

ct Netzwerke

Praxiswissen • Kaufberatung • Troubleshooting

Komplettpaket Diagnose und Reparatur

57 Tools – ein Download

VPN für Laptop und Smartphone

Praxis Virtualisierung

SBS-Migration auf Linux

Haftungsrisiken für Admins

Software für Server

Apple, Microsoft, Linux: Was drin ist,
was sie können, wo es kneift

Test und Technik

Einsteiger-USVs, intelligente Switches,
günstige Router, Server für Kleingruppen

NAS statt Server

Netzwerkspeicher für zu Hause und Büro



I:HOSTSERVER

Managed Hosting

IT-Sicherheit zertifiziert nach ISO 27001

- ✓ IT-Sicherheit
- ✓ Qualitätssicherung
- ✓ Datenschutz



Managed Hosting
zertifiziert nach
ISO 27001:2005 und
ISO 9001:2008

Hosting made in Germany

Professionelles Hosting am Standort Deutschland mit persönlichem und kompetentem Support. Individuelle Hostinglösungen vom Server bis zum Cluster-Cloudsystem, inklusive Beratung, Planung und Service 24/7

Wir bieten über 10 Jahre Erfahrung in Hosting und Systemadministration. Für mehr Performance, Sicherheit und Verfügbarkeit.

hostserver.de/hosting

I:HOSTSERVER
Berlin ■ Marburg ■ Frankfurt am Main

Beratung unter:
0 30 / 47 37 55 50



Liebe Leserin, lieber Leser,

Medienspieler, Fernseher, Smartphones und nicht zuletzt PCs brauchen ein vernetztes Heim, um ihr Potenzial voll entfalten zu können. In Büros, Praxen und Firmen sorgen Netzwerke für den Anschluss an die weite Welt sowie den Zugriff auf gemeinsame Dokumente und Drucker.

Mit unserem c't special lassen Sie diese Netze weiter aufleben: intelligente Switches, um das Sammelsurium aus Hubs und dummen Switches zu beseitigen, VPN-taugliche Router, um auch von unterwegs auf die Dateien zugreifen zu können, USVs, um gegen überraschende Stromausfälle gewappnet zu sein, und vor allem das richtige NAS als zentrale Dateiablage.

Bei wachsender Benutzerzahl lohnt sich auch die Überlegung, ob ein NAS noch genügt oder schon ein Server her muss. Wer diese Entscheidung zugunsten eines Servers fällt, sollte sich dazu mit Virtualisierung beschäftigen. Das hilft, die Zahl der Server-Systeme gering zu halten, ohne auf die Vorzüge mehrerer Instanzen verzichten zu müssen.

Trotz aller Technikbegeisterung sollten Sie dabei nicht die damit einhergehende Verantwortung aus den Augen verlieren: Als Administrator lernen Sie die rechtliche Situation einzuschätzen und erfahren, was Sie beim Betreiben eines Mail-Servers für andere zu beachten haben.



Peter Siering

NAS statt Server

Netzwerkspeicher bewahren nicht nur Dateien auf. Je nach Geräteklasse beliefern sie TV- und andere Mediengeräte mit Inhalten oder versorgen Benutzer mit E-Mail- und Groupware-Diensten, ganz wie ein echter Server. Unser Rundumschlag:

- 34 Entscheidungshilfe zwischen NAS und Server
- 40 NAS für das Heimnetz und das kleine Büro
- 47 Tipps für die Grundkonfiguration
- 52 Erweitern über den offiziellen Lieferumfang hinaus
- 56 Für die Profiligena



Tests und Technik

Alles, was Sie zum Aufbau eines Netzes brauchen: Router gleich mit VPN-Server, konfigurierbare Switches mit zahlreichen Extras, solide Server für Arbeitsgruppen und unterbrechungsfreie Stromversorgung – ergänzt um einige findige Produkte.

- 64 Server für Arbeitsgruppen
- 70 Intelligente Switches
- 78 Unterbrechungsfreie Stromversorgung
- 84 Router mit VPN-Server
- 90 Pfiffige Produkte fürs Netzwerk

Software für Server

Sowohl Apple als auch Microsoft wollen passend zu den Client-Betriebssystemen ihre Server-Software verkaufen. Auch Linux hat hier einiges zu bieten. Ein weiteres Pfund wirft Software zur Virtualisierung in den Ring. Unsere Sondierungshilfen:

- 94 Windows-Server-Varianten
- 98 Linux-Distributionen für Server
- 102 Apples Server-Welt im Detail
- 110 Pro und Contra von Virtualisierung

INHALT

Grundlagen

- 6 Kabel und Funk
- 10 Dienste und Protokolle
- 14 Kostenlose DynDNS-Dienste
- 20 Breitbandtarife für DSL und Kabel
- 26 Haftungsrisiken für Administratoren
- 31 Rechtlicher Rahmen für Mailserver

NAS statt Server

- 34 NAS oder klassischer Server
- 40 Für daheim
- 47 Erste Handgriffe
- 52 Mit Software aufwerten
- 56 Für kleine Firmen und Büros

Hardware für Netzwerker

- 64 Bezahlbare und leise Server für kleine Gruppen
- 70 Konfigurierbare Gigabit-Switches
- 78 Unterbrechungssicherer Notstrom fürs Büro
- 84 Router mit VPN-Zugang
- 90 Netzwerk-Tester
- 90 LAN-Temperatursensor
- 91 Rauchmelder-Design: Dualband WLAN-Basis
- 91 Dualband WLAN-Router
- 91 USB-Airprint-Server

Server-Software

- 92 Windows für Server
- 98 Linux für Server
- 102 Apples Server-Welt
- 110 Server: virtuell vs. real
- 114 E-Mail-Server mit Windows
- 118 Active Directory
- 126 Hyper-V Replica aufsetzen

Praxis, Tipps und Tricks

- 134 Netzwerk-Tools für die Fehlersuche
- 142 Von Microsoft SBS auf Linux
- 149 USV-gesteuert abschalten
- 152 Tipps für einen sicheren Start mit IPV6
- 158 Router und Mobilgeräte fürs VPN einrichten
- 164 OpenVPN-Server auf DD-WRT-Router
- 168 Hotline

Zum Heft

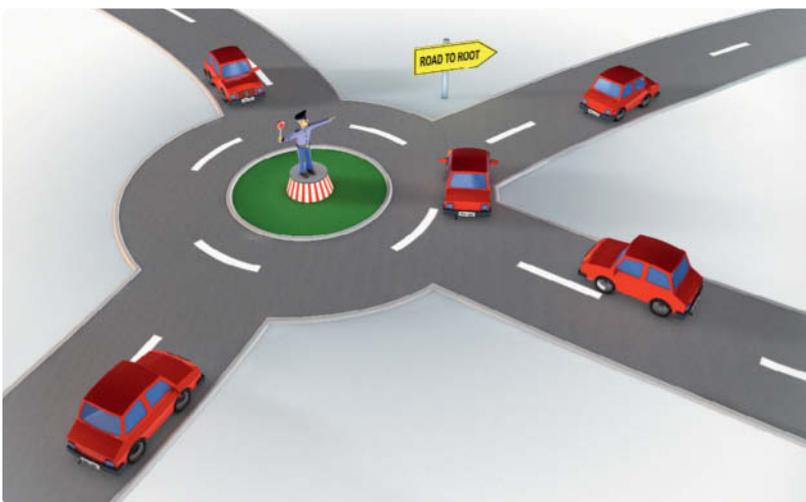
- 3 Editorial
- 167 Impressum
- 167 Inserentenverzeichnis



Komplettpaket Troubleshooting

Die wichtigsten Werkzeuge des c't-Netzwerkwerkzeugkastens bekommen Sie geballt als Download. Der Artikel zeigt Wege auf, um Problemen im Netzwerk auf die Schliche zu kommen. Einige Extraprogramme sind nur für Heftkäufer erhältlich.

