssoftware nicht infrage kommt. Das gilt beispielsweise für Hardwareprobleme oder für nicht fernsteuerbare Technik wie Drucker. Oder es fehlt eine Internetverbindung, beispielsweise weil der Router streikt oder ein Problem mit dessen Verkabelung besteht. Zwar vermag heutzutage oft die Mobilfunkverbindung des Smartphones als Backup-Leitung dienen. Doch was ist, wenn der Hilfesuchende damit überfordert ist, diese für Mitnutzung durch seinen PC freizugeben? Denkbar ist auch, dass Sie per Fernzugriff Sachen zu sehen bekämen, die Sie gar nicht sehen sollen oder wollen (zu persönlich, Datenschutz …).

Guck mal!

Zwar hilft bei erstaunlich vielen Problemen der simple Hinweis „Starte mal neu", doch eben nicht immer. Dann muss man das Problem erst mal verstehen, bevor man helfen kann. Wer mangels Fernwartungssoftware nicht selbst nachschauen kann, muss die nötigen Informationen auf anderem Wege erlangen.

Hilferufe treffen im Alltag meist telefonisch oder schriftlich per E-Mail oder Chat ein. Das kann an sich schon ein Problem darstellen: Denn einen Gesprächspartner versteht man am besten, wenn man ihn sieht und hört. Dann bekommt man all die subtilen Signale mit wie Gesichtsausdrücke, Handbewegungen und so weiter. Bei einer schriftlichen Kontaktaufnahme fällt dieser Subtext komplett weg. Daher der Tipp auch aus eigener leidvoller Erfahrung: Wenn Ihnen jemand nach der zweiten oder dritten schriftlichen Mitteilung immer noch nicht begreiflich machen konnte, was eigentlich los ist, dann wechseln Sie wenn möglich die Kommunikationsform. Per Telefon wird zwar schon deutlich mehr Subtext übermittelt, doch am besten geht es per Videofonie. Damit kommt man einem Gespräch von Angesicht zu Angesicht am nächsten. Dazu braucht es keine komplizierte Videokonferenz-Software. Einfache Videotelefonate klappen auch per Smartphone, etwa per WhatsApp, Signal, Discord und anderen Messengern. Eine Marktübersicht haben wir in [1] veröffentlicht.

Videofonie hilft noch bei etwas anderem: beim Vorführen des Problems. Der Hilfesuchende schaltet auf die Frontkamera um und hält drauf. Falls er damit überfordert ist: Einfach das Smartphone drehen. Per Videofonie können Sie zudem die Lösung vorführen, sofern auf Ihrer Seite alles Nötige dafür vorhanden ist.

Falls die Bildauflösung des Videotelefonats zu gering zum Erkennen wichtiger Details ist, etwa des Mauszeigers, lassen Sie Ihr Gegenüber mit dem Finger auf die richtige Stelle zeigen. Oder Sie unterbrechen das Videotelefonat vorübergehend, damit er von wichtigen Stellen Fotos macht und Ihnen schickt. Sofern er in der Lage dazu ist, hilft es oft, ihn diese Stellen in einer Bildbearbeitung mit einem farbigen Kreis umranden oder Pfeile an die richtige Stelle malen zu lassen. Unter Windows reicht dafür der bordeigene Oldie „Paint".

Wenn ohnehin beispielsweise im Homeoffice eine Videokonferenzsoftware vorhanden ist, bietet sie sich zum Helfen ebenfalls an. Bei vielen kann man den Desktop teilen. So können Sie Ihr Gegen-

