FRANZIS

MACH'S EINFACH

98 Anleitungen

HEIMNETZWERKE

Fernzugriff auf das Heimnetzwerk mittels VPN • So setzen Sie Ihren eigenen Webserver auf • u. v. m.

STEPHAN BREY

98 Anleitungen

HEIMNETZWERKE

Fernzugriff auf das Heimnetzwerk mittels VPN • So setzen Sie Ihren eigenen Webserver auf • u. v. m.

Der Autor

Stephan Brey ist Informatiker und Webdesigner und lebt in München. Er ist Spezialist für Off- und Online-Anwendungen, insbesondere Content-Management-Systeme wie Wordpress und Joomla sowie Onlineshop-Anwendungen. Der Fachbuchautor hat im FRANZIS Verlag bereits einige Fachbücher zu den Themen SEO und CMS veröffentlicht.

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über *http://dnb.ddb.de* abrufbar.

Lektorat: Ulrich Dorn
Satz: PC-DTP-Satz und Informations GmbH, Alexandra Kugge, München

Covergestaltung: Julia Harrer
ISBN: 978-3-645-20671-6
eISBN: 978-3-645-22481-9

Wie funktioniert das Buch?

Das Buch beschreibt das Einrichten von kleinen Netzwerken für zu Hause oder im eigenen Büro. Grundsätzlich gehen wir von den gängigsten Betriebssystemen und den am häufigsten verwendeten Routern aus, die von den drei größten Internetdienstanbietern bereitgestellt werden. Konkret sind das die Telekom, Vodafone sowie 1&1. Vodafone und 1&1 haben als Standardrouter die FRITZ!Box 6490 und die FRITZ!Box 7590. Die Telekom bietet seit langer Zeit den Router Speedport W724V an. Es sind auch andere Versionen des Speedport-Routers erhältlich, aber alle lassen sich auf gleiche Weise konfigurieren. Das Modell spielt daher nur eine untergeordnete Rolle.

Die Betriebssystemversionen der FRITZ!Box und der Speedports waren beim Erstellen dieses Buchs aktuell.

Wichtige Hinweise, Informationen, Links zu Downloads etc. befinden sich immer am Ende einer Beschreibung in einem umrandeten Kasten.

Wir glauben, dass das Buch Ihnen auch bei komplexeren Themen mit Rat und Hilfe zur Seite stehen wird.

Viel Freude beim Lesen.

Stephan Brey

Dieses Buch ist meinen Kindern Janosch, Felix und Leonie
sowie
meinen Geschwistern Andreas und Martina gewidmet.

Inhalt

3 Das Heimnetz ganz ohne Kabel

4 Internetnutzung einschränken

5 Netzwerk- und Hacking-Tools

6 Einen eigenen Webserver

aufsetzen

7 Fernzugriff auf das Netzwerk

8 Virtuelle Computer im Netzwerk verwalten

9 Netzwerkprobleme und

Lösungen unter Windows

10 Windows-Tipps und -Tricks

11 Glossar

Was genau ist ein Netzwerk?

1 Verbund netzwerkfähiger Geräte

Als Netzwerk bezeichnet man den Verbund mehrerer Computer, Computergruppen oder anderer netzwerkfähiger Geräte zum Zweck der Datenkommunikation; dazu gehören etwa Drucker, Smartphones, Tablets, Fernseher und andere.

- Netzwerke verbinden verschiedene Computer oder Systeme miteinander, um einen Datenaustausch zwischen diesen Rechnern möglich zu machen.

- Computernetzwerke haben nicht nur den Vorteil, dass mehrere Rechner Informationen austauschen können, ein Netzwerk ermöglicht auch das gemeinsame Nutzen von Ressourcen – alle Computer eines Netzwerks verwenden z. B. denselben Internetzugang oder greifen auf denselben Drucker zu.

- Ein weiterer Vorteil liegt darin, dass eine Kommunikation zwischen verschiedenen Rechnern auch auf eine große räumliche Entfernung möglich ist. So können beispielsweise zwei Standorte einer Firma in Deutschland systemtechnisch miteinander verbunden sein.