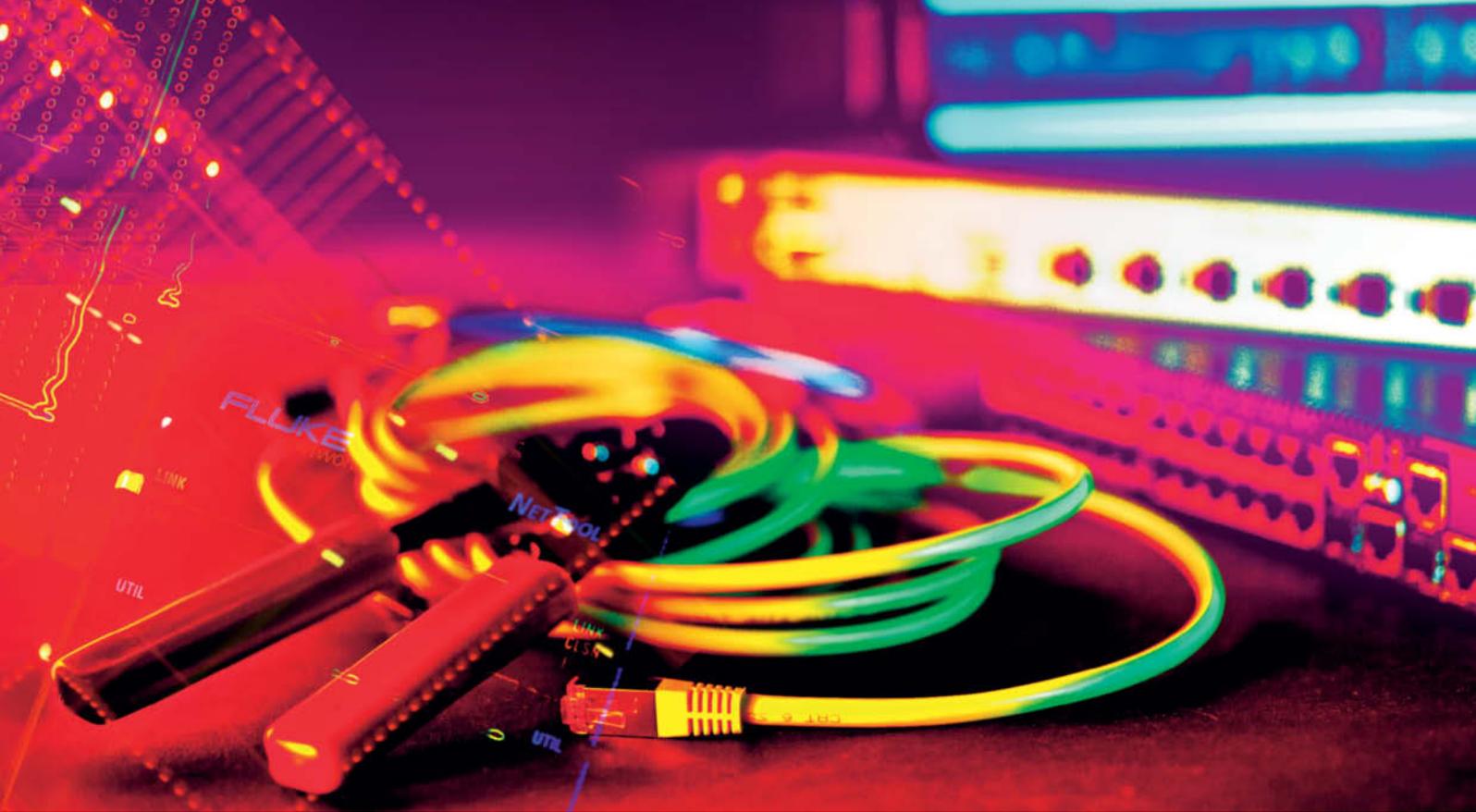
- 134 Netzwerk-Tools für die Fehlersuche



Praxis, Tipps und Tricks

Netzwerke sind deutlich pflegeleichter geworden, doch gleichzeitig sind die Möglichkeiten und Anforderungen gewachsen. Die Praxis-Artikel sowie die Tipps & Tricks stellen sich der einen oder anderen nicht allzu alltäglichen Aufgabe für den Admin-Alltag.

- 114 Windows Home Server als Mail-Server
- 126 Automatische Backups für Hyper-V-VMs
- 142 Vom Microsoft-SBS auf Linux umziehen
- 168 Fragen und Antworten aus der c't-Hotline



Ernst Ahlers

Kabel und Funk



www.ct.de/cs1304006

Bei einem selbstständigen Berufseinsteiger genügt noch der vom Internet-Provider bereitgestellte Router als Kern des kleinen Büronetzwerks. Doch schon, wenn der erste Angestellte dazukommt, reichen entweder die physischen Anschlüsse oder die Funktionen nicht mehr aus. Mit etwas Vorwissen lassen sich Fehlinvestitionen beim Ausbau des Netzes vermeiden.

Wenn die Kabelanschlüsse des Routers belegt sind, denkt fast jeder sofort daran, weitere Geräte per WLAN anzuschließen. Doch das ist nicht immer eine sinnvolle Idee: Selbst die derzeit schnellste, mit 1300 MBit/s beworbene WLAN-Variante nach dem kommenden IEEE-Standard 802.11ac transportiert über Distanz – in der c't-Testsituation 20 Meter durch mehrere Wände – je nach Gerätemodell allenfalls 150 bis 300 MBit/s auf Anwendungsebene (netto), also 19 bis 38 MByte/s. Die bisher gängige WLAN-Technik 802.11n kommt sogar nur auf etwas über 100 MBit/s (12 MByte/s).

Ein simples Patchkabel liefert an Gigabit-Ethernet-Schnittstellen dagegen 930 MBit/s netto (115 MByte/s), 10-Gigabit-Ethernet

(10GE) über Kabel (10GBaseT) oder Glasfasern (10GBaseSX, LX) gar das Zehnfache. 10GE ist inzwischen erschwinglich, wenn auch derzeit nur zum Anbinden richtig schneller Server und Massenspeicher (NAS, Network Attached Storage) sowie für Querverbindungen zwischen Gigabit-Switches in mittleren und großen Firmen sinnvoll eingesetzt.

Wenn Sie regelmäßig große Datenmengen wie etwa Backups oder zu bearbeitende Videos im Netz hin- und herschaufeln, spüren Sie den Unterschied der Nettodatenrate von WLAN und LAN unmittelbar. Das Kabel bleibt also auch in Zukunft erste Wahl. WLAN sollte man nach wie vor als Ergänzung eines verkabelten Netzes für mobile Geräte verstehen, mehr dazu weiter hinten.

Powerline Communication, die Datenübertragung über die Stromleitung, und ihre Pendanten für TV-Kabel – geläufig unter anderem als CoaxNet oder CableLAN – und Telefonkabel kommen hauptsächlich in Heimnetzen zum Einsatz. Dort nutzen sie vorhandene Medien für den Datentransport mit. Nützlich sind diese Techniken beispielsweise, um weit vom DSL-Router entfernte Räume mit WLAN zu versorgen, wenn sich dahin partout kein Ethernet-Kabel legen lässt.

Auch in manchen Hotels oder Krankenhäusern läuft die nachträglich installierte Gäste- beziehungsweise Patientenversorgung mit Internet über solche schon vorhandenen Systeme. Diese Alternativen transportieren Daten deutlich langsamer als Gigabit-



Ein konfigurierbarer Gigabit-Switch bildet den Kern kleiner Netze. Die Investition von 110 bis 400 Euro ist gut angelegt, auch wenn Sie Funktionen wie VLANs oder Radius-Authentifizierung jetzt noch nicht brauchen.

Ethernet (siehe Tabelle auf Seite 8). Fürs Büro taugen sie also wenig.

Kabel-Infrastruktur

Solange Sie im Heimbüro arbeiten, stören ein paar hinter den Schreibtisch geworfene Patchkabel nicht. Aber schon, wenn sich ein Vierer-Team auf mehrere Räume verteilt, sollten Sie über eine systematische Verkabelung nachdenken. Denn ein durch drei Zimmer verlegtes 20-Meter-Patchkabel lässt sich wesentlich schwerer austauschen als die 3-Meter-Variante, die zur Wandsteckdose führt, wenn mal ein Bürostuhl mit zu viel Gewicht darüber gerollt ist. Falls Sie die Installation selbst erledigen oder beim Einsatz eines Dienstleisters ein Auge darauf halten wollen, gibt der heise-Netze-Artikel „Strippen ziehen“ Hinweise zum Aufbau einer gigabitfähigen Kabel-Infrastruktur (siehe Downloads).

Denken Sie schon jetzt an die Zukunft: Das dort vorgeschlagene CAT5e-Kabel reicht zwar nach unserer Erfahrung für 10-Gigabit-Ethernet aus. Aber in einigen Jahren könnte sich die viermal schnellere Variante 40GBaseT ausbreiten. Falls Sie erwarten, solche Datenraten zu brauchen, sollten Sie schon jetzt CAT8-Kabel in die Wand oder den Kabelkanal bringen. Das – und die zugehörigen Patchfelder und

Dosen – richtig zu installieren ist aber Aufgabe von Fachfirmen.

Schaltstellen

Ein konfigurierbarer Gigabit-Switch (siehe Test auf Seite 70) bildet den Kern eines kleinen Netzes. Die 110 bis 400 Euro dafür sind gut angelegt, auch wenn Sie Funktionen wie VLANs oder Radius-Authentifizierung jetzt noch nicht brauchen. Allein die Möglichkeit, per Port Monitoring seltsamen Netzphänomenen auf die Schliche zu kommen, ist das Geld wert. Denn das Monitoring lässt sich einfach per Browser-Konfiguration einrichten, sodass man nicht mit in die Leitung eingeschleiften Diagnose-PCs mit zwei Schnittstellen oder passiven Taps tricksen muss.

Switches mit Fast Ethernet (100 MBit/s) sind zwar etwas billiger, aber die geringe Einsparung rechtfertigt die enorme Geschwindigkeitseinbuße nicht im Mindesten. Selbst geschenkt etwa aus Firmenauflösungen sollten Sie solche Geräte nicht mehr verwenden, denn alte Modelle haben eine unzeitgemäß hohe Leistungsaufnahme, was die Stromkosten treibt.

Falls das LAN später wächst, können Sie mehrere Switches kaskadieren, indem Sie sie schlicht miteinander verbinden. So werden aus 24 Ports 46, oder bei Wahl eines 48-Port-Modells als Erweiterung gleich 70 Ports. Stehen

Switches räumlich weit voneinander entfernt, dann ist eine optische Verbindung per Glasfaser mittels SFP/MiniGBIC-Modulen sinnvoll.