Lesen Sie mehr in c't Admin 2020

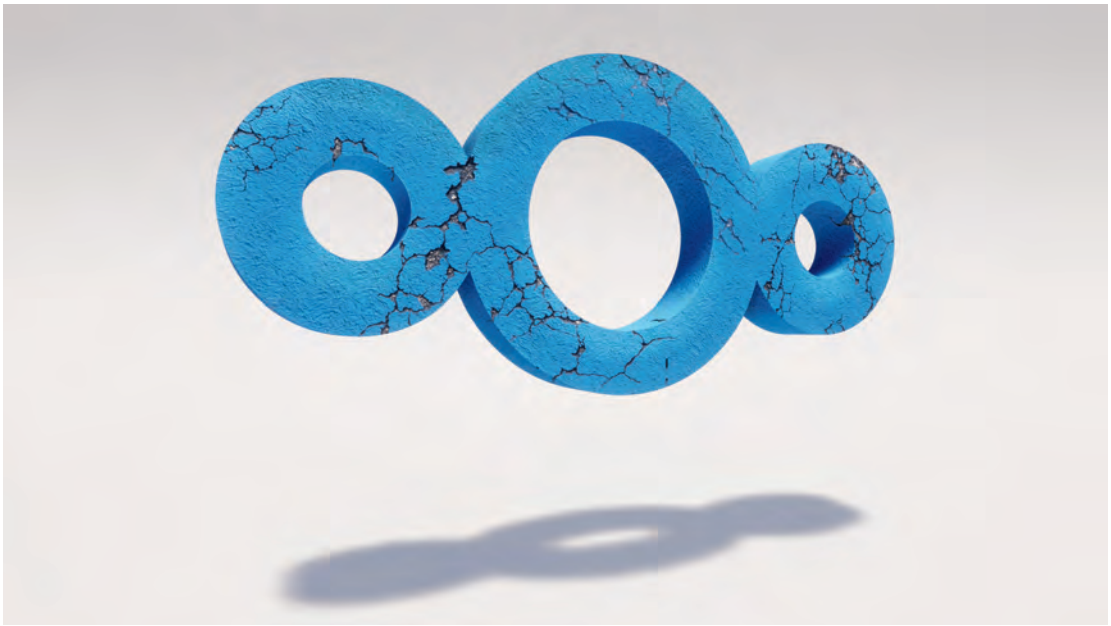


Bild: Hagen Kober

Nextcloud: Tipps für die Gruppenarbeit

Nextcloud bringt verteilt zusammenarbeitende Computer und Menschen einander näher. Doch die alternative Cloud ist manchmal spröde: Unsere Hinweise machen die neue Heimat schöner.

Von **Peter Siering**

Nextcloud kann beim Hoster, auf einem Mietserver oder auf dem hauseigenen NAS laufen. Dieser Beitrag ergänzt Installationsanleitungen [1, 2] um Tipps für frisch gebackene Nextcloud-Eigener und -Admins. Er hilft, die überbordenden Erwartungen zu justieren und gibt pragmatische Hilfestellungen zur geeigneten Nutzung.

Dreh- und Angelpunkt von Nextcloud sind Dateien: Nextcloud-Nutzer haben im Wesentlichen drei Möglichkeiten, Dateien darauf abzulegen. Sie können sie per Webbrowser dort hoch- und runterladen. Das Gleiche gelingt über das WebDAV-Protokoll ähnlich wie eine Freigabe im Netzwerk. Außerdem kann spezielle Client-Software Dateien speichern und abrufen.

Der Zugriff per Browser ist umständlich. Die zweite Methode, WebDAV, funktioniert wegen Unzulänglichkeiten des Protokolls [3] nur selten gut. Es möchte Dateien stets vollständig laden. Eine aktive Bearbeitung, wie man sie von Dateifreigaben

kennt, erlaubt WebDAV nicht. Außerdem variieren die Fähigkeiten von WebDAV-Clients stark. Kurzum: Nutzen Sie die beiden Methoden nur, wenn sich der Zugang nicht anders realisieren lässt.

Die deutlich bessere Methode stellt die Nextcloud-eigene Client-Software dar. Die gleicht automatisch Dateien zwischen lokalen Verzeichnissen und Nextcloud ab. Wenn sich die Datei auf einer Seite ändert, überträgt der Client sie auf die andere. Er nutzt dafür Funktionen, die im Hintergrund dafür sorgen, dass nicht nur die aktuelle Fassung der Datei erhalten bleibt, sondern auch die vorherigen Versionen – Nextcloud versioniert automatisch.

Wenn der Benutzer eine alte Fassung seiner Datei braucht, etwa weil er sich beim Bearbeiten eines Textes vergaloppiert hat, kann er über die Web-Oberfläche von Nextcloud alte Versionsstände der Datei abrufen. In die Web-Oberfläche bringt ihn ein Klick aus der Bedienoberfläche der Client-Software („Nextcloud im Browser öffnen“). Dort kann er im Kontextmenü einer Datei, das unter anderem über die drei Punkte erreichbar ist, unter „Details“ die „Versionen“ einsehen und alte wiederherstellen.

