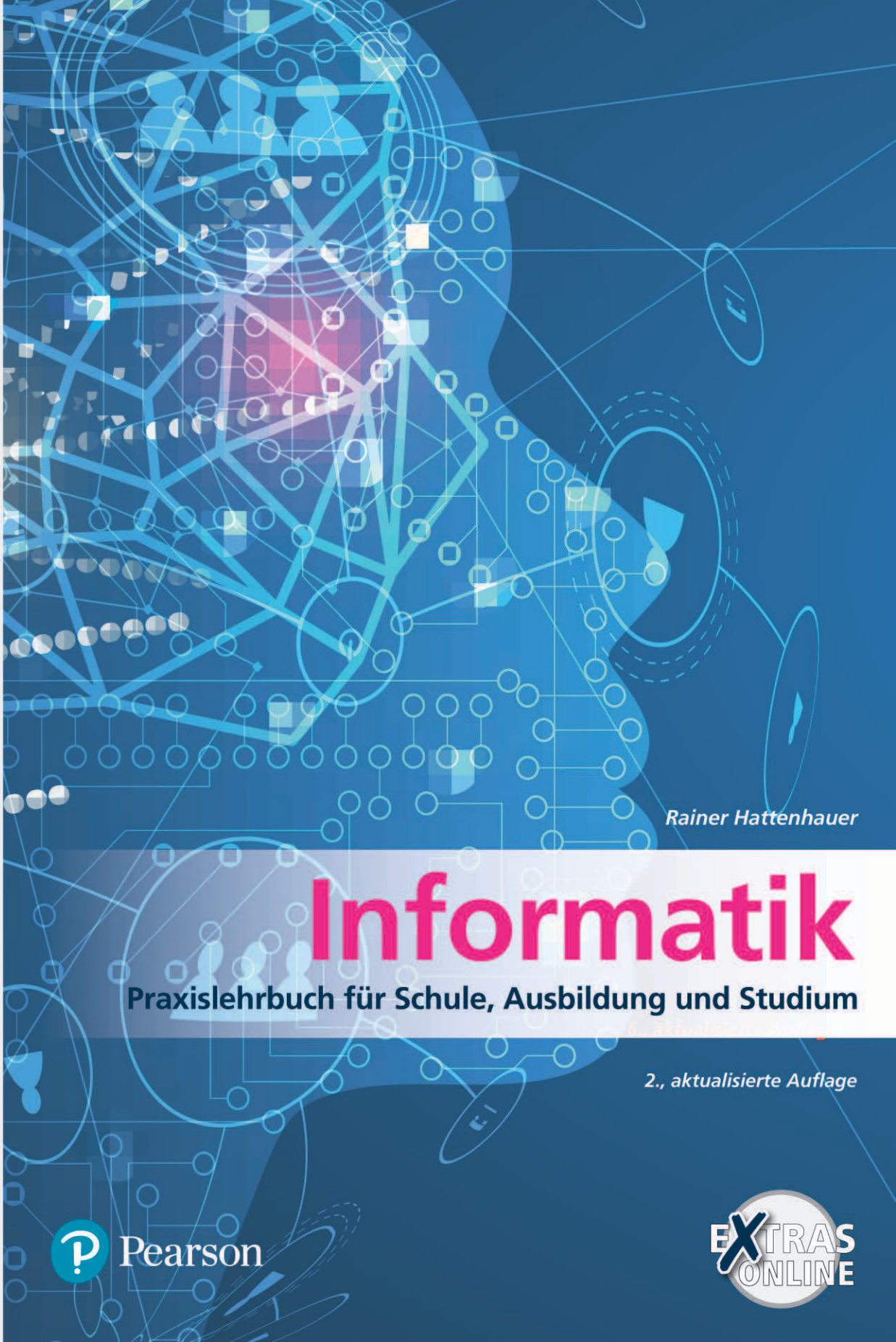


Rainer Hattenhauer

Informatik

Praxislehrbuch für Schule, Ausbildung und Studium

2., aktualisierte Auflage

Pearson

EXTRAS ONLINE

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

Die Informationen in diesem Buch werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt.
Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.Für Verbesserungsvorschläge und Hinweise auf Fehler sind Verlag und Autor dankbar.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien. Die gewerbliche Nutzung der in diesem Produkt gezeigten Modelle und Arbeiten ist nicht zulässig.

Fast alle Produktbezeichnungen und weitere Stichworte und sonstige Angaben,
die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt.
Da es nicht möglich ist, in allen Fällen zeitnah zu ermitteln, ob ein Markenschutz besteht,
wird das ®-Symbol in diesem Buch nicht verwendet.

Der Umwelt zuliebe verzichten wir auf Einschweißfolie.