- In Computernetzwerken haben die einzelnen Rechner oft unterschiedliche Aufgaben. Es gibt zentrale Computer in einem Netzwerk, die anderen Computern ihre Dienste anbieten. Sie heißen Server (engl. to serve = bedienen). Die Rechner in einem Netzwerk, die auf die Daten der Server zugreifen, sich also deren Dienste bedienen, nennt man Clients (zu Deutsch Kunde).

- Netzwerke können nach der räumlichen Ausdehnung, also ihrer Größe, unterschieden werden:

  Das PAN (*Personal Area Network*) hat eine Größe von etwa 10 Metern und bezeichnet die Vernetzung von Geräten im direkten persönlichen Umfeld, z. B. das Heimnetzwerk im Wohnzimmer oder die Verbindung von PDA und Rechner.

  Das LAN (*Local Area Network*) hat eine Ausdehnung von bis zu 900 Metern und wird meistens in Unternehmen eingesetzt.

  Das MAN (*Metropolitan Area Network*) umfasst bis zu 60 Kilometer. Das MAN ist ein Stadt- bzw. Regionalnetz.

  Das WAN (*Wide Area Network*) ist das Weitverkehrsnetz, es ist für weite Strecken konzipiert und erstreckt sich über Länder wie Kontinente.

- Netzwerke werden auch nach Art der Leitungsführung (Topologie), nach Art der Übertragung und nach Übertragungsgeschwindigkeit unterschieden.

Zum Buch!

Seien wir ehrlich: Im Grunde ist es heutzutage ein Kinderspiel, eine Internet- bzw. Netzwerkverbindung

mithilfe eines Routers wie der FRITZ!Box oder des Speedports herzustellen.

Die Geräte werden meist vorkonfiguriert verschickt, und in der Regel genügt das Anstöpseln der Kabel an den PC oder das Anklicken des WLAN-Symbols, und schon hat man seine Internetverbindung. Diesen Vorgang übergehen wir einfach und konzentrieren uns auf andere Aspekte eines kleinen Heimnetzwerks. Das Verbinden mehrerer Computer oder mobiler Geräte ist da weitaus spannender. Genau das wird in diesem Buch beschrieben. In einem Heimnetzwerk können alle Geräte miteinander sprechen und Daten austauschen. Das spart Zeit und Arbeit. Die Einrichtung ist relativ einfach.

2 Die wichtigsten Netzwerktypen

Unter einem Netzwerk versteht man eine beliebige Anzahl selbstständiger Computersysteme, die so miteinander verbunden sind, dass ein Datenaustausch möglich wird. Dazu muss neben einer physischen auch eine logische Verbindung der zu vernetzenden Systeme vorhanden sein. Letztere wird durch spezielle Netzwerkprotokolle wie TCP (*Transmission Control Protocol*) hergestellt. Bereits zwei miteinander verbundene Rechner können als Netzwerk betrachtet werden.

Netzwerke werden mit dem Ziel eingerichtet, Daten von einem System auf ein anderes zu übertragen oder gemeinsame Ressourcen wie Server, Datenbanken oder Drucker im Netzwerk zur Verfügung zu stellen. Je nach Größe und Reichweite des Rechnerverbunds werden

verschiedene Netzwerkdimensionen unterschieden. Zu den wichtigsten Netzwerktypen gehören:

- Personal Area Networks (PAN)
- Local Area Networks (LAN)
- Metropolitan Area Networks (MAN)
- Wide Area Networks (WAN)
- Global Area Networks (GAN)

Die physische Verbindung, die diesen Netzwerktypen zugrunde liegt, kann kabelgebunden oder auf Basis von Funktechnik realisiert werden. Oft stellen physische Kommunikationsnetze die Grundlage für mehrere logische Kommunikationsnetze, sogenannte *Virtual Private Networks* (VPN). Diese nutzen bei der Datenübertragung zwar ein gemeinsames physisches Übertragungsmedium, beispielsweise ein Glasfaserkabel, werden mittels Tunneling-Software jedoch logisch unterschiedlichen virtuellen Netzen zugeordnet.