Dateiaustausch

Das klappt gut, wenn ein Benutzer die Ablage für seine eigenen Dateien verwendet, kriegt aber eine eigene Dynamik, wenn weitere Benutzer ins Spiel kommen und an den gleichen Dateien werkeln. Nextcloud erlaubt es nämlich, Dateien oder Verzeichnisse mit anderen Nutzern zu teilen. Die sehen die dann auch in ihrem Nextcloud-Client beziehungsweise ihrem synchronisierten Verzeichnis. Ändern die dort eine geteilte Datei, verpasst Nextcloud ihr ebenfalls eine neue Version.

Spannend wird es, wenn eine geteilte Datei gleichzeitig auf mehreren Clients geändert wird: Nextcloud legt dann von sich aus eine Kopie der Datei mit den lokalen Änderungen an und verpasst ihr einen Zeitstempel. Der Benutzer muss dann die Dateien vergleichen und die Daten von Hand zusammenpuzzeln – die Synchronisierung kann da also keine Wunder vollbringen. Für das gleichzeitige Arbeiten an ein und derselben Datei bieten sich Funktionen zur Online-Zusammenarbeit an – dazu gleich mehr.

Zum Nutzungsalltag mit Nextcloud gehören allerdings auch hartnäckigere Synchronisierungsfehler, die damit enden, dass der Server eine Datei verriegelt („Locked“). Der Nextcloud-Client hat dann beim Versuch kapituliert, eine Datei zu synchronisieren. In einem solchen Fall kann sich der Nutzer allein nicht mehr helfen, sondern muss den Nextcloud-Admin um Hilfe bitten: Der versetzt das System in den Wartungsmodus und leert mit speziellen Befehlen eine Datenbanktabelle. Die einzelnen Schritte zeigt der Artikel später am Beispiel einer Container-Installation.

Gemeinsame Struktur

Subtilen Unterhaltungswert hat Nextcloud, wenn sich Mitglieder einer Arbeitsgruppe auf eine Struktur der Dateiablage einigen, wie sie das von Netzwerkfreigaben gewohnt sind: Ein Benutzer legt mit besten Absichten Ordner an und verschiebt die bisher erarbeiteten Dateien darin und berichtet stolz vom ausgelebten Ordnungsfleiß. Die anderen aber sehen davon nichts: Die Struktur aus Verzeichnissen und die Verteilung der Dateien darin ist normalerweise eine individuelle – obwohl die Benutzer darin dieselben Dateien sehen.

Solle eine Nextcloud-Instanz Benutzern eine einheitliche Verzeichnisstruktur vorsetzen, so muss der Admin zunächst mithelfen: Er aktiviert in der In-

Manchmal bleibt beim Synchronisieren

eine Dateisperre hängen. Die muss

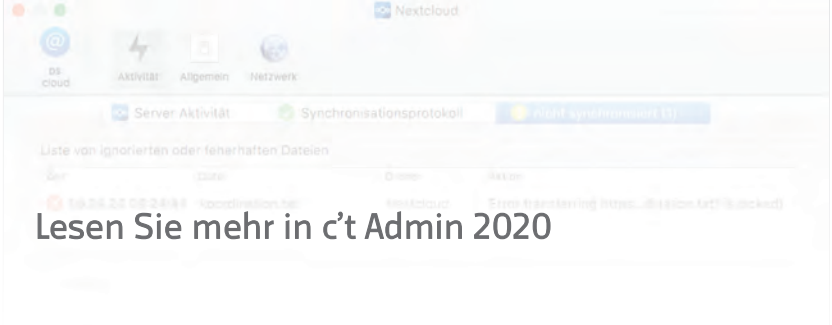


Bild: Andreas Martini

Was für Ihre neue Fritzbox wichtig ist

Nach einiger Zeit im Homeoffice und Arbeiten in der Cloud kann schon mal der Wunsch nach mehr Internet-Geschwindigkeit wachsen. Mit einem neuen Anschluss muss meist auch ein neues Zugangsgerät her, was oft eine Fritzbox ist. Wir zeigen, welches Modell wo am besten passt und wie man den Boxen neue Tricks beibringt.

Von **Ernst Ahlers**

AVM, die Mutter der zu Recht verbreiteten, oft heiß geliebten Fritzboxen, macht auch nicht alles auf Anhieb richtig, aber mehr richtig als viele andere Routerhersteller. Wer etwa die Vorteile des IPv6-Protokolls – jeder Rechner ist prinzipiell von überall her erreichbar – nutzen will, hat praktisch nur die Auswahl zwischen einer Fritzbox oder Geräten für Unternehmenseinsatz von Firmen wie Bintec, Draytek oder Lancom Systems. Denn bei IPv6 scheiterten in bisherigen c't-Tests viele Router anderer, im Small-Office/Home-Office-Segment (SOHO) tätiger Hersteller immer wieder an fehlenden oder falsch programmierten Optionen (zum Beispiel bei Dienstfreigaben unter wechselndem IPv6-Präfix).