10 9 8 7 6 5 4 3 2 1

24 23 22 21 20

ISBN 978-3-86894-912-4 (Buch)
ISBN 978-3-86326-962-3 (E-Book)

© 2020 by Pearson Deutschland GmbH
St.-Martin-Straße 82, D-81541 München
Alle Rechte vorbehalten
www.pearson.de
A part of Pearson plc worldwide

Programmleitung: Birger Peil, bpeil@pearson.de
Deskeditor: Elisabeth Prümm, epruemm@pearson.de
Korrektorat: Katharina Pieper
Coverabbildung: shutterstock.com
Herstellung: Claudia Bäurle, cbaeurle@pearson.de
Satz: Gerhard Alfes, mediaService, Siegen (www.mediaservice.tv)
Druck und Verarbeitung: DZS-Grafik, d.o.o., Ljubljana

Printed in the Slovenia

6.2.4 Einen Nameserver einrichten

DNS

Ein *Domain Name Server* (kurz: *DNS*) sorgt für die Umsetzung einer Internet-URL im Stil von *www.google.de* in eine IPv4- bzw. IPv6-Adresse.

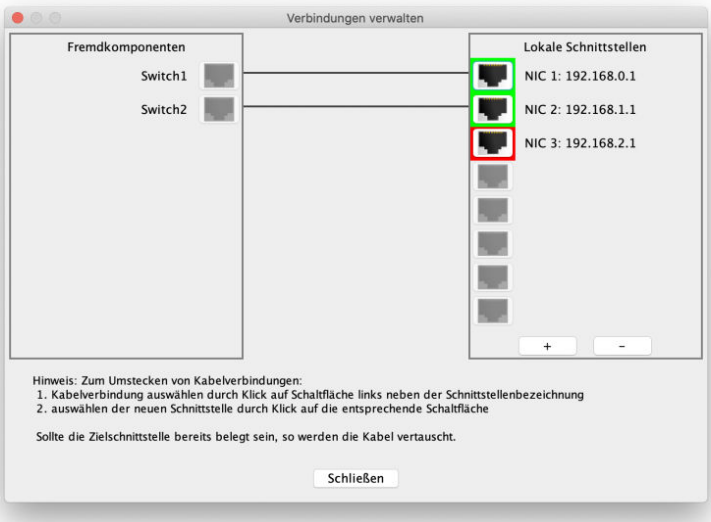
Stellen Sie sich vor, Sie müssten die Adresse eines Rechners im Internet über eine kryptische Zahlenkonfiguration im Stil einer IPv4- bzw. IPv6-Adresse im Browser eingeben. Das wäre sicher sehr unbequem. An die Stelle eines Adressübersetzers tritt ein DNS-Server, um Ihnen die Arbeit zu erleichtern. Die folgende Übung zeigt dessen Einrichtung in der Modellnetzwerkumgebung Filius.

Übung

Statten Sie ein bestehendes Filius-Netzwerk mit einem Nameserver aus.

ANLEITUNG

1. Ergänzen Sie zum Anschluss eines Nameservers einen weiteren Anschluss an den Vermittlungsrechner. Dazu führen Sie über diesem im Konstruktionsmodus einen Doppelklick aus und klicken im Konfigurationsmenü auf die Schaltfläche **Verbindungen verwalten**. Ergänzen Sie im folgenden Fenster über das **+**-Zeichen eine weitere Schnittstelle am Verbindungsrechner. Benennen Sie die Schnittstelle in `192.168.2.1` um.

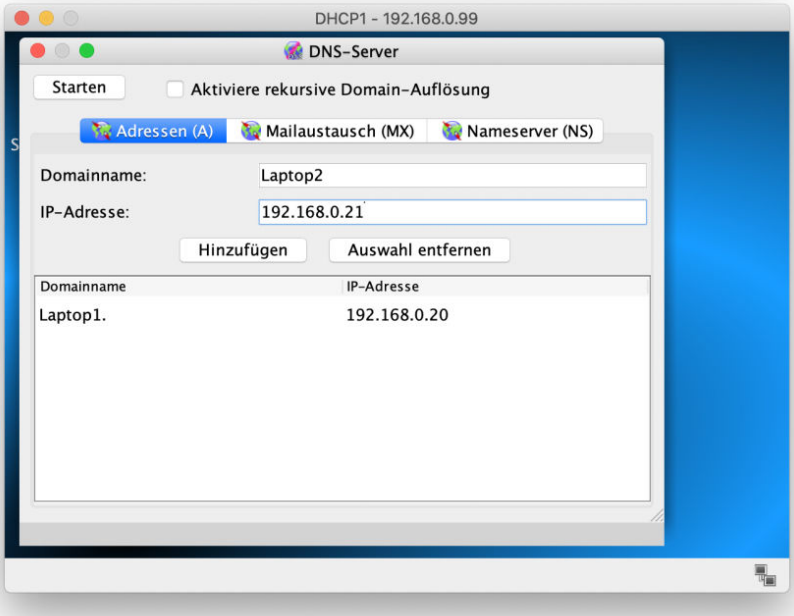


2. Ziehen Sie nun einen weiteren Rechner, der die Rolle des DNS übernehmen soll, aus der Hardwarebibliothek in die Konstruktionsoberfläche. Nennen Sie den Rechner *DNS*. Schließen Sie ihn am Vermittlungsrechner an und weisen Sie ihm die IP `192.168.2.99` zu. Als Gateway stellen Sie auf dem DNS die IP `192.168.2.1` ein.