Jeder Netzwerktyp wurde für spezielle Anwendungsbereiche entwickelt, beruht auf jeweils eigenen Techniken und Standards und bringt somit unterschiedliche Vorteile und Beschränkungen mit sich.

Personal Area Network (PAN)

Um einen Datenaustausch zu ermöglichen, lassen sich moderne Endgeräte wie Smartphones, Tablets, Laptops und Desktopcomputer ad hoc zu einem Netzwerk zusammenschließen. Das kann kabelgebunden in Form eines *Personal Area Network* (PAN) erfolgen. Übliche Übertragungstechniken sind USB und FireWire. Die kabellose

Variante, *Wireless Personal Area Network* (WPAN), stützt sich auf Techniken wie Bluetooth, Wireless USB, Insteon, IrDA, Zig-Bee oder Z-Wave. Ein kabelloses Personal Area Network, das via Bluetooth zustande kommt, wird Piconet genannt. PANs und WPANs erstrecken sich in der Regel nur über wenige Meter und eignen sich somit nicht dazu, Geräte in unterschiedlichen Räumen oder gar Gebäuden zu verbinden.

Neben der Kommunikation einzelner Endgeräte untereinander ermöglicht ein Personal Area Network den Verbindungsaufbau zu anderen, in der Regel größeren Netzwerken. Man spricht in diesem Fall von einem Uplink. Aufgrund der begrenzten Reichweite und einer vergleichsweise niedrigen Datenübertragungsrate kommen PANs in erster Linie zum Einsatz, um Peripheriegeräte im Hobby- und Entertainment-Bereich zu verbinden. Typische Beispiele sind kabellose Kopfhörer, Spielekonsolen und Digitalkameras. Im Rahmen des *Internet of Things* (IoT) dienen WPANs der Kommunikation von Kontroll- und Monitoring-Anwendungen mit niedriger Datenrate. Protokolle wie Insteon, Z-Wave und ZigBee wurden speziell für Smart Homes und Heimautomation entworfen.

Local Area Network (LAN)

Sollen mehrere Rechner zu einem Verbund zusammengeschlossen werden, erfolgt dies meist in Form eines *Lokal Area Network* (LAN). Ein solches Ortsnetz kann zwei Rechner in einem privaten Haushalt umfassen oder mehrere Tausend Geräte in einem Unternehmen. Auch Netzwerke in öffentlichen Einrichtungen wie Behörden, Schulen oder Universitäten werden als LAN realisiert. Ein weitverbreiteter Standard für kabelgebundene Local Area Networks ist Ethernet. Weniger gebräuchlich und weitgehend veraltet sind Vernetzungstechnologien wie

ARCNET, FDDI und Token Ring. Die Datenübertragung erfolgt entweder elektronisch auf Basis von Kupferkabeln oder über einen Lichtwellenleiter aus Glasfaser.

Werden mehr als zwei Rechner in einem LAN zusammengeschlossen, sind weitere Netzwerkkomponenten wie Hubs, Bridges und Switches erforderlich, die als Kopplungselemente und Verteilerknoten fungieren. Der Netzwerktyp LAN wurde entwickelt, um eine schnelle Übertragung großer Datenmengen zu ermöglichen. Abhängig vom Aufbau des Netzwerks und des verwendeten Übertragungsmediums ist ein Datendurchsatz von 10 bis 1.000 MBit/s üblich. LANs erlauben einen komfortablen Informationsaustausch zwischen den verschiedenen im Netzwerk verbundenen Geräten. Im Unternehmenskontext ist es üblich, mehreren Arbeitscomputern gemeinsame Fileserver, Netzwerkdrucker oder Anwendungen über LAN zur Verfügung zu stellen.

Wird ein lokales Netzwerk über Funk realisiert, spricht man von einem *Wireless Local Area Network* (WLAN). Die technischen Grundlagen des WLAN-Standards werden durch die Normenfamilie IEEE 802.11 definiert. Kabellose lokale Netzwerke bieten die Möglichkeit, Endgeräte bequem in ein Heim- oder Unternehmensnetz einzubinden, und sind kompatibel zu kabelgebundenen Ethernet-LANs. Der Datendurchsatz ist jedoch geringer als bei einer Ethernet-Verbindung.