Beim Internet per TV-Kabel – da wird IPv6 besonders wichtig, weil es kaum „richtiges" IPv4 mehr gibt – steht AVM ohnehin allein auf weiter Flur, wenn man sich nicht auf das vom Internetversorger angebotene Gerät verlassen will. Denn die Provider ordern gerne bei Fernost-Fabrikanten Modelle, die „einfach nur Internet" liefern. So sparen sie Kosten und hoffen, ihren Supportabteilungen das Leben zu erleichtern.

Fehler in der Betriebssoftware der Router, also der Firmware, werden bei den Providergeräten durchaus behoben. Aber so häufige Updates wie bei AVMs FritzOS, die auch Funktionserweiterungen – also einen Mehrwert – mitbringen (siehe Seite 66), gibt es anderswo nicht. Kurzum, wer sein Recht auf freie Wahl des Routers ausschöpfen will, kommt an den Fritzboxen kaum vorbei.

Wir geben auf den folgenden Seiten Ratschläge, worauf Sie bei der Anschaffung der zu Ihrem neuen Internetanschluss passenden Fritzbox achten müssen und schauen außerdem auf Optionen, die zurzeit besonders wichtig sind (VPN zwischen Homeoffice und Fritzbox in der Firma) beziehungsweise mittelfristig relevant werden, also schnelles (W)LAN mit NBase-T alias Multigigabit-Ethernet und Wi-Fi 6. Wo es passt, listen wir die aktuell erhältlichen Modelle mit ihrer Nummer.

Der Artikel auf Seite 84 zeigt, wie man sich mit IPv6 Wege von außen ins eigene Netz bahnt, um etwa Webcam-Bilder abzurufen oder Vatis PC fernzuwarten. Ab Seite 88 lernt die Fritzbox, unterstützt von einem Raspberry Pi und einem alten Smartphone, automagische Kostenminimierung für Gespräche in Mobilfunknetze. Die Internetverfügbarkeit lässt sich mit einem USB-LTE-Stick sicherstellen, indem die Fritzbox ins Mobilnetz wechselt, wenn der DSL- oder der Kabelanschluss ausfällt (Seite 96). Häufige Fragen rund um die Router klärt die FAQ ab Seite 100.

Providerauswahl

Welche Fritzbox Sie brauchen, hängt in erster Linie davon ab, für welches Internetangebot von welchem Provider Sie sich entscheiden. Denn der gibt

Fünf Fritzboxen bieten Auswahl für die drei wichtigsten Zugangsarten: DSL (7590 und 7530), TV-Kabel (6660 und 6591) und LTE-Mobilfunk (6890 LTE).

