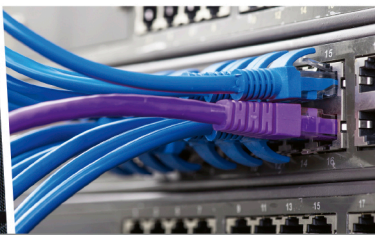
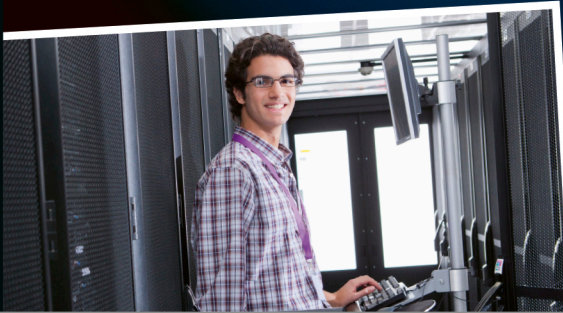


Harald Zisler



Für
Studium
Ausbildung
Beruf

Computer-Netzwerke

Grundlagen, Funktionsweise, Anwendung

- ▶ Planung, Aufbau und sicherer Betrieb von IT-Netzwerken
- ▶ Theorie und Praxis: von der MAC-Adresse bis zum Routing
- ▶ Protokolle und Techniken des OSI-Modells: IPv4/6, TCP, UDP, QUIC, VLANs, VoIP

9., aktualisierte Auflage



Rheinwerk
Computing

Kapitel 4

MAC- und IP-Adressen in der Praxis

Die Arbeit mit MAC- und IP-Adressen ist das tägliche Brot der Netzwerkadministration

4.1 MAC-Adressen

In Ihrer täglichen Netzwerkpraxis werden Sie vor allem bei der Einbindung neuer Geräte in Ihr LAN mit der MAC-Adresse zu tun haben. Sie werden die neuen Geräte anhand dieser Adresse identifizieren und die IP-Adresszuweisung vornehmen.

4.1.1 Ermitteln der MAC-Adresse

Die MAC-Adresse eines Netzwerkgeräts finden Sie im einfachsten Fall auf einem Aufkleber neben der Anschlussbuchse (Abbildung 4.1). Sie finden die Information vielleicht auch in das Gehäuse des *Netzwerk-Chips* fest eingraviert. Eventuell ist sie auch auf der Baugruppe aufgedruckt oder mit einem kleinen Aufkleber angebracht.



Abbildung 4.1: Aufkleber mit MAC-Adresse an einem internen Printserver

Wenn Sie immer noch nicht fündig geworden sind, müssen Sie die MAC-Adresse über das Betriebssystem selbst ermitteln. Handelt es sich dabei um einen PC, melden Sie sich dazu am betreffenden System mit der *Systembetreuererkennung* (`root` bzw. Administrator) an. Die notwendigen Befehle zur Abfrage finden Sie in Tabelle 4.1.

Betriebssystem	Kommando(s)
Linux	<code>ip -brief link show</code>
FreeBSD	<code>ifconfig -a</code>
Windows	<code>getmac /v</code>

Tabelle 4.1: Ermitteln der »eigenen« MAC-Adresse

Listing 4.1 zeigt ein Beispiel, wie Sie die eigene MAC-Adresse unter Linux ermitteln.

```
RE2# ip -brief link show
...
enp0s25    UP    00:11:6b:62:93:2e
           <BROADCAST,MULTICAST,UP,LOWER_UP>
...
```

Listing 4.1: Beispiel: Ermitteln der eigenen MAC-Adresse

Kontrollieren Sie immer nach, ob Sie auch das richtige Netzwerkgerät auslesen, da ein Rechner meist über mehrere davon verfügt (z. B. `lo`).

Können Sie die MAC-Adresse eines Geräts nicht mit der Abfrage nach Tabelle 4.1 vornehmen, verbinden Sie es mit einem PC per Cross-over-Kabel bzw. kreuzen bei Glasfaseranschlüssen beide Adern. Damit liegen beide Geräte in einem einzigen Netzwerksegment. Anschließend verwenden Sie in Abhängigkeit des von Ihnen benutzten Betriebssystems eines der Kommandos aus Tabelle 4.2. Listing 4.2 zeigt ein Beispiel, wie Sie die MAC-Adresse eines anderen Systems unter Linux ermitteln.