3. Tragen Sie die Adresse des Nameservers `192.168.2.99` in der entsprechenden Rubrik auf den bestehenden DHCP-Servern ein, sodass die Client-Rechner automatisch mit diesem bekannt gemacht werden. Achten Sie darauf, dass die entsprechenden Gateways auf den DHCP-Servern ebenfalls korrekt gesetzt wurden.

4. Installieren Sie auf dem künftigen DNS-Server die DNS-Software über das Softwareinstallationsicon.

5. Klicken Sie in der Softwareübersicht auf das Icon **DNS-Server**. Erstellen Sie folgendermaßen eine Tabelle zur Namensauflösung: Geben Sie für den ersten Rechner den Domainnamen `Laptop1` sowie die IP-Adresse `192.168.0.20` in die entsprechenden Felder ein. Betätigen Sie anschließend die Schaltfläche **Hinzufügen**. Fahren Sie so fort, bis alle Rechner in die Tabelle aufgenommen wurden.



Starten Sie den Domain Server über die Schaltfläche **Starten**. Testen Sie mithilfe einer Eingabezeile, ob Sie die einzelnen Rechner nun über Ihren Namen anpingen können (Beispiel: `ping Laptop1`).

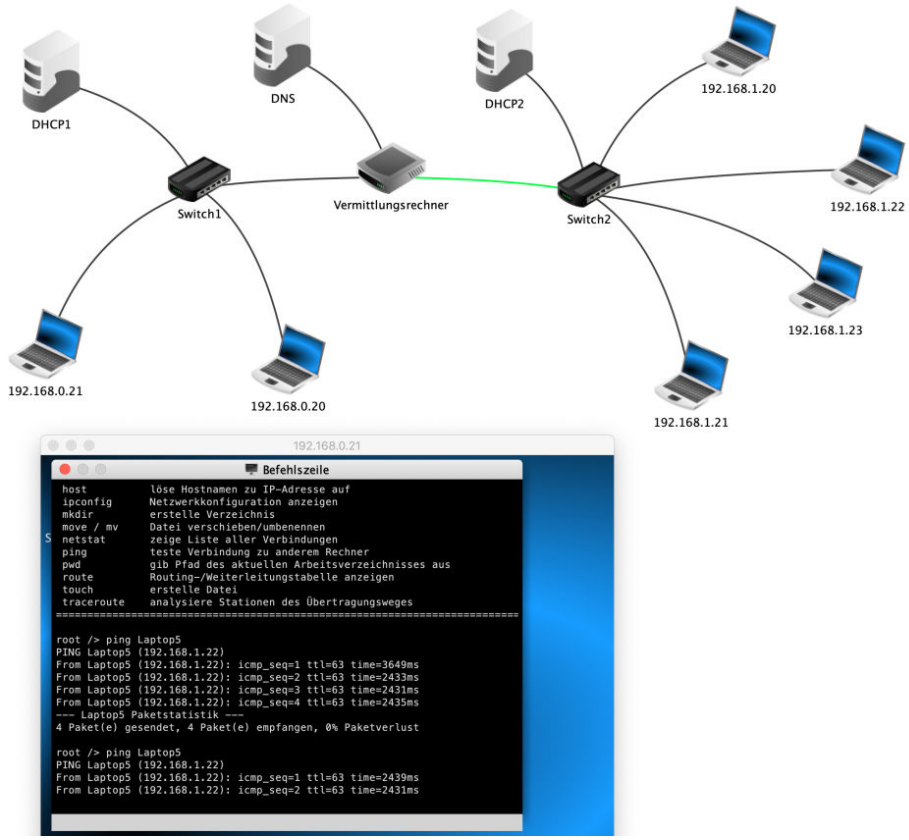


Abbildung 6.14: Die Namensauflösung im Netzwerk übernimmt nun der Domain Name Server. Die Laptops lassen sich gezielt über ihren Namen anpingen.

Damit hätten Sie ihre ersten Übungen auf dem Gebiet der Netzwerktechnik absolviert. Im nächsten Abschnitt schauen wir uns an, wie man Netzwerke in realen Umgebungen einrichtet.

6.2.5 Konfiguration von Netzwerken in realen Betriebssystemen

Die Konfiguration physischer Netzwerke ist heutzutage ein Kinderspiel, da die Anbindung an das Internet zumeist mit einem universellen Router bereits erfolgt ist. Dieser weist den Endgeräten per DHCP automatisch entsprechende IP-Adressen zu. Die Konfiguration erfolgt in der Regel per Browserinterface. In der Praxis schließt man zunächst einen Rechner per LAN-Kabel an den Router an. Dann loggt man sich nach

den Vorgaben des Herstellers auf dem Router ein und kontrolliert die Einstellungen des drahtlosen Netzwerks. Nachdem man dafür ein entsprechendes Passwort definiert hat, lassen sich weitere Endgeräte (Smartphones, Tablets, Laptops) in das WLAN des Routers einbinden.