Die Reichweite eines LAN ist vom verwendeten Standard und dem Übertragungsmedium abhängig, lässt sich jedoch durch Signalverstärker, sogenannte Repeater, erhöhen. Bei Gigabit-Ethernet über Glasfaser ist eine Signalreichweite von mehreren Kilometern möglich. Local Area Networks erstrecken sich jedoch nur selten über mehr als einen Gebäudekomplex. Mehrere LANs in geografischer Nähe

lassen sich zu einem übergeordneten *Metropolitan Area Network* (MAN) oder *Wide Area Network* (WAN) verbinden.

LAN (Quelle: *https://en.wikipedia.org/w/index.php?curid=7654281*)

Metropolitan Area Network (MAN)

Metropolitan Area Network (MAN) wird ein breitbandiges Telekommunikationsnetz genannt, das mehrere LANs in geografischer Nähe verbindet. In der Regel handelt es sich dabei um einzelne Niederlassungen eines Unternehmens, die über angemietete Standleitungen zu einem MAN zusammengeschlossen werden. Dabei kommen leistungsstarke Router und Hochleistungsverbindungen auf Basis von Glasfaser zum Einsatz, die einen deutlich höheren Datendurchsatz ermöglichen als das Internet. Die Übertragungsgeschwindigkeit zwischen zwei entfernten Knotenpunkten ist mit der Kommunikation innerhalb eines LAN vergleichbar.

Die Infrastruktur für MANs wird von international agierenden Netzwerkbetreibern zur Verfügung gestellt. Als Metropolitan Area Network verkabelte Städte lassen sich überregional in *Wide Area Networks* (WAN) und international in *Global Area Networks* (GAN) einbinden.

Mit Metro-Ethernet steht für MANs eine spezielle Übertragungstechnik zur Verfügung, mit der sich leistungsstarke *Metro-Ethernet-Netze* (MEN) auf Basis von *Carrier-Ethernet* (CE 1.0) oder *Carrier-Ethernet 2.0* (CE 2.0) aufbauen lassen.

Ein Standard für größere regionale Funknetze, sogenannte *Wireless Metropolitan Area Networks* (WMAN), wurde mit IEEE 802.16 entwickelt. Die als WiMAX (*Worldwide Interoperability for Microwave Access*) bekannte Technologie

ermöglicht es, sogenannte WLAN-Hotzones einzurichten. Dabei handelt es sich um mehrere im Verbund arbeitende WLAN-Zugriffspunkte an verschiedenen Standpunkten. In Deutschland kommen WMANs zum Einsatz, um Endkunden in Regionen mit fehlender Infrastruktur eine leistungsstarke Anbindung an das Internet zu bieten. Der geläufige Übertragungsstandard DSL ist technisch bedingt nur da verfügbar, wo Kupferkabel verlegt wurden.

Wide Area Network (WAN)

Während Metropolitan Area Networks nah beieinanderliegende Standpunkte in ländlichen Regionen oder Ballungsgebieten verbinden, erstrecken sich Weitverkehrsnetze, sogenannte *Wide Area Networks* (WAN), über große geografische Bereiche wie Länder oder Kontinente. Die Anzahl der in einem WAN verbundenen lokalen Netzwerke oder Einzelrechner ist prinzipiell unbegrenzt.

Während LANs und MANs aufgrund der geografischen Nähe der zu verbindenden Rechner oder Netzwerke auf Basis von Ethernet realisiert werden können, kommen bei Weitverkehrsnetzen Techniken wie IP/MPLS (*Multiprotocol Label Switching*), PDH (*Plesiochrone Digitale Hierarchie*), SDH (*Synchrone Digitale Hierarchie*), SONET (*Synchronous Optical Network*), ATM (*Asynchronous Transfer Mode*) und selten noch das veraltete X.25 zum Einsatz.