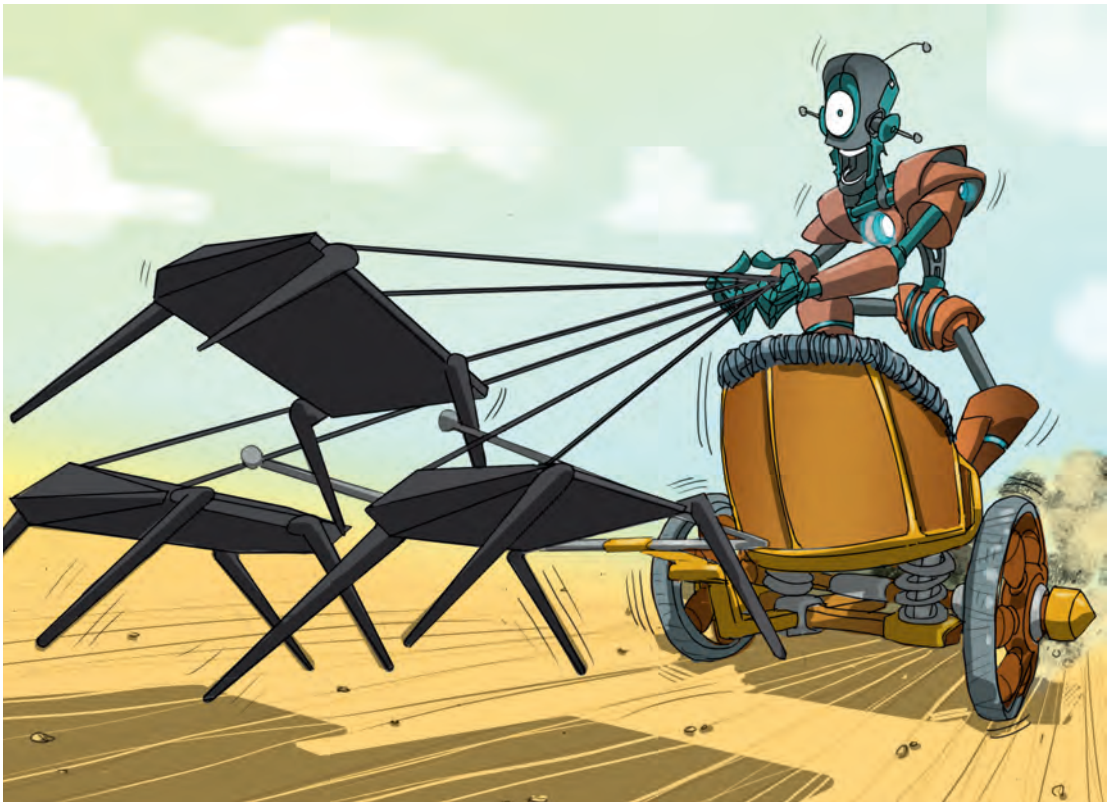


Bild: Thorsten Hübner

WLAN-Steuerung für Access-Points

Manchmal können Repeater oder Mesh-Kits zu wenig, etwa wenn man überall schnelles WLAN getrennt für Familie, Gäste und Smart-Home-Gadgets möchte. c't schaut auf vier WLAN-Controller-Lösungen für Mehrzonen-Netze und liefert Tipps für die Einrichtung.

Von **Sebastian Piecha**

Wer mehrere Funknetze für verschiedene Anwendungen haben möchte, dem genügt ein einfacher Repeater oder ein Mesh-WLAN-Kit nicht. Denn die können immer ein Netz weiterleiten, oft auch ein zweites, aber nie ein drittes oder gar viertes. Der Weg zum Mehrzonen-WLAN im ganzen Haus führt deshalb über eine Infrastruktur mit Access-Points, die die Multi-SSID-Technik und VLAN-Tagging beherrschen. Dann muss man den Cloud-geschwätzigen, gegen Attacken anfälligen Staubsauger nicht ins gleiche WLAN stecken wie das smarte Türschloss.

Solche WLANs möchte man auch bei kleinen Installationen möglichst zentral einrichten statt per individueller Konfiguration jeder einzelnen Basis. Dafür haben viele Access-Point-Hersteller WLAN-Controller im Angebot, sei es als eigenes Gerät (Appliance), Server-Software, virtuelle Maschine oder Cloud-Dienst. Wir vergleichen die Controller-Optionen von vier Anbietern preisgünstiger APs: Grandstream, Mikrotik, TP-Link und Ubiquiti.

Mit solch einer zentralen Instanz können auch kleine Firmen eine Authentifizierung über individuelle Passwörter oder Zertifikate mit WPA2-Enterprise (auch WPA2-Radius bzw. -EAP) einrichten, sodass man nicht überall die WLAN-Einstellungen ändern muss, wenn ein Mitarbeiter ausscheidet. Ebenso lässt sich ein Hotspot mit Einmal-Vouchern aufbauen, der beispielsweise Hotelgästen über ein Portal den Internetzugang für einen bestimmten Zeitraum gewährt.

Muss man zusätzliche APs installieren, um mehr Fläche zu versorgen, oder dieselbe besser, dann geht das mit einem Controller sehr leicht: Oft genügt es schon, die neue Basis nur anzuschließen, manchmal braucht sie auch einen Tastendruck. Damit eine solch einfache Provisionierung klappt, muss der neue AP freilich vom selben Hersteller kommen wie die alten. Schließlich überwacht der Controller das Netz auch: Man sieht leicht, wie viele Clients sich auf welche APs und die Funkbänder (2,4 und 5 GHz) verteilen, welchen Traffic sie verursachen und wo vielleicht ein WLAN-Flaschenhals entsteht.

Netzprobe

Wir haben pro Hersteller mindestens zwei Access-Points mit den zugehörigen Controllern live ausprobiert und dafür ein nichttriviales Netz aufgebaut (siehe Grafik). Als Besonderheit soll eine SSID (logisches Funknetz) mit dynamischer VLAN-Zuweisung laufen: Der Radius-Server teilt dem AP bei der Anmeldung eines Clients mit, in welche Netzzone

Testnetz mit VLANs

Als Prüfstein für die WLAN-Controller-Funktionen dient ein Netz mit mehreren VLANs, in dem die AP-Steuerung von den Nutzerdaten getrennt ist.