Soll die Querverbindung Daten schneller als mit den heute üblichen 1000 MBit/s von Gigabit-Ethernet transportieren, dann können Sie mehrere Ports bündeln (Link Aggregation). Ab vier gebündelten Links lohnt es sich aber schon, über ein Upgrade auf 10-Gigabit-Ethernet nachzudenken. Denn solche Bündel beschleunigen zwar den Gesamtdurchsatz, nicht aber einzelne logische Verbindungen.

Switches, die auch Energie per Power-over-Ethernet liefern (PoE nach IEEE 802.3af für maximal 13 Watt Gerätebedarf oder 802.3at, 25 Watt), sind typischerweise ein-, zweihundert Euro teurer. Sie werden nicht nur beim Einsatz von VoIP-Telefonen nützlich, sondern ersparen bei WLAN-Basen und LAN-Überwachungskameras die kosten-trächtige Installation zusätzlicher Stromsteckdosen. Allerdings lohnt sich ein PoE-Switch erst ab etwa vier versorgten Geräten, darunter kommen Sie mit einem herkömmlichen Modell und separat installierten PoE-Injektoren billiger davon.

Funk ergänzt Kabel

Wenn mobile Geräte wie Ultrabooks, Tablets und Smartphones auch im Büro einen



Powerline-Adapter, die Daten über die Stromleitung schicken, gibt es in vielen Bauformen, unter anderem mit integriertem Switch und WLAN-Basis. Allerdings ist ihr Einsatz in Firmen kaum sinnvoll. Sie sind besser in Heimnetzen aufgehoben, da der Nutzdurchsatz nur zwischen 40 und 100 MBit/s liegt, selten darüber.

Auch über TV-Koaxkabel und interne Telefonleitungen lassen sich Daten jagen: Zwar gibt es passende Adapter, aber preisgünstige Exemplare schaffen typischerweise nur 30 bis 90 MBit/s Nettodurchsatz.



schnellen Netzzugang haben sollen, gleich ob zum Internet oder zu internen Diensten, bietet sich das Ergänzen des installierten Kabel-LAN um einen oder mehrere WLAN-Access-Points (APs), also Basisstationen, an.

Doppelbasen

Dabei sollten Sie AP-Modellen den Vorzug geben, die sich zum einen per PoE speisen lassen, was die Installation vereinfacht.

Zum anderen sollten die Basen in beiden WLAN-Bändern 2,4 und 5 GHz parallel funken. Dann können Sie langsame Smartphones, die nur 2,4 GHz beherrschen, getrennt von den flotteren, dualbandfähigen Ultra-books auf 5 GHz bedienen. So nutzen Sie das für WLAN zugeteilte Funkspektrum besser aus, was der Datenrate zugutekommt.

Weitere Nützlichkeiten sind Multi-SSID, VLAN-Mapping und Radius-Authentifizierung:

Mit Multi-SSID kann der AP auf jedem seiner Funkmodule mehrere logische Funkzellen anbieten, etwa für Mitarbeiter und Gäste getrennt. Das VLAN-Mapping sorgt dann dafür, dass die Trennung im Kabel-LAN fortgesetzt wird und die Gäste zwar ins Internet kommen, aber nicht auf interne Hosts zugreifen können. Für den separierten Internetzugang muss dann ein Router sorgen, der mehrere VLANs bedienen kann. Auch solche Geräte sind inzwischen für

Datenraten typischer Anwendungen

Anwendung	Datenrate	Charakteristik
Chatten	< 0,0001 MBit/s	schubweise
Internet-Telefonie	0,016 bis 0,080 MBit/s	durchgehend
Musik-Streaming	0,03 bis 0,3 MBit/s	durchgehend
DivX/Xvid-Video (MPEG-4)	1 bis 1,3 MBit/s	durchgehend
unkomprimiertes CD-Audio	1,5 MBit/s	durchgehend
Websurfen, E-Mail	1 bis 6 MBit/s	schubweise
DivX/Xvid in HD	4 bis 8 MBit/s	durchgehend
DVD-Video (MPEG-2)	5 bis 10 MBit/s	durchgehend
HD-Video (H.264, MPEG-2)	10 bis 20 MBit/s	durchgehend
UHD-Video (H.264, H.265)	10 bis 40 MBit/s	durchgehend
Backup, Daten kopieren	90 bis 900 MBit/s	schubweise
unkomprimiertes HD-Video (1080p, 24 Bit/Pixel)	3000 MBit/s	durchgehend
unkomprimiertes UHD-Video (2160p, 24 Bit/Pixel)	12 000 MBit/s	durchgehend

Vernetzungstechniken

Technik	Reichweite im Gebäude	Datenrate auf Medium	Typische Datenrate auf Anwendungsebene
TV-Kabel (Koax)	bis 600 Meter Kabellänge	max. 200/500 MBit/s	30 bis 200 MBit/s
Telefonkabel (Zweidrahtleitung)	bis 600 Meter Kabellänge	max. 200/500 MBit/s	80/200 MBit/s
Powerline (HomePlug AV)	bis 200 Meter Kabellänge	max. 200/600 MBit/s	20 bis 200 MBit/s
Bluetooth 3.0	typisch 20 Meter	max. 3 MBit/s (54 MBit/s ¹)	0,9 bis 2,7 MBit/s (5 bis 20 MBit/s ¹)
WLAN IEEE 802.11g	typisch 20 Meter	max. 54 MBit/s	5 bis 20 MBit/s
WLAN IEEE 802.11n	typisch 20 Meter	max. 72 / 144 / 300 / 450 / 600 MBit/s ²	40 bis 200 MBit/s
WLAN IEEE 802.11ac	typisch 20 Meter	max. 87 / 180 / 390 / 867 / 1333 ... 6933 MBit/s ²	50 bis 400 MBit/s
WLAN IEEE 802.11ad	typisch 5 Meter (Zimmer)	max. 4620 / 6757 MBit/s	noch unbekannt
Ethernet (Fast/Gigabit/10G)	bis 100 Meter Kabellänge	100/1000/10 000 MBit/s	93/930/9300 MBit/s

¹ mit WLAN als sekundärem Medium ² abhängig von Implementierung und Konfiguration (1 bis 8 Antennen, 20 bis 160 MHz Kanalbreite)



WLAN-Access-Points im Rauchmelderdesign sitzen unauffällig an der Decke und werden übers LAN-Kabel mit Strom versorgt. Zyxels NWA1123 (links) etwa funkt in beiden WLAN-Bändern parallel und bietet für Firmen nützliche Extras wie Multi-SSID und VLAN. Allerdings kostet er auch das Vierfache eines Single-Band-AP (Tenda W301A).

unter 100 Euro zu haben, beispielsweise Ciscos RV110W.

In kleinen Teams ist die individuelle WLAN-Anmeldung per Nutzernamen und Passwort (Authentifizierung per IEEE 802.1x/Radius) wohl überflüssig: Ein nach dem Praktikantenabschied geändertes WLAN-Passwort lässt sich auf einem Dutzend Geräten noch einigermaßen schmerzfrei ändern. Doch wenn die Gruppe wächst, ist es sinnvoll, jedem Mitarbeiter eigene Zu-

gangsdaten zu geben (siehe Download-Links). WLAN-APs für Firmeneinsatz unterstützen das in aller Regel, und auch im LAN lässt sich diese Technik mit den ab Seite 70 getesteten Switches verwenden.

Sinnvolle Funkdatenraten

Während für Heimanwender schon seit Herbst 2012 WLAN-Router verfügbar sind, die bis zu 1300 MBit/s brutto schnelle

Funknetze nach IEEE 802.11ac aufspannen, kommen erst jetzt kompatible WLAN-APs für den Firmeneinsatz heraus. Für solche müssen Sie pro Stück mehrere Hundert Euro veranschlagen, während für Geräte nach dem etablierten Standard 802.11n mit bis zu 300 MBit/s etwa 150 Euro fällig werden. Letztere sind zumindest für die nächsten zwei Jahre noch die sinnvollere Wahl, weil bisher nur sehr wenig Mobilgeräte mit 11ac-WLAN kursieren. (ea)

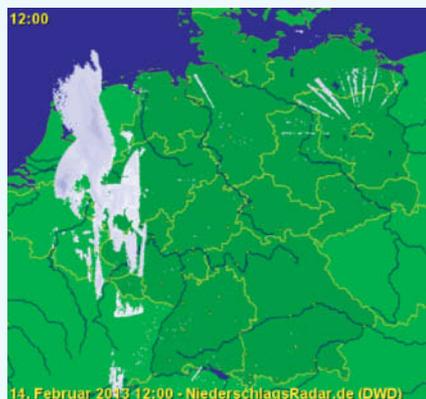
5-GHz-Besonderheiten

Die Bundesnetzagentur hat für WLAN-Betrieb im 5-GHz-Band zwei Frequenzblöcke bereitgestellt: 5,15 bis 5,35 GHz und 5,47 bis 5,725 GHz. Dort finden 19 WLAN-Kanäle zu 20 MHz Breite Platz, also das Sechsfache gegenüber dem 2,4-GHz-Band, sodass sich Wohnungsnachbarn dort wesentlich besser ausweichen können und so gegenseitige Störungen vermeiden. Oberhalb von 5,725 GHz sind 120 MHz für Richtfunk (BFWA) reserviert.