Wide Area Networks sind meist im Besitz einer bestimmten Organisation oder eines Unternehmens und werden privat betrieben oder vermietet. Darüber hinaus nutzen Internetserviceprovider WANs, um lokale Unternehmensnetzwerke und Endkunden an das Internet anzubinden.

WAN (Quelle: *https://commons.wikimedia.org/wiki/File:Gateway_firewall.svg*)

Global Area Network (GAN)

Ein weltumspannendes Netzwerk wie das Internet wird als *Global Area Network* (GAN) bezeichnet. Das Internet ist jedoch nicht der einzige Rechnerverbund dieser Art. Auch international tätige Unternehmen unterhalten abgeschottete Netzwerke, die mehrere WANs umfassen und so Firmenrechner weltweit verbinden. GANs nutzen die Glasfaserinfrastruktur von Weitverkehrsnetzen und schließen diese durch internationale Seekabel oder Satellitenübertragung zusammen.

Virtual Private Network (VPN)

Ein *Virtual Privat Network* (VPN) ist ein virtuelles Kommunikationsnetz, das die Infrastruktur eines physischen Netzwerks nutzt, um Computersysteme logisch zu verbinden. Dabei kann es sich um jeden der oben dargestellten Netzwerktypen handeln. Am gängigsten ist jedoch das Internet als Transportmedium. Es verbindet nahezu alle Rechner weltweit und steht im Gegensatz zu privat betriebenen MANs oder WANs kostenlos zur Verfügung. Der Datentransfer erfolgt innerhalb eines virtuellen Tunnels, der zwischen einem VPN-Client und einem VPN-Server aufgebaut wird.

Kommt das öffentliche Netz als Transportmedium zum Einsatz, werden Virtual Private Networks in der Regel verschlüsselt, um die Vertraulichkeit der Daten sicherzustellen. VPNs kommen zum Einsatz, um LANs über das Internet zu vernetzen oder einen Fernzugriff auf ein Netzwerk oder einen Einzelrechner über die öffentliche Verbindung zu ermöglichen.

VPN (Quelle: *https://privacycanada.net*)

3 Geräteanforderungen im Netzwerk

Ein Heimnetzwerk verbindet netzwerkfähige Geräte und erlaubt es ihnen, untereinander und mit dem Internet zu kommunizieren (ein Internetzugang vorausgesetzt). Heute sind nur Geräte üblich, die entweder WLAN integriert haben oder eine Schnittstelle für kabelgebundenes Ethernet besitzen – oder natürlich beides. Gerade wenn Sie Geräte an Ihr Netzwerk anschließen möchten, die entweder nur WLAN oder nur eine Ethernet-Buchse anbieten, ist dies schon gleich eine Information darüber, welches Übertragungsmedium Sie für welches Gerät brauchen.

Falls beides unterstützt wird oder einfach modular nachgerüstet werden kann, wie z. B. bei einem klassischen PC, wird es von den Benutzern und vor allem ihren Anwendungen abhängen, welches Übertragungsmedium das geeignetere ist. Wenn Sie sehr viele Geräte im Heimnetz eingebunden haben, können Sie den Datentransfer der einzelnen Geräte priorisieren.

Eine Ethernet-Buchse erkennen Sie an der klassischen sogenannten RJ45-Bauform mit acht Kontakten.

Da andere Technologien (wie z. B. ISDN) Buchsen mit gleicher Bauform verwenden, empfiehlt es sich im Zweifel, einen Blick auf die Buchse zu werfen. Bei vielen Geräten ist die Buchse schon mit dem Schriftzug „Ethernet“ gekennzeichnet. Bleibt immer noch Unsicherheit, können Sie über die Dokumentation eines Geräts prüfen, ob es sich um eine Ethernet-Buchse handelt. Allerdings muss hinzugefügt werden, dass ISDN eigentlich keine Wahl mehr ist.

ISDN ist out. Lange lebe DSL!

Neben der Schnittstelle für das Netzwerk ist auch der zukünftige Standort für das Gerät von Interesse. Schon allein wegen des Standorts kann sich WLAN oder kabelgebundenes Ethernet anbieten, da es z. B. aufwendig sein kann, ein neues Kabel zu verlegen, oder Stahlbetondecken die Nutzung von WLAN erschweren.