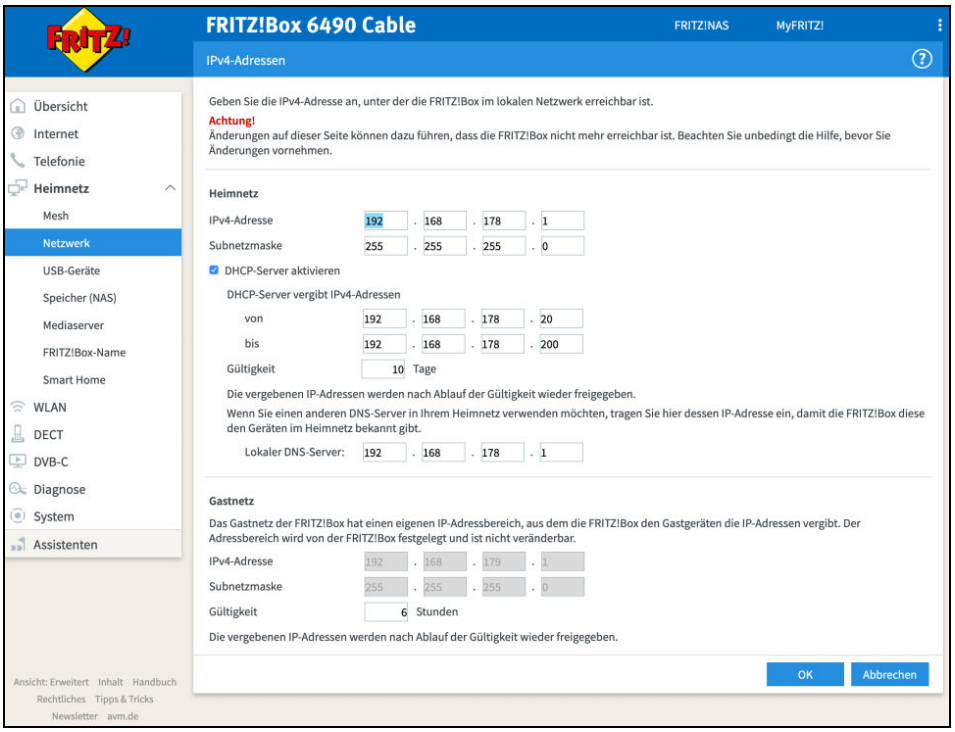


Abbildung 6.15: Netzwerkkonfigurationsbereich einer Fritz!Box. Im vorliegenden Fall wurde der darauf befindliche DHCP-Server konfiguriert und aktiviert.

Auf Seiten der Clients findet man in den gängigen Betriebssystemen entsprechende Tools zur Konfiguration der Netzwerkschnittstellen (LAN, WLAN). Die Schnittstellen sind standardmäßig so vorkonfiguriert, dass die Adressvergabe per DHCP erfolgt. In den seltensten Fällen ist es sinnvoll, davon abzuweichen und statische IP-Adressen vorzugeben.

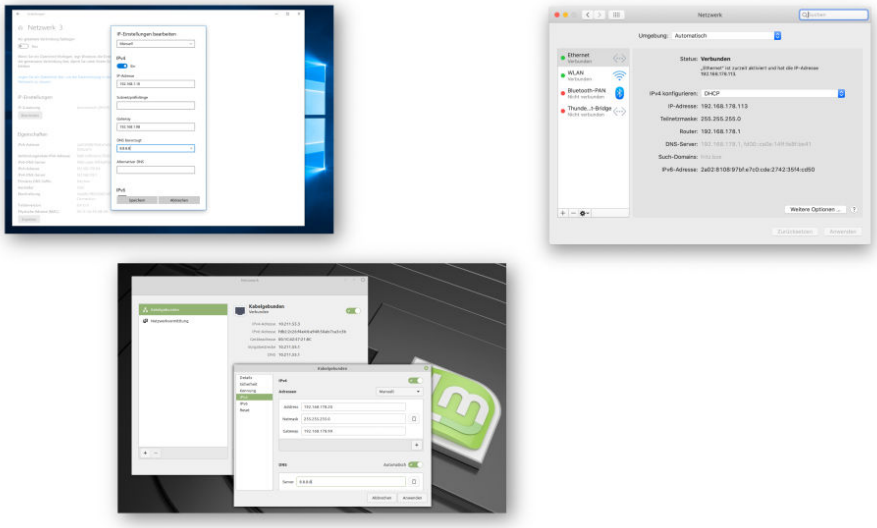


Abbildung 6.16: Die Netzwerkkonfigurationstools von Windows, macOS und Linux Mint

6.2.6 Datenaustausch und Netzwerkfreigaben

Eine wichtige Anwendung in heimischen Netzwerken ist der Datenaustausch über spezielle freigegebene Verzeichnisse *(Netzwerkfreigaben)* oder der direkte Austausch von Dateien zwischen den Einzelgeräten über drahtlose Netzwerke. Folgende Protokolle haben sich als praktikabel erwiesen:

- **NFS:** Das *Network File System* entstammt der Unix-Welt und ist das Mittel der Wahl, wenn man Daten ausschließlich zwischen Linux-/Unix-Rechnern austauschen möchte.
- **SMB:** Möchte man Daten in heterogenen Umgebungen zur Verfügung stellen, dann wird in der Regel auf das *Server Message Block*-Kommunikationsprotokoll zurückgegriffen. Dieses Protokoll wird gleichermaßen von Unix-, Linux-, Mac- und Windows-Rechnern verstanden. Unter Unix/Linux ist zur Nutzung allerdings die Installation der Samba-Software erforderlich.
- **Airdrop:** Im Apple-Universum lassen sich Dateien zwischen den verschiedenen Clients eines drahtlosen Netzwerks austauschen. Dazu werden die Funktechniken Bluetooth bzw. WLAN verwendet.
- **NFC:** Beim Verfahren der *Near Field Communication* werden Daten über sehr kurze Distanzen übertragen. Das können beispielsweise Bilddateien sein, die durch das Aneinanderhalten zweier Smartphones zwischen diesen getauscht werden, aber auch Kontodaten, die für den Prozess des bargeldlosen Bezahlens vom Smartphone auf entsprechender NFC-Terminals an Supermarktkassen übertragen werden. Diese Technik nutzen beispielsweise Bezahldienste wie Apple Pay und Google Pay.

Übung

Erstellen Sie ein Tauschverzeichnis auf Ihrem Rechner, mit dessen Hilfe Sie Dateien zwischen unterschiedlichen Endgeräten austauschen können.

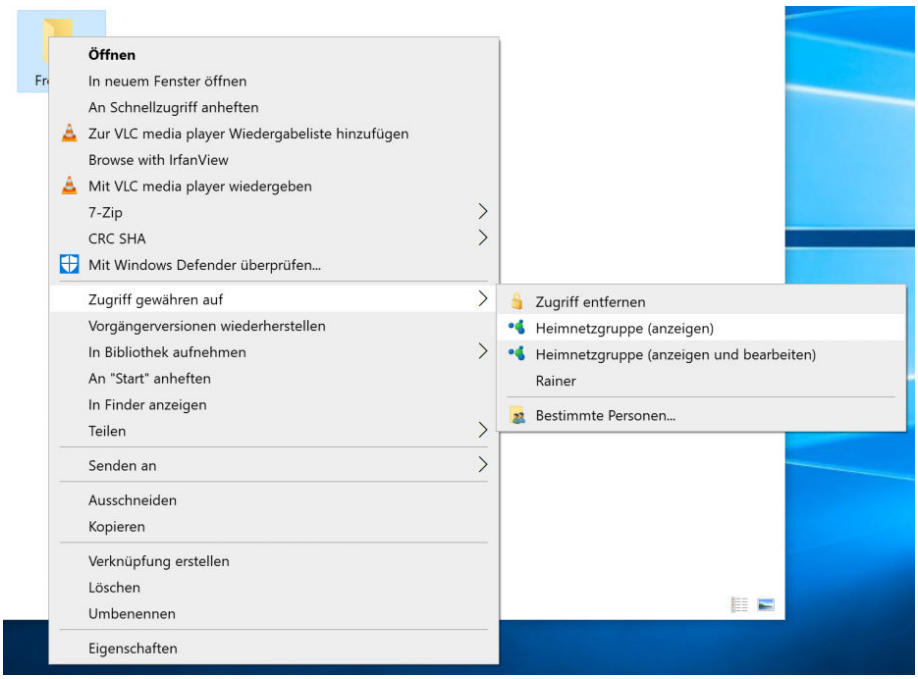
LÖSUNG

Die folgende Anleitung bezieht sich auf einen Windows-10-Rechner. Benutzer von macOS- bzw. Linux-Rechnern finden entsprechende Anleitungen im Internet, indem Sie nach dem Begriff *netzwerkfreigabe macos* bzw. *netzwerkfreigabe linux* googeln.

1. Erstellen Sie innerhalb Ihres Heimverzeichnisses einen Ordner namens `Freigabe`.

2. Führen Sie über dem soeben erstellten Ordner einen rechten Mausklick durch. Wählen Sie aus dem Kontextmenü die Option **Zugriff gewähren** aus und wählen Sie in der erscheinenden Liste ein Freigabelevel, z.B. die Freigabe innerhalb der Heimnetzgruppe oder die Freigabe für bestimmte Nutzer des Rechners.

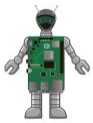
   Sie haben im Falle der Heimnetzgruppe die Möglichkeit, den Ordner nur lesbar (**Heimnetzgruppe(anzeigen)**) bzw. lesbar und schreibbar (**Heimnetzgruppe(anzeigen und bearbeiten)**) freizugeben.



Die Freigabe taucht nun im Bereich *Netzwerk* auf und kann von allen angeschlossenen Rechnern genutzt werden. Die Nutzung der Freigabe funktioniert sogar in heterogenen Netzwerken, d.h. mit einer Mischung aus Windows, macOS oder Linux-Rechnern, sofern diese sich in derselben Netzwerkgruppe befinden.