Der untere 5-GHz-Block ist ausschließlich für Indoor-Betrieb vorgesehen, im oberen Block darf man APs auch außerhalb von Gebäuden betreiben. Da im 5-GHz-Band auch militärische und Wetterradare arbeiten, müssen Access Points oberhalb von 5,25 GHz Radarsignale erkennen können und dann automatisch den Kanal wechseln (DFS, Dynamic Frequency Selection). Dabei geht die WLAN-Verbindung für 60 Sekunden verloren, denn der AP muss den neuen Kanal erst auf Radarsignale überprüfen, bevor er und seine Clients wieder senden dürfen. Auf 5 GHz verhält sich WLAN also anders als auf 2,4 GHz.

Um Problemen mit Wetter-Radarsystemen aus dem Weg zu gehen, lassen manche AP-Hersteller die Kanäle 120, 124 und 128 bewusst aus. Denn zwischen 5,60 und 5,65 GHz betreibt beispielsweise der Deutsche Wetterdienst (DWD) seine 16 Radarstationen; hier ist sogar eine DFS-Wartezeit von 10 Minuten vorgeschrieben.

WLAN-Basen, die die kurzen Radarimpulse nicht sicher erkennen können oder DFS erst gar nicht implementieren, und



trotzdem die Kanäle 120 bis 128 nutzen, stören die Wetterradare, besonders prägnant in Ballungsräumen. Stellt der DWD solche Störungen fest, benachrichtigt er die Bundesnetzagentur über die vermutliche Lage. Die Himmelsrichtung kann der DWD mit seinen Radaren ziemlich genau feststellen ($\pm 0,2^\circ$). Das erleichtert dem Peilwagen der Bundesnetzagentur die Suche. Findet dieser den Betreiber des störenden AP, muss der sein Gerät umkonfigurieren oder ausschalten. Der Betreiber hat dann nicht nur für die Kosten des Messeinsatzes aufzukommen, sondern zahlt vielleicht auch ein Bußgeld wegen einer Ordnungswidrigkeit.

Das Radarsystem des Deutschen Wetterdienstes leidet immer wieder unter Störungen fehlerhafter 5-GHz-WLAN-Basen: Im Februar 2013 waren um den Standort Berlin-Tempelhof zahlreiche Speichen erkennbar, die Niederschlag anzeigen, wo keiner fällt.





Peter Siering

Dienste und Protokolle

Wer vor der Aufgabe steht, für eine simple Anforderung wie das Drucken mit einigen Netzwerk-Clients die richtige Lösung zu finden, wird schnell von Akronymen für Dienste und Protokolle erschlagen. Da hilft unser Wegweiser für die gängigen Aufgaben, Plattformen, Protokolle und Dienste im lokalen Netz.

Die gängigste „Sprache“, die alle Client- und Server-Betriebssysteme und sonstige Gerätschaften im Netzwerk heute miteinander sprechen, ist das Internet Protocol (**IP**). Es sorgt dafür, dass ein Befehl oder eine Datei das gewünschte Ziel findet. Auch wenn es „Internet“-Protokoll heißt: Es wirkt auch im lokalen Netz und unabhängig davon, ob Sie ein Gerät per WLAN, Netzwerkkabel oder eben per Internet-Verbindung erreichen.

IP sieht vor, dass jeder Teilnehmer eine eindeutige Adresse hat. Die 32 Bit großen IPv4-Adressen sind heute noch der Standard, die 128 Bit großen IPv6-Adressen wenig in Betrieb – aber meist parallel aktiv. Oft vergibt ein DSL-Router oder Server im lokalen Netz die Adressen (**DHCP**, Dynamic Host Configuration Protocol).

Öffentliche IPv4-Adressen, die übers Internet erreichbar wären, sind knapp. Deshalb benutzt man in lokalen Netzen üblicherweise „private“ Adressen. Die Verbindung zum Internet wird dann über einen Router hergestellt, der eine öffentliche Adresse besitzt. Per Network Address Translation (**NAT**) modifiziert er die ins Internet herausgehenden Netzwerkpakete so, dass sie von seiner

öffentlichen IPv4-Adresse zu stammen scheinen. Die eingehenden Antworten übersetzt er entsprechend zurück.

Jeder gängige DSL-Router benutzt NAT. Das hat positive Seiten: Alle Dienste, PCs und anderen Geräte hinter einem solchen Router sind zunächst vor direkten Angriffen aus dem Internet geschützt. In den Augen vieler Nutzer überwiegen die Nachteile: Immer wieder scheitern Netzwerkdienste an NAT, zum Beispiel solche zur Fernunterstützung und Video-Telefonie. Sie brauchen externe Vermittler, die dann als Brücke über den oder die NAT-Router fungieren.

Sollen Dienste im internen Netz aus dem Internet erreichbar sein, muss der Router Anfragen an einzelne Ports an das richtige lokale System weiterleiten. Das heißt **Port Forwarding** und oft kombiniert man es mit einem Dienst, der die regelmäßig wechselnde IP-Adresse eines DSL-Anschlusses mit einem weltweit eindeutigen Namen versieht (**DynDNS**).

Namen

Apropos Namen: Irgendwer im Netz sollte sprechende Namen wie „MeinServer“ in IP-

Adressen verwandeln. Windows-Systeme verwenden dafür in erster Instanz **Broadcasts**, fragen also alle Geräte im lokalen Netz. Außerdem einigen sie sich auf ein System, das regelmäßig ins Netz gerufene Namensankündigungen sammelt. Das funktioniert manchmal leider eher schlecht als recht.

Das Domain Name System (**DNS**), der Internet-Namensdienst lohnt sich erst, wenn sich mehr als eine Handvoll Rechner in einem lokalen Netz tummelt. Moderne Windows-Server setzen es für den Betrieb eines Active Directory (**AD**) voraus, also Microsofts eigenen Verzeichnisdienst, der alle Systeme im Netz mit einer Benutzerdatenbank versorgt.

In Windows-Netzen ohne Active Directory kann **WINS** (Windows Internet Naming Service) die Namensauflösung beschleunigen. Hier ist es umgekehrt: Obwohl Internet dransteht, taugt es nur für lokale Netze. Alle Clients registrieren sich dort und richten ihre Namensanfragen dorthin. Als WINS-Server eignet sich nur ein dauerlaufendes System, egal ob unter Linux mit Samba, etwa ein NAS, oder ein Original-Windows-Server. Sowohl DNS- als auch WINS-Server sind in die IP-Konfiguration eines jeden Systems einzu-

tragen (ein DHCP-Server kann diese Daten übermitteln).

In Windows Vista hat Microsoft mit dem Peer Name Resolution Protocol (**PNRP**) ein neues Verfahren zur Namensauflösung in Peer-to-Peer-, also Server-losen Netzen eingeführt. Es ist eng mit IPv6 verbunden und hilft Windows-Nutzern bei zwei Dingen: Es erlaubt eine stressfreie Überbrückung von Routern und NAT für die Remote Unterstützung und bringt ihnen Heimnetzgruppen, die das Freigeben von Dateien und Druckern in kleinen Netzen auf die Eingabe eines Passworts reduzieren.

Außerhalb der Microsoft-Welt spielt PNRP keine Rolle: Apple hat mit **Bonjour** ein eigenes Verfahren entwickelt, dem Multicast-DNS-Techniken zugrunde liegen. Viele Linux-Distributionen bringen eine kompatible Implementierung als Avahi-Daemon mit. Von Apple gibt es entsprechende Dienste auch für Windows – das ist dort vor allem dann nützlich, wenn man Windows mit Apple-Geräten und -Software benutzen will, sprich iTunes, iPhones und iPads, aber auch Time Machine oder Airport.

Bonjour unter Windows ist aber nicht nur dann nützlich: Auf Wunsch annonciert der Dienst auch SMB-Freigaben auf Windows-Maschinen; die Software ist im Bonjour-SDK für Windows enthalten (siehe Downloads), das man mit einer Apple-ID herunterladen kann. Die frei zugänglichen „Bonjour Services for Windows“ hingegen helfen, zielgerichtet einen passenden (Windows-)Treiber für Drucker zu finden, die sich im Netz per Bonjour zu erkennen geben.

Dateien austauschen

Die am weitesten verbreitete Technik, um auf Dateien auf anderen Rechnern im lokalen Netz zuzugreifen, ist ein Protokoll mit dem Namen Server Message Block (**SMB**), das auch als Common Internet Filesystem (**CIFS**) bekannt ist. Ursprünglich stammt es aus der IBM/Microsoft-Welt, weswegen jedes Windows ohne Weiteres im Netz auf die SMB-Freigaben anderer Rechner zugreifen kann.

Die überwiegende Zahl von NAS-Geräten benutzt die freie SMB-Implementierung Samba, um Dateien anzubieten. Auch Mac OS X hat das Protokoll gelernt. Ebenso wie aktuelle Windows-Versionen setzt sich mehr und mehr das grundlegend überarbeitete SMB2 durch. Es wirft viele Altlasten über Bord und ist in vielerlei Hinsicht heutigen Anforderungen besser gewachsen.

In der Apple-Welt ist nach wie vor auch das Apple-eigene **AFP** (Apple Filesharing Protocol) gefragt: Unbedingt empfehlenswert ist es, wenn Macs übers Netz Backups per Time Machine auf einem Server abladen sollen. Das geht je nach Version auch mit



Ein WINS-Server kann die Namensauflösung in Windows-Netzen ohne Active Directory/DNS beschleunigen, muss aber auf allen Systemen bekannt sein.

einem SMB-Server, ist dort wegen fehlender Funktionen aber deutlich riskanter.