Neben schon genannten Kriterien ist auch die Anzahl der Geräte wichtig, die über WLAN oder Ethernet betrieben werden sollen. Möchten Sie z. B viele Geräte über Ethernet betreiben, müssen entsprechend viele Ethernet-Anschlüsse zur Verfügung gestellt werden.

Ob Sie ein sogenanntes Virtual Private Network (VPN) einrichten sollten, hängt von Ihrer Anforderung ab – etwa ob von außerhalb Ihres Heims oder Büros vom Internet aus auf eines oder mehrere Ihrer Geräte zugegriffen werden soll.

Auch das Thema Heimautomatisierung (Smart Home) sollten Sie kurz überdenken. Möchte man z. B. eine Türsprechanlage in seinem Heim installieren, kann man auf Systeme zurückgreifen, die über das Heimnetzwerk angebunden werden können. Wie bei der Heimtelefonie

ergibt sich der Vorteil, dass man keine veralteten Vier-Draht-Kabel mehr verlegen muss, sondern ein reguläres Netzwerkkabel, das später flexibel auch für andere Anwendungen genutzt werden kann.

Mögliche Endgeräte im Netzwerk:

- Internetrouter
- Ethernet-Switch
- WLAN-Access-Point
- WLAN-Repeater
- WLAN-Client-Bridge
- WLAN-Client
- PowerLine-Adapter
- Kabel für das Ethernet

FRITZ!SmartHome mit FRITZ!Powerline

Im Bereich der Heimautomatisierung gibt es derzeit eine Vielzahl von konkurrierenden Schnittstellen, vor allem für das Übertragungsmedium Funk. Wir bevorzugen FRITZ!SmartHome mit FRITZ!Powerline. Warum? Weil es im Kontext mit der FRITZ!Box einfach ausgereift ist.

4 Benutzeranforderungen im Netzwerk

Welche Anforderungen bestehen, wenn im Heimnetzwerk mehr als ein Anwender (User) vorhanden ist oder mehrere User geplant sind? In einem Familiennetzwerk zum Beispiel sollen Sohn, Tochter und Oma in das Heimnetz integriert werden. Jedes Mitglied dieser Familie hat eigene Bedürfnisse und erledigt andere Dinge. Wie ist es da mit der Bandbreite? Ist WLAN noch sinnvoll oder eher Kabel?

Letztlich erwartet ein User von einem Heimnetzwerk, dass es für ihn transparent ist. Darunter ist zu verstehen, dass der Anwender es möglichst intuitiv versteht. Damit sind jedoch keine technischen Hintergründe gemeint, sondern ein Netzwerk sollte für den User so einfach und so verständlich wie möglich sein. Der User surft im Internet, lädt Daten in die Cloud, spielt online, sieht sich einen Film an, und diese Anwendungen müssen tadellos funktionieren.

Doch Personen und ihre Erwartungen sind individuell, und der Begriff „tadellos“ ist sehr dehnbar. Wenn jemand online ein Echtzeitstrategiespiel spielt oder unter Wettbewerbsbedingungen einen Shooter, möchte er die Verzögerungen für die Datenübertragung auf ein Minimum beschränken, denn jede Millisekunde ist kostbar. Wenn man ein Telefongespräch (Voice-over-IP) über sein Netzwerk führt, sollte das Gespräch stabil, ohne hörbare Störungen und flüssig im Dialog verlaufen. Das Nachladen einer Seite der Tageszeitung auf dem Tablet sollte spätestens nach einem Schluck Kaffee abgeschlossen sein.