3. Sie beenden die Freigabe per rechtem Mausklick über dem Verzeichnis und Auswahl des Kontextmenüpunkts **Zugriff gewähren auf** • **Zugriff entfernen**.

Übung: Raspberry als NAS



Statten Sie den Raspberry Pi mit einem USB-Memorystick aus. Geben Sie den Memorystick als Netzwerkspeicher in Ihrem lokalen Netzwerk frei. Sie erhalten damit ein kleines NAS-System.

LÖSUNG

Wir verwenden zur Einbindung des Sticks die bekannte SAMBA-Fileserver-Software.

1. Stecken Sie den USB-Stick an einen USB-Port des Raspberry Pi und rufen Sie über **Systemwerkzeuge** • **GParted** das Partitionierungswerkzeug *GParted* auf. Löschen Sie die bestehende FAT-Partition auf dem Stick und erstellen Sie eine ext4-Partition (vgl. *Kapitel 3*).

   Das ext4-Dateisysstem arbeitet unter Linux deutlich performanter.

2. Installieren Sie die Samba-Software auf dem Raspberry Pi mitmilfe des folgenden Befehls:

   ```
   sudo apt-get update
   sudo apt-get install samba samba-common smbclient
   ```

   Bestätigen Sie die Nachfrage, die `smb.conf`-Datei auf den verwendeten Router Ihres Heimnetzwerks anzupassen.

3. Prüfen Sie, ob der Samba-Fileserver läuft:

   ```
   sudo service smbd status
   sudo service nmbd status
   ```

   Verlassen Sie die Ausgaben der Befehle jeweils durch Betätigen der Taste Q.

4. Definieren Sie einen Samba-Benutzer, der auf die Freigabe zugreifen darf. Wählen Sie dazu den Standardbenutzer `pi` aus und geben Sie auf Nachfrage dessen Passwort ein (theoretisch könnten Sie hier auch ein anderes Passwort speziell für die Freigabe via Samba definieren):

   ```
   sudo smbpasswd -a pi
   ```

   Später können Sie mit der Kombination `pi/<Sambapasswort>` auf die Freigabe zugreifen. Damit wäre der Samba-Fileserver grob vorkonfiguriert.

5. Nun richten wir noch ein Verzeichnis auf dem Stick ein, welches die zu tauschenden Daten enthält. Dazu benötigen Sie zunächst den korrekten Pfad zum Stick innerhalb des Dateisystems. Dass erledigen Sie durch Eingabe des folgenden Befehls:

```
pi@raspberrypi:~ $ df -h
Dateisystem    Größe Benutzt Verf. Verw% Eingehängt auf
/dev/sda         29G     44M   27G    1% /media/pi/<Nummer>
```

   Wichtig ist hier der Eintrag `/media/pi/<Nummer>` mit einer Nummer, die charakteristisch für das verwendete Speichermedium ist.

6. Erstellen Sie auf dem Stick ein Tauschverzeichnis namens `tausch`:

```
sudo mkdir /media/pi/<Nummer>/tausch
```

7. Gewähren Sie den Nutzern des Verzeichnisses unter Linux maximale Lese-/Schreibrechte:

```
sudo chmod a+rw tausch/
```

8. Sichern Sie die Originalkonfigurationsdatei in Ihrem Heimverzeichnis, falls etwas schiefläuft:

```
sudo cp /etc/samba/smb.conf ~
```

9. Bearbeiten Sie nun die Samba-Konfigurationsdatei mithilfe eines Kommandozeileneditors wie z.B. *leafpad*:

```
sudo leafpad /etc/samba/smb.conf
```

10. Ergänzen Sie am Ende der Datei folgende Zeilen:

```
[tausch]
path = /media/pi/<Nummer>/tausch
available = yes
valid users = pi
read only = no
browsable = yes
public = yes
writable = yes
```

11. Speichern Sie die Datei und starten Sie den Samba-Daemon neu:

```
sudo service smbd restart
sudo service nmbd restart
```

Nun können Sie mit einem Netzwerkbrowser von einem anderen PC oder dem Wirtsystem aus das Netzwerk durchsuchen und die Freigabe ausfindig machen. Für den Zugriff benötigen Sie die oben definierte Login/Passwort-Kombination.