In der PC-Welt eher ungebrauchlich ist das aus der Unix-Welt stammende Network File System (**NFS**). An Benutzerkonten ausgerichtete Authentifizierung sieht es nicht vor, sondern vertraut als zugriffsberechtigt erklärten Systemen vollständig.

Für den Dateizugriff besonders auf entfernte Systeme kommen auch noch **FTP** (File Transfer Protocol) und **WebDAV** (Web-based Distributed Authoring and Versioning) in Betracht. Als Alternative für den Zugriff auf Dateien im lokalen Netz sind sie schlecht geeignet.

Drucken

Beim Drucken im Netzwerk begegnet einem wieder **SMB**. Das Protokoll kennt spezielle Funktionen zum Übermitteln von Druckdaten. Außerdem benutzen Windows-Clients und -Server zahlreiche Remote Procedure Calls (RPCs), um sich über Details der Auftragsbearbeitung und die Bestückung mit passenden Treibern abzustimmen (Windows-PCs laden passende Treiber automatisch von dem Server, der den Drucker bereitstellt).

Während SMB-Druckdienste nur dann gebräuchlich sind, wenn auf beiden Seiten Windows aktiv ist, funktionieren das Line Printer Daemon Protocol (**LPD**), JetDirect und das Internet Printing Protocol herstellerübergreifend: LPD-fähige Drucker heißen oft

auch TCP/IP-Printer; die Clients werden auch als LPR-Clients bezeichnet.

Sie nehmen direkt Druckjobs an und kennen keine ausklügelte Technik, um Treiber hin- und herzuschieben. Das heißt, die Daten sind in einem für den Drucker verständlichen Format anzuliefern, auf dem Client muss also ein zum Drucker passender Treiber aktiv sein. Ähnlich arbeitet das von HP erfundene **JetDirect**. LPD und JetDirect bringen Funktionen für die Behandlung mehrerer Jobs in Warteschlangen (**Queues**) mit.

Ähnlich weit verbreitet ist inzwischen das Internet Printing Protocol (**IPP**). Es benutzt HTTP oder HTTPS zum Transport sowohl für die Druck- als auch für die Verwaltungsdaten. Je nach Plattform unterscheiden sich die verwendeten URLs für den Zugriff auf einen konkreten Drucker subtil. Mancherorts heißt es `ipp://server/printers/drucker`, andernorts steht `http` davor. Gemeint ist das Gleiche.

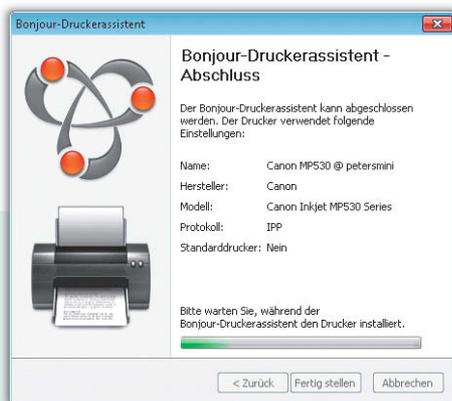
Gängige IPP-Implementierungen in Mac OS und Unix (CUPS) bieten mehr als nur reine Verwaltungsfunktionen; unter anderem erkennen sie oft die Beschaffenheit eingehender Druckdaten und können sie geeignet für den angeschlossenen Drucker ausgeben – das heißt, das dort zwischen Ein- und Ausgang eine leistungsfähige Softwareschicht vermittelt und auf der Client-Seite womöglich ein generischer, meist PostScript-Treiber genügt. Das kann man geschickt ausnutzen, um fehlende Treiber zu kompensieren.



Der Finder in Mac OS X erlaubt per „Mit Server verbinden“ die Kontaktaufnahme mit Netzwerklaufwerken verschiedenster Couleur in sehr eingängiger Weise.



Apples Bonjour hilft, auf Windows installiert, auch bei der Druckertreiberinstallation.



Namensdienste

	Linux	Mac OS X	Windows
NetBIOS/Broadcast	✓	✓	✓
DNS	✓	✓	✓
WINS	✓	✓	✓
Bonjour	✓	✓	-
PNRP	-	-	✓

Streamen

Für das Ausliefern von Audiodateien im lokalen Netz haben sich zwei Standards etabliert. In der Apple-Welt ist das Digital Audio Access Protocol (**DAAP**) verbreitet, das Apple mit iTunes eingeführt hat und das inzwischen in diversen Geräten anzutreffen ist. Voraussetzung dafür ist in der Regel ein funktionierender Bonjour-Protokollstack. Ergänzt wird es durch die **AirPlay**-Schnittstelle, die sich der drahtlosen Übertragung widmet.

In letzter Zeit tauchen auch Miracast und Google Chromecast als Streaming-Helfer auf. Aber noch verwendet die übrige Welt Audio-Video-Erweiterungen des Universal Plug and Play Protocol (**UPnP AV**). UPnP-AV-Geräte zielt oft auch das **DLNA**-Logo. Das steht für die Digital Home Working Group, eine von Sony und Intel ins Leben gerufene Non-Profit-Organisation, der inzwischen nahezu alle Unterhaltungstechnikanbieter angehören. Sie kümmert sich um die Standardisierung und die Kompatibilität der Geräte.

DLNA ist deutlich weiter gefasst als nur Streamen von Audio- und Videodaten: Die Zertifizierung kann sich auf alle Arten von beteiligten Geräten beziehen, Speicher wie NAS, Medien-Spielgeräte wie Mobile-Player oder TV-Geräte und sogar Drucker – letztlich alles, was man als Heimnetz- oder mobiles Gerät einordnen kann. Auf gängigen NAS-Boxen findet man DAAP- und DLNA-Server friedlich nebeneinander vereint. Auch gibt es Windows-Clients mit DAAP-Funktionen und umgekehrt, Mac- und iPhone-Clients mit DLNA-Funktionen.

Dateizugriffe

	Linux	Mac OS X	Windows	Windows Server
SMB	S/C	S/C	S/C	S/C
NFS	S/C	S ¹ /C	-	S/-
WebDAV	S/C	-/C	-/C	S/C

S=Server/C=Client, ¹ Verwaltungssoftware fehlt

Terminaldienste

Bleiben die Dienste übrig, um entfernte Geräte zu steuern. Insbesondere für administrative Zugriffe auf entfernte Geräte gilt in Unix/Linux-Kreisen **SSH** (Secure Shell) als das Mittel der Wahl. Der Zugang auf die Kommandozeile entfernter Systeme ist verschlüsselt und für die Authentifizierung können statt Passwörtern private und öffentliche Schlüssel zum Einsatz kommen.

SSH erleichtert das Aufbauen von Tunneln, sodass man über eine SSH-Verbindung auch grafische Anwendungen fernbedienen kann. Darüber hinaus taugt SSH noch für eine ganze Reihe weiterer Dinge, etwa um Daten von einem auf den anderen Server zu sichern, um regelmäßig Daten auf einem entfernten System abzufragen und so weiter. Das steinalte, unverschlüsselte und weniger universelle **Telnet**-Protokoll sollte man nur ausnahmsweise in vertrauenswürdigem Netzen verwenden.

Für die Fernsteuerung von Windows hat sich das Remote-Desktop-Protokoll (**RDP**) etabliert. Alle „besseren“ Windows-Versionen, also nicht die Home-Ausgaben, enthalten einen RDP-Server, lassen sich also übers Netz bedienen. RDP ist auf Komfort und Geschwindigkeit ausgelegt. Dateiaustausch, Drucken, Audioausgabe und Copy&Paste zwischen lokalem und ferngesteuertem PC sind für heutige RDP-Clients und -Server selbstverständlich.

Aber nicht nur Windows-Clients beherrschen dieses Protokoll. Im Windows-Server lässt sich der Dienst einerseits zum Administrieren übers Netz einsetzen, andererseits aber auch in einen Applikationsmodus schalten, in dem der Server dann als sogenannter **Terminal-Server** viele Benutzer parallel mit einer Windows-Sitzung oder auf Wunsch auch einzelnen Applikationen versorgt.

Weniger ausgefeilt, dafür aber auf nahezu allen gängigen Betriebssystemen zu haben ist **VNC**. Die ursprünglich als Virtual Network Computing entwickelte Software erlaubt ebenfalls die Fernsteuerung eines entfernten

Rechners und gilt heute als plattformunabhängig. Anders als RDP etwa „kapert“ VNC normalerweise die Systemkonsole – das heißt, man sieht lokal die entfernt ausgeführten Bedienschritte und es gibt kein Session-Management.

Apple greift für die Bildschirmfreigaben, also die Fernsteuerung von Mac OS X auf das VNC-Protokoll zurück, ergänzt es aber um Verschlüsselung, Copy&Paste und Session-Management.

Identitätskreise

Während es für die meisten Dienste und Protokolle im Netz Alternativen gibt, scheint für eine Aufgabenstellung weitgehend Einigkeit zu herrschen: Die Daten für geräteübergreifende Identitätsdienste, etwa Benutzernamen, Kennwörter, Gruppen und so weiter fragt man mit **LDAP** ab (Lightweight Directory Access Protocol). Das Protokoll erlaubt auch schreibende Zugriffe, die in der Regel von spezieller Management-Software aus erfolgen, ist aber fürs schnelle Lesen und Durchsuchen der darunter liegenden Datenbank optimiert.