Betriebssystem	Kommando(s)
Linux	<code>arp -a ip neigh</code>
FreeBSD	<code>arp -a</code>
Windows	<code>arp -a</code>

Tabelle 4.2: Ermitteln einer MAC-Adresse von einem anderen System aus

```
RE1: ~# ip neigh
192.168.0.102 dev eth0 lladdr 00:11:6b:62:93:2e REACHABLE

RE1: ~# arp
Address          HWtype  HWaddress           Flags Mask    Iface
192.168.0.102    ether    00:11:6b:62:93:2e    C              eth0
```

Listing 4.2: Beispiel: Ermitteln einer MAC-Adresse von einem anderen System aus

Nicht in jedem Fall kommen Sie mit diesen Standardmitteln weiter. Mancher Printserver z. B. lässt sich das erste Mal nur mit einer Spezialsoftware konfigurieren. Dabei müssten Sie »nur« eine IP-Adresse zuweisen, wofür Sie ja die MAC-Adressangabe benötigen. Vielleicht haben Sie einen managbaren Switch? Schließen Sie das Gerät, das anonym bleiben soll, an einem freien Port an. Im Verwaltungsmenü des Switchs können Sie die MAC-Adresse anschließend auslesen. Meist finden Sie diese unter Menüs wie **Dynamic Forwarding Table** oder **MAC-Table**.

4.1.2 Ändern der MAC-Adresse

Sie können das Ändern von MAC-Adressen im Rahmen von Hochverfügbarkeitsszenarien sinnvoll nutzen. Fällt ein Server aus, leiten Sie damit ohne große Umkonfiguration der Systeme den Netzwerkverkehr auf die Redundanz um. Auch bei der Konfiguration von Reservegeräten kann diese Vorgehensweise für Sie nützlich sein. Die notwendigen Kommandos finden Sie in Tabelle 4.3.

Betriebs-system	Kommando
Linux	<code>ifconfig <Gerät> hw ether <Mac-Adresse-neu></code>
FreeBSD	<code>ifconfig <Gerät> link <Mac-Adresse-neu></code>
Windows	Verändern des Registry-Eintrags oder, falls angeboten, im Eintrag bei der Systemsteuerung

Tabelle 4.3: Verändern der MAC-Adresse

Listing 4.3 zeigt ein Beispiel, wie Sie die MAC-Adresse einer Reserve-Netzwerkkarte unter FreeBSD ändern.

```
RE2# ifconfig rl0
rl0: .....
      ether 00:02:44:50:14:47
      .....
RE2# ifconfig rl0 link 00:02:44:50:13:45

RE2# ifconfig rl0
rl0: .....
      ether 00:02:44:50:13:45
      .....
```

Listing 4.3: Beispiel: Ändern der MAC-Adresse einer Reserve-Netzwerkkarte unter FreeBSD

4.1.3 Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«

Mit dem `arp`-Kommando können Sie auch Einträge im ARP-Cache setzen und löschen. Es ist sowohl in der Unix-Welt als auch auf Windows-Rechnern vorhanden. Die Befehlsoptionen sind alle ähnlich: Mit `arp -s <IP-Adresse> <Mac-Adresse>` werden Einträge gesetzt, mit `arp -d <IP-Adresse>` gelöscht.

4.1.4 ARP-Spoofing erkennen

Das (böswillige) Ändern der MAC-Adresse ist auch unter dem Begriff *ARP-Spoofing* bekannt. Angreifer bedienen sich dieser Methode, wenn sie eine *Man-in-the-Middle*-Attacke beginnen wollen. Einen Angriff auf Ihr Netzwerk durch einen manipulierten ARP-Cache erkennen Sie daran, dass alle IP-Adressen auf eine einzige MAC-Adresse zeigen, wie Listing 4.4 zeigt. Wenn Sie auf Derartiges stoßen, müssen Sie sofort handeln. Ihre Systeme sind in größter Gefahr!

```
RE1: ~# arp -a
? (192.168.0.52) auf 00:1b:11:1f:9e:86 [ether] auf eth0
? (192.168.0.53) auf 00:1b:11:1f:9e:86 [ether] auf eth0
? (192.168.0.54) auf 00:1b:11:1f:9e:86 [ether] auf eth0
? (192.168.0.55) auf 00:1b:11:1f:9e:86 [ether] auf eth0
```

Listing 4.4: Beispiel: ARP-Cache nach Spoofing (»vergifteter« ARP-Cache)

4.2 IP-Adressen setzen

Sie können IP-Adressen manuell direkt am Client oder automatisiert im Netz zuweisen. Für größere Netze sollten Sie vorher eine schlüssige Planung hinsichtlich der Adressen selbst vornehmen. Unterteilen Sie Ihr Netz nach Kriterien wie Filialen, Aufgabenbereichen, Infrastruktur oder auch Datenschutz. Sie können damit auch an Übersichtlichkeit gewinnen. Auch die Gerätenamen, die wiederum mit den IP-Adressen zusammengeführt werden, beziehen Sie in diese Planungen mit ein. Sie finden in Tabelle 4.4 Anhaltspunkte, die Ihnen bei Ihrer Netzplanung helfen können.