VPN-Server mit dem Raspi

Den Datenverkehr von Smartphone oder Notebook in öffentlichen WLANs sollte man mit VPN-Technik wie WireGuard schützen. Wer keinen VPN-Zugang mieten will, kann günstig und mit überschaubarem Aufwand selbst ein System als WireGuard-VPN-Server herrichten – ein Raspberry Pi genügt.

Von **Peter Siering**

Für WireGuard als VPN-Zugangstechnik sprechen einige Punkte: Das Protokoll ist Roaming-robust, VPN-Verbindungen überleben Wechsel zwischen WLAN- und Mobilfunkbetrieb ohne spürbare Unterbrechung. Die Einrichtung ist leicht, weil auf beiden Seiten nur je ein Zertifikat notwendig ist. Aufgrund des neuartigen Ansatzes verspricht WireGuard obendrein maximale Geschwindigkeit bei blitzschnellem Verbindungsaufbau.

Die typischen Rollen von Client und Server sieht WireGuard selbst gar nicht vor. Letztlich ist es nur eine Technik, die sichere Tunnel zwischen Systemen (Peers) knüpft. Ein in VPN-Kreisen typisches Road-Warrior-Szenario mit einem Server und Clients wird erst daraus, wenn man einem Peer die besondere Rolle des Servers zuschanzt und ihm als Gateway beibringt, die Pakete der anderen Peers geeignet weiterzuleiten – also letztlich als Router für sie zu arbeiten.

Als WireGuard-Server eignen sich derzeit Linux-basierte Systeme, egal ob ein vollwertiges Serversystem, ein V-Host oder ein Raspberry Pi. Die Clients bauen über einen UDP-Port einen Tunnel zum Server auf und schicken alle Daten dann durch ihn hindurch. Man hat es nicht mit speziellen Protokollen

oder besonderen Portkombinationen zu tun. Es genügt eine einfache Weiterleitung, wenn der Server hinter einer Firewall oder einem heimischen Router steht.

Wer WireGuard nutzt, muss sich darüber im Klaren sein, dass der Erfinder Jason A. Donenfeld noch munter daran arbeitet. Es erscheinen laufend neue Versionen. Das heißt, man wird in nächster Zeit mit den Updates allerhand zu tun haben. Und viel wichtiger: Er rät explizit von produktivem Einsatz ab, weil viele Aspekte noch nicht akribisch untersucht sind. Andererseits sind die Vorzüge verlockend.

Letztlich müssen Sie selbst entscheiden: Sind die Vorzüge das Risiko wert? Als Maßnahme, um in öffentlichen Netzen die Pakete vor den Blicken anderer Nutzer und eventuell der Betreiber zu schützen, ist es sicher eine gute Wahl. Als alleiniges Zugangsprotokoll zur Wartung eines Unternehmensnetzes mit empfindlichen Daten wird man es eher nicht empfehlen – genauso, wie seine Vorgänger.

Adressen würfeln

Bevor Sie sich den wesentlichen Handgriffen der Installation zuwenden, sollten Sie den zukünftigen WireGuard-Server vorbereiten. Wir zeigen das im Folgenden für Debian und Raspbian. Es lässt sich auf viele andere Distributionen übertragen. Zunächst müssen Sie sich Gedanken darüber machen, welche IP-Adressen Sie den VPN-Clients zuteilen. Die müssen bei WireGuard in einem separaten IP-Netzwerk landen, in dem auch der Server eine Adresse bekommt.

Der WireGuard-Server dient dann als Router. Das heißt, er leitet die von einem WireGuard-Client eingehenden Pakete über seinen Internet-Zugang wei-

Sicher unterwegs

Ein Client in einem nicht vertrauenswürdigen Netz wie einem WLAN-Hostspot verbindet sich mit dem VPN-Server. Der Client greift dann nicht mehr direkt auf Dienste im Internet zu, sondern schickt alle Daten verschlüsselt durch den Tunnel zum VPN-Server. Der packt sie aus und schickt sie an andere Systeme im Internet weiter. So laufen durch das nicht vertrauenswürdige Netz nur verschlüsselte Daten. Oft kommt solche Technik zum Einsatz, um sicheren Zugriff auf ein firmeneigenes Netzwerk einzurichten.