Implementierungen gibt es eine ganze Reihe: Apples Open Directory für die Apple-Welt, Microsofts Active Directory für Windows und diverse auf OpenLDAP aufbauende Implementierungen. Sowohl Apple als auch Microsoft verheiraten ihrerseits den LDAP-Verzeichnisdienst mit **Kerberos** für die Authentifizierung im Netz. Dieser Dienst stellt Benutzern Tickets aus, die sie bei Zugriffen auf Netzwerkressourcen vorweisen müssen. (ps)

Fernsteuerung

	Linux	Mac OS X	Windows
SSH	C/S	C/S	-/-
RDP	C/-	-/-	C/S
VNC	C/S	C/S	-/-

S=Server/C=Client

Sofortige und sichere Fernwartung

Unabhängig von der Plattform, unabhängig vom Standort



Jetzt mit Fernsteuerung von MAC und mobilen Geräten



NetSupport Manager Remote Control für jede Plattform



Weitere Informationen:



Sofortige und sichere Fernwartung

Unabhängig von der Plattform, unabhängig vom Standort

NetSupport Manager Remote-Control-Software, mit umfassender Multi-Plattform-Unterstützung für Windows®, Linux, Mac® und mobile Geräte, kombiniert mit fortschrittlicher System-Management-Funktionalität, bietet seit über 23 Jahren Helpdesk-Profis die Leistungsfähigkeit, um den täglichen Supportanforderungen gerecht zu werden.

Die neuen NetSupport Controls für Mac und mobile Geräte bieten Ihnen die Möglichkeit, per Fernzugriff auf Ihre Unternehmenssysteme- und Server eine Verbindung von einem Apple Mac oder einem iOS- oder Android-Tablet und Smartphone herzustellen. Dadurch erhalten Sie noch mehr Flexibilität zur Unterstützung Ihrer Anwender vom Hauptsitz aus oder von unterwegs.

Erfahren Sie mehr und laden Sie sich eine kostenlose 30-Tage-Testversion herunter:
www.netsupportmanager.com



Reiko Kaps

Kostenlose DynDNS-Dienste



www.ct.de/cs1304014

An den meisten privaten Internetanschlüssen bekommen Router keine festen IP-Adressen. Deshalb hat sich der Dienstleister Dyn.com vor Jahren etabliert: Darüber lässt sich für wechselnde IP-Adressen ein leicht zu merkender Hostname registrieren, über den man unterwegs ohne Weiteres auf sein LAN zugreifen kann. Doch Dyn.com hat sein Angebot inzwischen stark eingeschränkt – Alternativen sind gefragt.

Einen richtigen Domainnamen bekommen normalerweise nur solche Internet-Stationen, die über eine feste öffentliche IP-Adresse angesprochen werden – das ist praktisch, denn so muss man sich nicht die IP-Adresse eines Webservers merken (z. B. 193.99.144.80), sondern nur heise.de.

Eine solche Adress-zu-Namen-Umsetzung ist natürlich auch für den privaten Bereich

nützlich, etwa damit die Tochter für die Fernwartung von Papis PC nicht jedes Mal vorher die IP-Adresse per Telefon erfragen muss – private DSL-Anschlüsse erhalten meist keine festen IP-Adressen, sondern spätestens nach jeder Einwahl eine neue.

Das weltweite Domain Name System, in dem auch heise.de eingetragen ist, ist aber nicht für schnelle Änderungen von IP-Adressen ausgelegt; DNS-Einträge müssen

zwecks Ressourcenersparnis Stunden bis Tage gültig sein. Für Anschlüsse mit wechselnden IP-Adressen hat man daher später eigens das dynamische Domain Name System eingeführt (DDNS), bei dem sich IP-Adressen einträge umgehend aktualisieren lassen.

Dienstleister wie Dyn.com haben dafür eine übers Webinterface zugängliche Schnittstelle geschaffen: Teilnehmer tragen dort über einen Browser eine IP-Adresse zu

Der bei D-Link angelegte Dyn-Account lässt sich um einen weiteren DynDNS-Eintrag erweitern, wenn man sich direkt bei Dyn anmeldet.

einem Hostnamen ein und der Anbieter füttert damit das DDNS (gemäß RFC-Spezifikation 2136). Mit etwas Know-how lässt sich ein solcher Dienst auf beliebigen Root-Servern einrichten, sodass es weltweit eine Menge DynDNS-Anbieter gibt. Damit man die Adressänderungen automatisch übermitteln kann, haben sie Update-Verfahren spezifiziert und viele bieten auch eigene Client-Programme, die auf Teilnehmer-PCs laufen. Bei modernen Routern gehört ein solcher Client mittlerweile ebenfalls zum Pflichtenheft.

Nach der Anmeldung bei einem solchen Anbieter wählen Sie aus dem Vorrat an Domains, die der DynDNS-Anbieter für diesen Zweck registriert hat, eine aus (zum Beispiel homeunix.net oder it.cx), tragen in die Maske einen beliebigen Hostnamen ein (zum Beispiel opaspc) und ordnen ihm die öffentliche IPv4-Adresse des Routers zu – fertig. Nun können Sie Ihren Internet-Anschluss aus dem Internet über die registrierte Domain erreichen (z. B. opaspc.it.cx). Um auf Dienste hinter dem Router zuzugreifen, etwa um einen PC aus der Ferne zu warten, müssen Sie im Router nur noch eine Port-Weiterleitung für den jeweiligen Dienst eintragen.

Für viele Nutzer genügt ein einziger Hostname und bei den meisten DynDNS-Anbietern lassen sich im Rahmen von Gratisangeboten sogar mehrere registrieren. Das war auch jahrelang beim Platzhirsch Dyn.com der Fall, früher unter dem branchenprägenden Namen DynDNS bekannt. Deshalb sind heute die meisten Router, aber auch Webcams oder NAS-Speicher auf dessen Dienst spezialisiert.

Dyn.com hat sein Gratisangebot aber im Laufe der letzten Jahre stark beschnitten. Inzwischen gibt es kostenlose Dienste nur während einer 30-tägigen Testphase. Für viele Interessenten kommt Dyn.com nicht

mehr infrage. Wir haben daher aus der Vielzahl an DynDNS-Angeboten exemplarisch einige herausgegriffen, die grundlegende DynDNS-Dienste gratis anbieten. Zu den gängigen Anbietern zählen No-IP und TwoDNS. Freedns.afraid.org und dtDNS berücksichtigen wir, weil sie zahlreiche Spezialoptionen anbieten. Die dritte Gruppe bilden Dienste, die Routerhersteller implementieren oder die zu Webhosting-Paketen gehören. Wir zeigen deren Vorzüge und Nachteile und erklären auch, wie man sie nutzt, wenn Geräte nicht dafür ausgelegt sind.

DynDNS-Dienst für zu Hause

Die DynDNS-Angebote umfassen meist eine Fülle von Funktionen, je nach Dienst kosten einige davon allerdings Gebühren – wenn auch nur wenige Euro im Jahr. Je nach Anbieter zählen dazu etwa Einträge für Mailserver (MX), Wildcard-Namen, DynDNS-Einträge für IPv6-Adressen (AAAA) oder auch CNAME-Einträge. Das sind Alias-Einträge, die auf DNS-Einträge verweisen. So lassen sich etwa mehrere virtuelle Hosts auf einem Webserver mit nur einer IP-Adresse betreiben. Die Gratisangebote erstrecken sich meist auf ein bis fünf frei wählbare Hostnamen für IPv4-Adressen – Domainnamen gibt dabei der Anbieter vor.

Läuft der eigene Internet-Anschluss zu Hause nur mit IPv4, genügt bereits ein einziger DynDNS-Name: Der Router reicht aus dem Internet eingehende Anfrage an die hinter ihm laufenden Geräte und Dienste bei IPv4 immer per Port-Weiterleitung weiter, aus dem Internet ruft man dabei immer nur die eine externe Adresse des Routers auf. IPv6 wird jedoch zunehmend wichtiger, denn dabei bekommen alle hinter dem Router laufenden Netzwerkgeräte auch eigene, im Internet gültige IPv6-Adressen. Will man also den eigenen PC, das NAS und die

Webcam per DynDNS im Internet bekannt machen, muss man beim DynDNS-Anbieter bereits drei Hostnamen dafür vorsehen.

Adressen aktualisieren

Adressen kann man per Hand im Web-Interface des DynDNS-Dienstes aktualisieren. Weil das auf Dauer umständlich ist, gibt es Update-Programme, die die Aufgabe automatisch bewältigen. Dazu zählen etwa ddclient, das unter Linux und Unixen läuft, oder das Windows-Programm „DynDNS Simply Client“. Einige Dienste bieten auch eigene Clients an (siehe Downloads).

Diese Programme ermitteln periodisch, ob sich die externe, öffentliche IPv4-Adresse des Internetanschlusses geändert hat. Trifft das zu, senden sie die neue Adresse an den Dienst und werten dessen Antwort aus. Es dauert dann etwa eine Minute, bis der DynDNS-Eintrag aktualisiert ist. Das ist recht komfortabel, funktioniert so aber nur auf Macs, Windows- oder Linux-PCs.