Doch warum sind solche Überlegungen überhaupt hilfreich? Als Antwort zwei Beispiele: WLAN bietet den Vorteil der kabellosen Mobilität, doch die WLAN-bedingte Zugriffskontrolle auf das geteilte Medium der Funkschnittstelle kann schnell dazu führen, dass Daten verzögert gesendet werden. Das ist üblicherweise kein

Problem für die meisten Anwendungen, doch wenn man für das Onlinegaming die Zugriffszeiten zuverlässig optimieren möchte, empfiehlt sich ein kabelgebundenes Übertragungsmedium. Wichtige Daten sollten regelmäßig als Backup auf ein externes *Network Attached Storage*-(NAS-)Gerät gespeichert werden. Schon heute ist ein Datenvolumen von mehreren Gigabytes eher die Regel als die Ausnahme. Eine hohe Bandbreite des Übertragungsmediums und somit der Einsatz von Gigabit-Ethernet oder dem aktuellsten WLAN-Standard sind hier von Vorteil.

Ein weiterer wichtiger Aspekt bezüglich der Anforderungen an Ihr Heimnetzwerk ist die Sicherheit. Die Hauptpunkte sind die Absicherung gegen unautorisierten Zugriff von außen und die Frage, ob und in welchem Umfang bestimmte Benutzerkategorien Zugriff auf Ihr Netzwerk haben sollten. Hier einige Kriterien, die Sie beachten müssen.:

- Möchte ich Besuchern z. B. über WLAN Zugang zum Internet gewähren? Möchte ich aber auch, dass die Besucher meine Daten auf einem NAS-Gerät oder Mediaserver einsehen bzw. kopieren können?

- Möchte ich mit einem beruflich genutzten Computer auf das Internet zugreifen, ihn aber von meinem restlichen Netzwerk trennen, um Wechselwirkungen zu vermeiden?

- Möchte ich die Computer meiner Kinder nur auf bestimmte Geräte und/ oder bestimmte Bereiche des Internets zugreifen lassen, sie aber von meinem restlichen Netzwerk trennen?

Die Lösung: All diese Fragen und Aufgaben lassen sich mithilfe der FRITZ!-Box schnell und einfach lösen.

Grundlegende How-tos im Heimnetz

5 Bestandsaufnahme: Netzwerkplanung

Bevor Sie loslegen, sollten Sie sich einen kleinen Überblick über alle Geräte verschaffen, die auf das Netzwerk zugreifen sollen, ja ein Teil davon sind – also eine Bestandsaufnahme dessen, welche Geräte wie mit dem Netzwerk verbunden sein sollen.

- Welche Geräte besitzen Sie, und wie sollen sie miteinander Daten austauschen? Ein typisches Szenario wären zum Beispiel ein Windows-PC, ein Apple Mac, ein iPad und ein Android-Smartphone, dazu Drucker, NAS und Smart-TV.

- Welche Geräte nutzen WLAN, und welche können auf Kabel zurückgreifen – etwa der Desktop-PC neben dem Router?

Kabelverbindungen

Kabelverbindungen sind meist etwas schneller als WLAN-Verbindungen. Das hängt aber auch von der Leistung der Netzwerkkarte ab.