Bild: Albert Hulm

Netzwerk-Live-Diagnose

Welcher Nutzer legt gerade meine Internet-Leitung lahm? Welche Netzwerkgeräte sind aktiv und wie viele Daten übertragen sie gerade? Solche Fragen beantwortet kaum ein Heim- oder Unternehmensrouter. Die Lücke lässt sich mit dem mächtigen und doch übersichtlichen Monitoring-Tool ntopng schließen.

Von **Johannes Weber**

Wenn Sie ein Heim- oder Firmennetz administrieren und detaillierte Auskünfte über den laufenden Verkehr brauchen: Verschwenden Sie keine Zeit damit, die Menüs Ihres Routers nach solchen Monitoring-Funktionen abzugrasen. Bessere Heimrouter zeigen vielleicht die aktuelle Auslastung der Sende- und Empfangsrichtung, aber mehr nicht. Selbst hochpreisige Enterprise-Firewalls schreiben nur brav ins Log, welche Geräte IP-Sitzungen aufgebaut haben (z. B. für Downloads oder Videokonferenzen), und das auch erst, wenn sie beendet sind; Sie merken allenfalls hinterher, wenn etwas aus dem Ruder gelaufen ist.

Hilfsweise kann man den gesamten Verkehr aufzeichnen und ihn beispielsweise in Wireshark analysieren. Dazu klemmt man einen präparierten PC, wie wir ab Seite 150 beschreiben, in das Netzwerk ein und lässt ihn gesendete und empfangene Pakete mitschneiden. Zum Anzapfen eignen sich Spiegelports von managebaren Switchen oder TAPs, die man ins Kabel einschleift (Terminal Access Point). Manche Heim-Router können den IP-Verkehr ebenfalls aufzeichnen.

Die Position des Mitschnittgeräts ist entscheidend: Damit es relevanten Verkehr mitschneidet, muss es zwischen Quelle und Ziel des zu analysierenden Verkehrs von Netzwerkstationen oder Subnetzen stehen. Einen TAP fügen Sie also in die LAN-Leitung zum Router ein, wenn Sie zum Beispiel den Internet-Verkehr von Smart-TV und Webcam analysieren wollen. Wenn Sie statt eines TAPs den Spiegelport verwenden wollen, müssen Smart-TV und Webcam direkt an diesem Switch angeschlossen sein.

Allerdings hat jede der Mitschnittmethoden Grenzen: Bei hoher Last können Pakete durchrutschen oder die Latenz wird zu lang. Verfälschte Mitschnitte erschweren aber die Analyse oder vereiteln sie sogar. Wie Sie kostengünstige Mitschnittgeräte aufsetzen und was sie von ihnen erwarten können, beschreiben wir ab Seite 150. Allerdings lauern bei Mitschnitt und beim Auswerten etliche Stolperfallen. Hilfestellung dafür finden Sie ab Seite 156, wo wir zudem auf Szenarien in Unternehmensnetzen eingehen.

Wenn es halbwegs praktikabel wäre, würden viele Admins den Verkehr ganzjährig aufzeichnen, um etwa mittels historischer Daten auch spät entdeckte Einbrüche rekonstruieren zu können. Das scheitert aber schon an Plattenplatzanforderungen. In der Praxis begnügt man sich damit, Metadaten des Verkehrs aufzuzeichnen, also etwa Quelladresse, Zieladresse, Quell- und Zielport, Protokoll, übertragenes Volumen. Spezialisierte Monitoring-Tools lesen solche Daten umgehend aus den IP-Paketen aus und blenden sie als „NetFlow“ in grafischen Oberflächen ein – so kann man den

Netzverkehr-Mitschnitt mit TAPs

Einen Terminal Access Point schleift man in die Verbindung zwischen Quelle und Ziel ein, im Beispiel sind das ein Smart-TV und das Internet. Den Verkehr anderer Geräte, etwa PC und NAS (gestrichelte Linie) sehen TAP und Mitschnittgerät nicht.

Bild: Henning Rathjen

Campusnetz-Planung

Erstmals können Fabriken und Institute ihre WLAN-gestützten Infrastrukturen mit einem lokalen Mobilfunknetz ergänzen und so ihre Produktion optimieren. Doch wer braucht ein solches Campusnetz und wie konzipiert man es?