Viele Dienste aktualisieren die DynDNS-Informationen auch über ein Web-API. Diese Schnittstelle lässt sich durch Kommandozeilenprogramme wie wget oder curl aus Skripten heraus ansprechen (siehe Downloads).

Bei Fritz!Boxen und auch einigen D-Link-Routern lässt sich aus den Angaben des Web-API zudem ein Freifeld füllen, sodass der Router auch DynDNS-Dienste bedienen kann, für die er eigentlich nicht vorbereitet war.

DynDNS-Helfer

Will man vom DynDNS-Urgestein Dyn.com zu einem anderen Anbieter wechseln, ist es bei Diensten, auf die unbekannte Nutzer zugreifen, nützlich, wenn man beide zumindest für eine Übergangszeit parallel betreiben kann. Auf PCs ist das kein Problem – die

Der DynDNS-Dienst Afraid.org verknüpft kostenlos sogar IPv6-Adressen mit einem DNS-Namen.

Editing mynova.chickenkiller.com

Type: AAAA explanation

Subdomain: mynova

Domain: chickenkiller.com (public)

Destination: 2001:06f8:090a:0001:0000:0000:00 Forward to a URL

TTL: For our premium suppl seconds (optional)

Wildcard: Enabled for all subscribers (more info)

Save!

Clients oder Skripte müssen einfach beide laufen. Auf Routern oder Netzwerkspeichern lässt sich jedoch nur ein DynDNS-Anbieter einstellen: Deshalb aktualisiert man das zweite DynDNS-Konto anfangs am besten per PC. Das empfiehlt sich auch dann, wenn die billige IP-Webcam nur mit einem einzigen DynDNS-Anbieter kooperiert und einen eigenen, vom Router abweichenden DynDNS-Namen braucht. Für Server mit IPv6-Adressen sollte der Update-Client ohnehin auf dem jeweiligen Gerät laufen, denn den hinteren Teil der IPv6-Adresse ermitteln die Geräte selbst – etwa per Zufallszahl oder aus der MAC-Adresse der Netzwerkkarte.

D-Link-DDNS

Über den Netzwerkausrüster D-Link kann man doch noch an ein kostenloses Dyn.com-Konto gelangen. Unter der Adresse www.dlinkddns.com erhält man nach der Anmel-

dung einen DynDNS-Namen, der sich per Client oder Webbrowser aktualisieren lässt. Mit D-Links DynDNS-Angebot sollten sich dann auch Netzwerkgeräte mit einem DNS-Namen versorgen lassen, die ausschließlich die DynDNS-Dienste von Dyn.com unterstützen.

Dyn

Wenn Sie sich mit dem über D-Link eingerichteten, kostenlosen Account bei Dyn anmelden, können Sie sogar einen weiteren DynDNS-Eintrag anlegen, der sich auf eine von Dyn bereitgestellte Domain (wie dyndns.org) bezieht. Unter dem Menüpunkt „DynDNS Pro/Hosts“ finden Sie dazu den Link „Add New Hostname“ neben „DynDNS Hostnames“, der zum Einrichtungsformular führt. Wählen Sie nun einen Hostnamen und eine Domain aus der Liste sowie den Servicetyp „Host with IP Address“ – zusätzlich zur

IPv4-Adresse nimmt der Dienst hier auch eine IPv6-Adresse entgegen.

Neben den in den Routern verbauten Update-Programmen empfiehlt der Dienst seinen eigenen namens Dyn Updater (Windows, Mac OS) sowie ddclient unter Linux oder das Tool inadyn – für beide erzeugt er auf Wunsch auch passende Konfigurationen. Außerdem können Sie die Einträge bei Dyn auch per URL aktualisieren, Details dazu erklärt der Anbieter auf seiner Webseite.

Afraid.org

Die Webseite des DynDNS-Anbieters Afraid.org kommt in einem schlichten Tabellen-Design daher und wirkt auf den ersten Blick etwas unübersichtlich. Den Link zum Anmeldeformular finden Sie erst am unteren Ende der Startseite unter „Sign up!“ (<https://freedns.afraid.org/signup>). Nach der Anmeldung und dem Abklicken der Bestätigungsnachricht können Sie neue DynDNS-Namen über den Menüpunkt „Subdomains“ einrichten: Mit „Add a new Subdomain“ legt man deren Typ (A, AAAA, CNAME...), den Namen (Subdomain) sowie deren Ziel (Destination) fest. Bei IPv4 (Type A) müssen Sie hier die IP-Adresse des Routers, bei IPv6 (Type AAAA) die feste, global gültige IPv6-Adresse des jeweiligen Geräts eintragen. Den Haken bei Wildcard können Sie weglassen, wenn Sie keinen virtuellen Webserver betreiben möchten.

Hosts/Redirects

Add Host

Manage Hosts

Manage Groups

Download Client

Upgrade to Enhanced

Need Help?

Support Center

Troubleshooting Guide

Dynamic Update Client

Support Ticket

Contact Us

Add a host

Fill out the following fields to configure your host. After you are done click 'Create Host' to add your host.

Own a domain name?
Use your own domain name with our DNS system. [Add](#) or [Register](#) your domain name now or read more for pricing and features.

Hostname Information

Hostname: cte-st zaplo.org

Host Type: DNS Host (A) DNS Host (Round Robin) DNS Alias (CNAME)

Port 80 Redirect Web Redirect AAAA (IPv6)

IP Address: 193.99.145.162

Assign to Group: - No Group - [Configure Groups](#)

Enable Wildcard: Wildcards are a Plus / Enhanced feature. [Upgrade Now!](#)

Accept Mail for your Domain
Let No-IP do the dirty work. Setup [POP](#) or [forwarding](#) for your name.

Mail Options

MX Record MX Priority

Enter the name of your external mail exchangers (mx records) as hostnames not IP addresses.

5

If you would like a more MX records, please upgrade to [No-IP Plus](#) or [Enhanced](#).

Zurücksetzen Update Host

Einige der angezeigten No-IP-Optionen – etwa für IPv6 – lassen sich nur gegen Bezahlung einsetzen.

Das übersichtliche TwoDNS konzentriert sich auf einige DynDNS-Möglichkeiten – IPv6 gehört leider noch nicht dazu.



Die DynDNS-Einträge bei A afraid.org lassen sich über etliche DynDNS-Clients oder über den Aufruf einer URL aktualisieren: Unter dem Menü „Dynamic DNS“ in der Tabelle am Seitenende finden Sie über zwei Links dazu fertige Batch-Skripte für die Kommandozeilen-Tools wget und curl. Dort stehen außerdem deren Download-Adressen. In der FAQ erklärt der Betreiber aber auch, dass die kostenlosen DynDNS-Namen nicht von Googles Suchmaschine gefunden werden.

Dyndnsfree.de

Eigentlich führt der Namen des deutschen DynDNS-Anbieters in die Irre: Der kostenlose Account bei Dyndnsfree.de endet nach 30 Tagen, dauerhafte DynDNS-Zugänge kosten im Jahr knapp 6 Euro. Dyndnsfree spricht dafür durchgängig deutsch und hilft beim eigenen Linux- und Windows-Client, dem Linux-Client

ddclient sowie bei der Einrichtung auf Routern von AVM, D-Link, Lancom und Bintec. Adressen lassen sich aber auch über eine URL aktualisieren, die nach dem Muster `http://user:passwort@dynup.de/nic/update?hostname=DynDNSName&myip=IP-Adresse` aufgebaut ist. Jeder im Account angelegte DynDNS-Name (DynDNS-Domains) bekommt bei Dyndnsfree eigene Zugangsdaten.

MyFritz

Läuft am Internetzugang eine halbwegs aktuelle Fritz!Box, gelangt man über die von AVM bereitgestellte DynDNS-Alternative MyFritz auf sein Gerät. Dazu müssen Sie sich zuerst bei MyFritz anmelden: Öffnen Sie die Fritz!Box-Verwaltungsfläche im Browser über die URL `http://fritz.box`. Im Menü links wählen Sie nun „Internet“ und „MyFritz!“ und aktivieren den Dienst. Besitzen Sie noch kein

Konto, hilft Ihnen die Fritz!Box beim Anlegen. Sie benötigen dafür lediglich ein Passwort und eine gültige E-Mail-Adresse.

Anschließend erreicht man den Router über eine auf `myfritz.net` endende Adresse aus dem Internet. Alternativ kann man sich auf der MyFritz-Webseite anmelden und bekommt dort einen Link zur eigenen Fritz!Box gezeigt.

No-IP.com

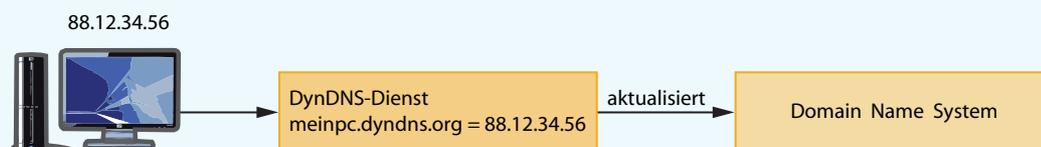
Beim vom US-Unternehmen Vitalwerks betriebenen DynDNS-Dienst No-IP erhält man nach der Anmeldung mit E-Mail-Adresse und Passwort kostenlos maximal drei Hostnamen, die der Dienst mit IPv4-Adressen verknüpft. Falls Sie diese Einträge nicht innerhalb von 30 Tagen aktualisieren, löscht No-IP sie automatisch aus der Datenbank – warnt aber vorher per E-Mail davor.