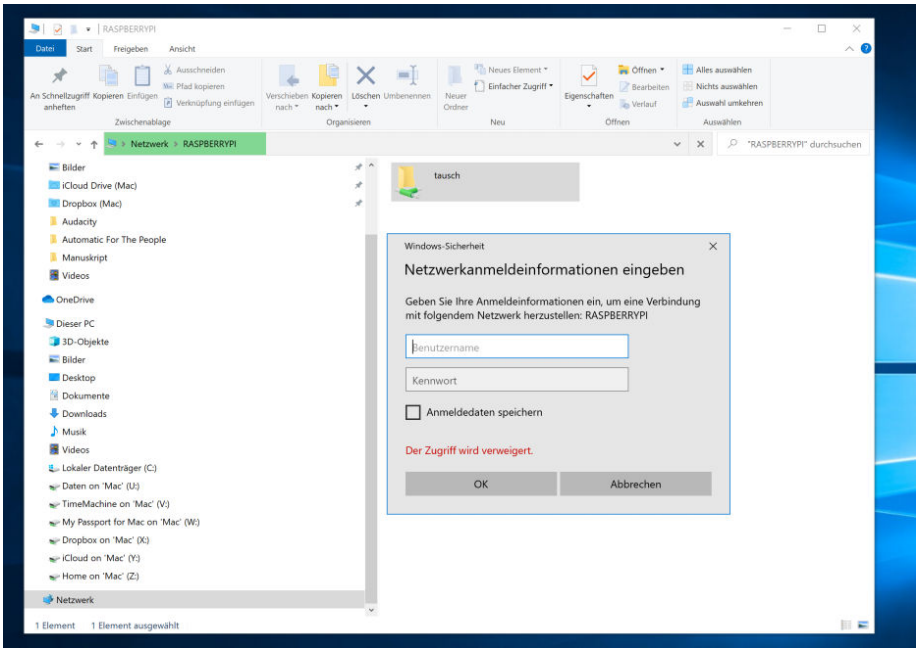


Abbildung 6.17: Für den Zugriff auf die Freigabe ist eine Login/Passwort-Kombination erforderlich.

6.2.7 Cloudspeicherdienste

Daten in der Cloud

„There is no cloud – it's just someone else's computer!" – Dieser in Nerd-Kreisen verbreitete Spruch besagt, dass die Clouddienste der großen Anbieter nichts anderes sind als reservierte Speicherbereiche auf deren Serverparks. Immer mehr Anbieter haben mittlerweile das Vermieten von Speicherkapazität als Geschäftsmodell entdeckt. Ein Terabyte Cloudspeicher kosten aktuell um die 10 € pro Monat, in der Basisversion, die einige wenige Gigabyte umfasst, gibt es den Cloudspeicher sogar umsonst. Die bekanntesten Anbieter von Cloudspeicher sind Dropbox, Google (Google Drive), Apple (iCloud) und Microsoft (OneDrive). Microsoft und Apple binden den Speicher transparent in das jeweilige Betriebssystem ein. Das hat den Vorteil, dass man auf unterschiedlichen Endgeräten bei Nutzung der Clouddienste stets die gleichen Oberflächen/Desktops mit identischen Heimverzeichnissen vorfindet. So kann man ein Dokument am heimischen PC beginnen und auf der Bahnfahrt die Arbeit per Laptop oder Tablet fortführen, ohne das Dokument umständlich umkopieren zu müssen.

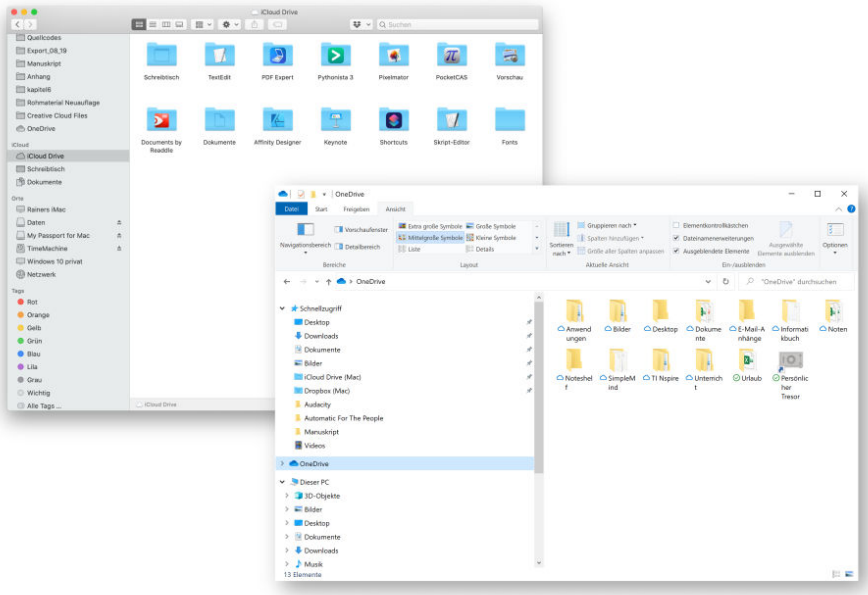


Abbildung 6.18: Windows 10 und macOS nutzen die Clouddienste als zentralen Massenspeicher für das jeweilige Betriebssystem.

6.3 Drahtlose Netzanbindung

Im Zuge des Digitalisierungskonzepts der Industrienationen wächst der Bedarf der Anwender, an jedem beliebigen Ort mit ausreichender Bandbreite online zu gehen. Dazu bieten sich drahtlose Netzwerke in Gestalt von WLAN-Hotspots oder Mobilfunknetze an.