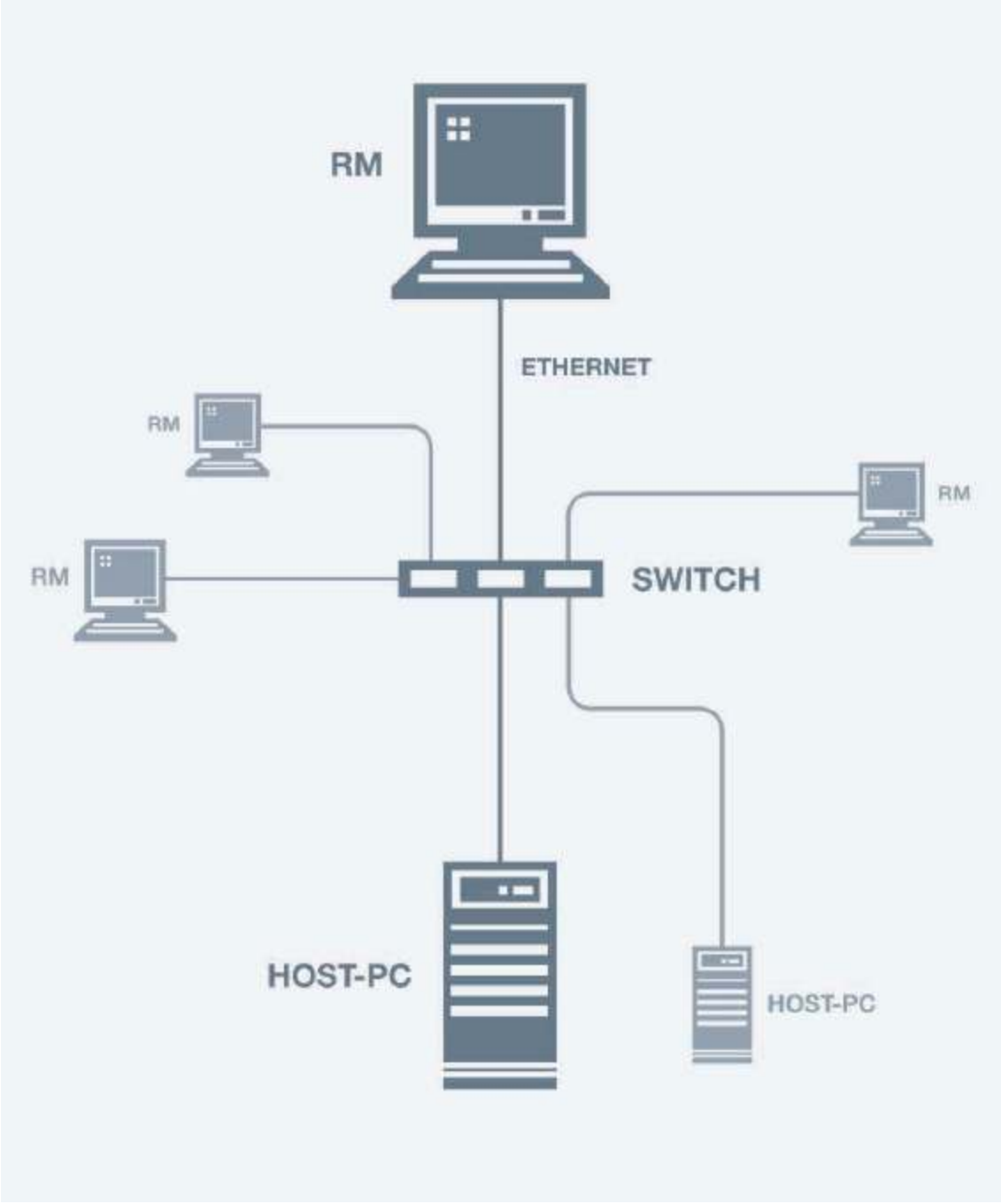
6 Ein Ethernet-Netzwerk installieren

Dieses Kapitel widmet sich der Frage, wie man ein Ethernet-Netzwerk installiert, beispielsweise von den Ethernet-Buchsen Ihres Internetrouters bis zu einer Ethernet-Buchse Ihres PCs. Das folgende Bild zeigt das Prinzip einer Ethernet-Netzwerk-Installation und die möglichen Komponenten. Ein Teil dieser Komponenten ist in einer Heimnetzwerkumgebung optional, und es hängt von der individuellen Installation und Ihnen ab, ob Sie sie einsetzen oder nicht.

Wer keinen Router hat und zwei oder mehr Rechner miteinander verbinden will, der hat zwei Möglichkeiten:

- Die erste Möglichkeit ist, ein Crossover-Kabel zu verwenden. Dabei spielt ein Rechner den Server, also den Hauptrechner, und der bzw. die anderen Rechner sind Clients. Wichtig dabei ist die Vergabe fester IP-Adressen.

- Möglichkeit zwei und auch die bessere Lösung ist, eine Verbindung über einen Switch herzustellen. Ein Switch ist eine Art Hub, aber mit doppelt verdrehten Drähten, die keine Kommunikation mit zwei oder mehr Rechnern ermöglichen, ohne einen Server oder einen Router zu verwenden. Wieder sollten feste IP-Adressen vergeben werden.



(Quelle: *chemanager-online.com*)

Und so geht es:

1 Der Internetrouter wird per Ethernet-Patchkabel an einen Ethernet-Switch angeschlossen.