Dynamisches DNS

Die im Domain Name System abgelegten Zuordnungen zwischen Klartext-Hostnamen und IP-Adressen werden üblicherweise eher selten geändert – schließlich handelt es sich dabei meist um Server oder große Internet-Router. Rechner an klassischen Internetzugängen per DSL oder

Kabel erhalten allerdings fast nie eine feste IP-Adresse, die aber für einen DNS-Eintrag nötig wäre. Abhilfe schafft hier dynamisches DNS (auch DynDNS): Der eigene Rechner meldet seine aktuelle IP-Adresse an einen Dienst, der sie mit einem Hostnamen im DNS verknüpft und möglichst

schnell weltweit bekannt macht. Dank dieses Verfahrens erreicht man den Rechner nun immer über seinen DNS-Namen, das Domain Name System liefert auf Nachfrage die aktuelle IP-Adresse für den Hostnamen zurück, über die Browser und andere Programme dort laufende Dienste finden.



PC am DSL-Anschluss

Der eigene Rechner (oder Router) sendet seine öffentliche IP-Adresse an den DynDNS-Dienst, der sie mit dem Hostnamen verknüpft und im DNS bekannt gibt.

DynDNS-Dienste

Anbieter	Dyn	D-Link	Joshua Anderson	Dyndnsfree	AVM	Vitalwerks	Ingolf Zimmer	dtDNS	Strato	TwoCom
Website	dyn.com	dlinkddns.com	freedns.afraid.org	dyndnsfree.de	myfritz.net	noip.com	dyndns.servermaster.de	www.dtdns.com	strato.de	twodns.de
kostenlos	14 Tage	✓	✓	30 Tage	nur für AVM-Kunden	✓	✓	✓	nur für Strato-Kunden	✓
Hostnamen	32	1 (+1)	5	5	k. A.	3	3	5	k. A.	5
IPv4 / IPv6	✓ / ✓	✓ / ✓	✓ / ✓	✓ / -	✓ / ✓	✓ / -	✓ / -	✓ / -	✓ / -	✓ / -
CNAME	-	-	✓	-	-	✓	-	-	-	-
Wildcards	-	-	-	✓	-	-	✓	✓	-	✓
kostenpflichtig	✓	✓ (Dyn)	✓	✓	- ¹	✓	- ¹	✓	- ¹	-
Hostnamen	32		25	5		25		unbegrenzt		
Laufzeit	1 Jahr		1 Jahr	1 Jahr		1 Jahr		unbegrenzt		
Betrag	20 US-\$		30 US-\$ ¹	5,88 €		15 US-\$		5 US-\$ einmalig		
IPv4 / IPv6	✓ / ✓		✓ / ✓	✓ / -		✓ / ✓		✓ / -		
CNAME			✓	-		✓		-		
Wildcards			✓	-		✓		✓		
Anmelde-Infos	Kreditkarte, E-Mail, Adresse	E-Mail, User-Name	E-Mail	Name, E-Mail	E-Mail	User-Name, E-Mail	Name, Adresse, Festnetz-Nr., E-Mail	Name, Adresse, E-Mail	Angaben zum Hosting-Paket	E-Mail

¹ siehe Text

⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ⊖ sehr schlecht ✓ vorhanden - nicht vorhanden k. A. keine Angabe

Einen neuen DynDNS-Namen legen Sie bei No-IP über den Menüpunkt „Hosts/Redirects“ an: Geben Sie dazu einen Hostnamen wie „meinrouter“ ein, wählen eine der unter „NO-IP Free Domains“ gelisteten Domains sowie einen „Host Type“. Beim kostenlosen Angebot funktionieren „DNS Host (A)“, „DNS Alias (CNAME)“ sowie die Redirects. IPv6-Adressen setzt No-IP nur mit kostenpflichtigen Zugängen in den AAAA-Record eines DNS-Namens ein. Ist der gewünschte Hostname bereits vergeben, weist das Formular nach dem Speichern über „Update Host“ darauf hin.

Diese Adresse lässt sich nun entweder über den von No-IP favorisierten Update-Client oder mittels der über das API bereitgestellten URL-Schemen aktualisieren.

Servermaster.de

Der nach eigenen Aussagen nur über Spenden finanzierte DynDNS-Dienst von Servermaster.de verlangt für die Anmeldung nicht nur den Namen, die E-Mail-Adresse und die vollständige Anschrift. Man muss zusätzliche eine Festnetznummer angeben und zu guter Letzt der Datenspeicherung zustimmen. Während andere Anbieter nur eine Bestätigungsnachricht senden und das Konto meist über einen darin enthaltenen Link aktivieren, ruft ein Servermaster-Mitarbeiter dafür die angegebene Festnetznummer an. Klappt das nicht, klemmt auch die Konto-Freischaltung.

Diese Sammelleidenschaft setzt der Dienst auch bei den DynDNS-Einträgen fort: Neben den technisch notwendigen Angaben will Servermaster.de für jeden Eintrag wissen, welchen Zweck er erfüllen soll, ob Windows, Linux oder ein Router (samt Hersteller und Modell) den Eintrag aktualisieren und ob der Internetzugang täglich zwangsgesrennt wird.

Von allen von uns überprüften Anbietern verlangt Servermaster.de für seine Dienste

die meisten persönlichen Daten, die weit über das übliche oder gar notwendige Maß hinausgehen. Laut Betreiber seien die umfangreichen Angaben aus rechtlichen Gründen unabdingbar und man wolle dem Identitätsbetrug damit vorbeugen.

dtDNS

Auch der US-Anbieter dtDNS verlangt bei der Anmeldung eine vollständige Adresse samt Rufnummer. Beim Validieren nutzt der Dienst aber den üblichen Weg über eine E-Mail sowie einen Aktivierungs-Link. Anschließend lassen sich maximal fünf DynDNS-Namen anlegen und über das Web-Interface bearbeiten – per Vorgabe arbeiten sie als Wildcard.

Alle anderen Funktionen sowie weitere Hostnamen kosten bei dtDNS zwar Geld, aber im Unterschied zu anderen nur eine relativ geringe Einmalgebühr von 5 US-Dollar. Dafür bekommen Sie unbegrenzt viele DynDNS-Namen sowie die Zusatzfunktion „Offline Handler“: Ist die DynDNS-Adresse nicht erreichbar, benachrichtigt dtDNS den Surfer oder leitet die Anfrage auf eine alternative IP-Adresse oder Webseite um.

Strato-Hosting

Als kostenlose Dreingabe lässt sich bei Stratos Webhosting-Angeboten eine DynDNS-Funktion hinzuschalten: Dabei nutzt man den zum Strato-Angebot gehörenden, eigenen Domain-Namen für die DynDNS-Hostnamen. Allerdings müssen Sie den Update-Clients das Masterpasswort des Hosting-Angebots zur Authentifizierung mitgeben, ein eigenes nur für diesen Zweck gültiges lässt sich in der Strato-Oberfläche nicht einrichten.

Stratos DynDNS-Dienst aktualisiert die Adressangaben über das DynDNS-Protokoll, sodass man den Dienst mit vielen kostenlo-

sen Update-Clients und per URL-Aufruf nutzen kann.

TwoDNS.de

Beim in Berlin sitzenden Anbieter TwoDNS erhält man fünf kostenlose DynDNS-Namen: Nach der Anmeldung mit einer E-Mail-Adresse und einem Passwort gelangt man auf eine sehr einfach gehaltene deutsche Verwaltungsoberfläche. Für einen neuen DynDNS-Namen braucht es nur einen selbst vergebenen Hostnamen sowie eine der Domains aus der Liste des Anbieters. Fürs Auffrischen der DynDNS-Einträge setzt TwoDNS auf ein auch per HTTPS erreichbares Web-API. Darüber können Sie nicht nur die Adresse aktualisieren, sondern auch neue DynDNS-Einträge anlegen. Wie das funktioniert, beschreibt der Betreiber ausführlich auf seiner Webseite. TwoDNS wirkt sehr übersichtlich und einsteigerfreundlich, leider beherrscht es kein IPv6.

Fazit

Muss man nur IPv4-Adressen mit einem DynDNS-Namen verknüpfen, hat man die Wahl zwischen vielen Anbietern. Deren Angebote ähneln sich zumeist, Unterschiede gibt es nur bei der Hostname-Anzahl. Beim Funktionsumfang sticht das nur englischsprachige Afraid.org heraus, das auch im kostenlosen DynDNS-Angebot IPv6 und viele andere DNS-Eintragstypen unterstützt. Die Funktionsfülle kann aber auch verwirren: Übersichtlicher und mit deutscher Bedienoberfläche bringt TwoDNS selbst Einsteiger schnell zum Ziel. Ähnlich einfach wirkt auch der Konkurrent No-IP – allerdings spricht der Dienst nur Englisch. Muss es unbedingt ein DynDNS-Name von Dyn.com sein, legt man sich bei D-Link ein kostenloses Konto an: Der Netzwerkhersteller greift dabei auf die Dienste von Dyn.com zurück. (rek) **ct**