6.3.1 WLAN

Prinzipiell erfolgt die Vernetzung über WLAN in gleicher Weise wie die in *Abschnitt 6.1.5* beschriebene kabelgebundene Vernetzung über die Ethernet-Schnittstele. Die Übertragungsstandards im WLAN-Bereich werden in der Normenfamilie 802.11 definiert. ▶Tabelle 6.2 zeigt die wichtigsten Implementierungen. In aktuellen Routern findet man heute in der Regel den Standard 802.11ac vor.

Name	Verabschiedet	Frequenzband	Transferrate
802.11	1997	2,4 bis 2,485 GHz	2 MBit/s
802.11a	1999	5 GHz	54 MBit/s
802.11b	1999	2,4 bis 2,4835 GHz	11 MBits/
802.11g	2003	2,4 bis 2,4835 GHz	54 MBit/s
802.11g++	2005/proprietär	2,4 bis 2,4835 GHz	bis zu 125 MBit/s
802.11n	2009	2,4 bis 2,4835 GHz,optional 5 GHz	600 MBit/s
802.11ac	2013	5 GHz	bis zu 1299 MBit/s
802.11ad	2013	60 GHz	bis zu 6930 MBit/s

Tabelle 6.2: Vergleich der WLAN-Standards. Bei 802.11g++ handelt es sich um ein proprietäres Format, das einige Hersteller selbst entwickelt haben. Die Werte der Transferraten sind Bruttowerte. In der Realität kann der Anwender lediglich 30 bis 50 % der angegebenen theoretischen Bandbreite nutzen.

Ein wesentlicher Unterschied zum konventionellen LAN besteht in der Notwendigkeit, den drahtlosen Datenverkehr zu verschlüsseln: Schließlich möchte niemand, dass der Nachbar oder ein Passant vor dem Haus „mitlauscht“ oder sich kostenlos in den teuer bezahlten Internetzugang einklinkt.

Zu diesem Zweck wurden Verfahren zur WLAN-Verschlüsselung entwickelt, die in ▶Tabelle 6.3 aufgeführt sind. In der Regel erfolgt heute die Verschlüsselung über WPA2.

Kürzel	Name	Art der Verschlüsselung	Sicherheit
WEP	Wired Equivalent Privacy	Verschlüsselung mit Prüfbitfolge, 24-Bit-Initialisierungsvektor	Gering
WPA	Wi-Fi Protected Access	Zusätzlich zu WEP Verwendung von dynamischen Schlüsseln, 48-Bit-Initialisierungsvektor	Mittel
WPA2	Wi-Fi Protected Access 2	Implementierung des Verschlüsselungsalgorithmus AES (Advanced Encryption Standard)	Hoch

Tabelle 6.3: Übersicht über die wichtigsten WLAN-Verschlüsselungstypen

Zur Einrichtung eines WLAN müssen folgende Informationen vorliegen:

- Die **SSID:** Der *Service Set Identifier* bezeichnet den frei wählbaren Namen eines Funknetzes.
- Die **Art der Verschlüsselung:** Hier empfiehlt sich die Auswahl der bestmöglichen Verschlüsselung, die der verwendete Router anbietet, also in der Regel *WPA2*.
- Der **Pre-Shared Key (PSK)** oder ein **Hexadezimalschlüssel:** Bei einem symmetrischen Verschlüsselungsverfahren verwenden Anwender und Router denselben PSK. Dabei handelt es sich um eine Passphrase, d.h. ein längeres Passwort. Aus dem PSK wird schließlich der eigentliche Schlüssel generiert, der in Hexadezimalform notiert wird.

Copyright

Daten, Texte, Design und Grafiken dieses eBooks, sowie die eventuell angebotenen eBook-Zusatzdaten sind urheberrechtlich geschützt. Dieses eBook stellen wir lediglich als **persönliche Einzelplatz-Lizenz** zur Verfügung!

Jede andere Verwendung dieses eBooks oder zugehöriger Materialien und Informationen, einschließlich

- der Reproduktion,
- der Weitergabe,
- des Weitervertriebs,
- der Platzierung im Internet, in Intranets, in Extranets,
- der Veränderung,
- des Weiterverkaufs und
- der Veröffentlichung

bedarf der **schriftlichen Genehmigung** des Verlags. Insbesondere ist die Entfernung oder Änderung des vom Verlag vergebenen Passwort- und DRM-Schutzes ausdrücklich untersagt!
Bei Fragen zu diesem Thema wenden Sie sich bitte an: **info@pearson.de**

Zusatzdaten
Möglicherweise liegt dem gedruckten Buch eine CD-ROM mit Zusatzdaten oder ein Zugangscode zu einer eLearning Plattform bei. Die Zurverfügungstellung dieser Daten auf unseren Websites ist eine freiwillige Leistung des Verlags. **Der Rechtsweg ist ausgeschlossen**. Zugangscodes können Sie darüberhinaus auf unserer Website käuflich erwerben.

Hinweis
Dieses und viele weitere eBooks können Sie rund um die Uhr und legal auf unserer Website herunterladen:

https://www.pearson-studium.de