Von **Dušan Živadinović**

Jahrelang haben vor allem große Unternehmen ein separates Funkband für die Vernetzung ihrer Produktionsanlagen gefordert. Im Herbst 2019 hat die Bundesnetzagentur endlich einen 100 MHz breiten Block zwischen 3,7 bis 3,8 GHz speziell für Campusnetze reserviert. Firmen, die ein solches Band schon länger gefordert hatten, planen längst, ihre Produktion damit aufzurüsten.

Vielen Unternehmen ist aber noch unklar, worin genau die Vorteile eines Mobilfunk-Campusnetzes liegen, denn sie verwenden für viele Prozesse schon längst das etablierte und preisgünstige WLAN als Campusnetz. Je nach Anwendung kann man mit WLAN aber schnell an Grenzen stoßen.

Wir fassen daher zunächst die prinzipbedingten WLAN-Nachteile zusammen, damit Sie anhand Ihrer Anforderungen entscheiden können, ob Ihnen ein mobilfunkgestütztes Campusnetz weiterhilft. Anschließend beschreiben wir Planungsstrategien für den Aufbau sowie grundlegende Alternativen zur Verwaltung des Netzes.

Ausgangspunkt WLAN-Schwächen

Die WLAN-Konzepte sind einige Jahrzehnte alt. Ursprünglich ging es den Entwicklern nur darum, IP-Pakete über ein von Ethernet abgeleitetes Funkmedium zu übertragen. Das erkennt man daran,

dass ein WLAN-Access-Point wie eine Ethernet-Bridge arbeitet und besonders, weil der Zugriff der Geräte auf den Funkkanal zufallsgesteuert erfolgt (Carrier Sense Multiple Access/Collision Avoidance, CSMA/CA).

Das hat weitreichende Folgen:

- WLAN-Geräte können Pakete nicht innerhalb fester Fristen zustellen. Diese sind zum Beispiel für die Steuerung von Fertigungsrobotern erforderlich, etwa um sie umgehend anhalten zu können, falls ein Mensch einen Gefahrenbereich betritt.
- Man kann unterschiedlichen WLAN-Geräten keine festen, aber unterschiedlichen Geschwindigkeiten zuweisen (z. B. 30 MBit/s für einen USB-Stick und 50 MBit/s für ein Tablet). Allenfalls lassen sich Datenpakete von bestimmten IP-Diensten bevorzugt gegenüber anderen behandeln (zum Beispiel Voice-over-IP vor Webzugriffen). Aber das schließt nicht aus, dass mit WLAN das eine oder andere Paket zu spät oder gar nicht am Ziel ankommt. Beides sind Ausschlusskriterien für Prozesse mit harten Anforderungen an Übertragungsfristen und hohe Zuverlässigkeit.
- WLAN-Geräte funken generell munter durcheinander, so wie sie gerade eine freie Sendelücke erwischen. Je mehr WLAN-Geräte im Netz sind, desto wahrscheinlicher sind Kollisionen von Datenpaketen und desto länger muss jedes einzelne warten, bis es eine Lücke findet – die Effizienz lässt also umso stärker nach, je mehr Nutzer eine Basisstation versorgen soll.
- Ein nahtloser Zellenwechsel ist mit WLAN grundsätzlich nicht möglich (seamless handover). Das verhindert auf großen Geländen beispielsweise den Einsatz in autonomen Fahrzeugen.

Diese konzeptionellen Nachteile ziehen sich bis hin zur heute verbreiteten WLAN-Spezifikation IEEE 802.11ac durch. Hinzu kommen regulatorische Grenzen: Aufgrund der Sendeleistungsbestimmungen ist für die vollständige Abdeckung großflächiger industrieller Bereiche (mehrere Quadratkilometer) oft eine Vielzahl von WLAN-Access-Points erforderlich. Beispielsweise darf WLAN mit maximal 1 Watt EIRP senden, aber dieser Wert gilt für alle Antennen zusammen (kein Mauseloch für MIMO). So gilt zwischen 5,470 und 5,725 GHz eine Obergrenze von 0,05 W/MHz als spektrale Begrenzung.

Die Reichweite von Mobilfunkbasisstationen ergibt sich aus diversen Parametern. Zunächst setzt die Bundesnetzagentur (BNetzA) in ihrer Verwaltungsvorschrift keine Obergrenze für die maximale Sendeleistung von Campusnetzen – abgesehen von den gesetzlichen Grenzwerten zum Schutz von Personen. Nur für den Fall, dass sich Nachbarn nicht einigen können (Verhandlungsgebot für Betreiberabsprachen) wird pragmatisch ein Feldstär-