Konfigurationsfrage	Problematik/Hinweise
IPv4- oder IPv6-Adressen	Kommen reine (ältere) IPv4-Geräte vor (Printserver, NAS, Router ...)? Das interne »Verwaltungsnetz« und das »Arbeitsnetz« können verschiedene IP-Adressversionen haben.

Feste IP-Adressen ohne DHCP-Server	Pro: keine zentrale Instanz, die ausfallen kann (DHCP-Server), hohe Ausfall- und Sabotagesicherheit Contra: Übersichtlichkeitsprobleme möglich, zum Teil umständliche Verwaltung, da jedes Gerät einzeln bearbeitet werden muss
Feste IP-Adresse über DHCP-Server	Pro: vereinfachte netzweite Geräteverwaltung, sogar mit Datenbankeinsatz möglich Contra: Bei einem Ausfall des DHCP-Servers ist kein Netzwerkbetrieb möglich.
IP-Adresse über DHCP-Server (wechselnde Adresse)	Pro: Endgerät ist nicht über IP-Adresse identifizierbar. Contra: nicht für Geräte geeignet, wie z. B. Printserver
Unterteilung in Teilnetze oder verschiedene Netze	Pro: Abbildung von betrieblichen Strukturen, Erhöhung des Datenschutzniveaus Contra: Geräte benötigen bei »Umzug« in ein anderes Teilnetz eine neue IP-Adresse; eine genauere Planung ist notwendig.

Tabelle 4.4: Hinweise zu Adresszuweisung und Netzkonfiguration

Neben der IP-Adresse müssen Sie auch noch die richtige Netzmaske setzen (siehe Abschnitt 3.5.2, »Netz- und Subnetzmaske, Unterteilung von Netzen«). Im Beispiel möchten Sie zwei IPv4-Teilnetze mit maximal 62 Teilnehmern anlegen:

Beispielaufgabe: Berechnung der Subnetzmaske mit »ipcalc«

Netz 1: 192.168.0.0 – 192.168.0.63

Netz 2: 192.168.0.64 – 192.168.0.127

Der Lösungsweg sieht so aus:

Verwenden Sie dazu das Werkzeug *ipcalc*. Sie können das kleine Programm für viele Betriebssysteme bekommen. Es erspart Ihnen die Rechnerei mit den Binärzahlen.

In Abschnitt 3.5.3, »Berechnungen«, finden Sie weitere Berechnungen mit *ipcalc*.

■ Ermittlung der Netzmaske:

Eingabe: `ipcalc 192.168.0.0 – 192.168.0.63`

Ausgabe: `deaggregate 192.168.0.0 – 192.168.0.63`

`192.168.0.0/26`: Die Netzmaske in CIDR-Schreibweise lautet /26.

- Die Berechnung des zweiten Adressblocks führt zum gleichen Ergebnis.
- Ausgabe der Subnetzmaske in Nicht-CIDR-Schreibweise:

Eingabe: ipcalc /26

Ausgabe:

```
Address: 255.255.255.192      11111111.11111111.11111111.
11000000
Netmask: 255.255.255.0 = 24  11111111.11111111.11111111.
00000000
Wildcard: 0.0.0.255          00000000.00000000.00000000.
11111111
=>
Network: 255.255.255.0/24    11111111.11111111.11111111.
00000000
HostMin: 255.255.255.1      11111111.11111111.11111111.
00000001
HostMax: 255.255.255.254    11111111.11111111.11111111.
11111110
Broadcast: 255.255.255.255   11111111.11111111.11111111.
11111111
Hosts/Net: 254               Class invalid
```

4.2.1 Netzwerkkonfiguration von PCs

Für das Setzen von IP-Adressen und weiteren Einstellungen benutzen Sie meist die Werkzeuge der grafischen Benutzeroberfläche (kurz GUI für *Graphical User Interface*). Diese sind Ihnen sicher bekannt, deshalb gehe ich nur kurz darauf ein.

Windows

In Windows 10 und 11 erreichen Sie die Netzwerkkonfiguration am einfachsten über die Suche. Geben Sie dort »Netzwerk« ein; daraufhin bietet Ihnen die Suche bereits das gesuchte **Netzwerk- und Freigabecenter** als Treffer an. Wenn Sie darauf klicken, öffnet sich ein Fenster wie in Abbildung 4.2.

Sie können nun die **Status von Ethernet** sehen. Wählen Sie die gewünschte Netzwerkkarte und anschließend das **Internetprotokoll Version 4** oder **Internetprotokoll Version 6**. Anschließend klicken Sie auf **Eigenschaften** (Abbildung 4.3).

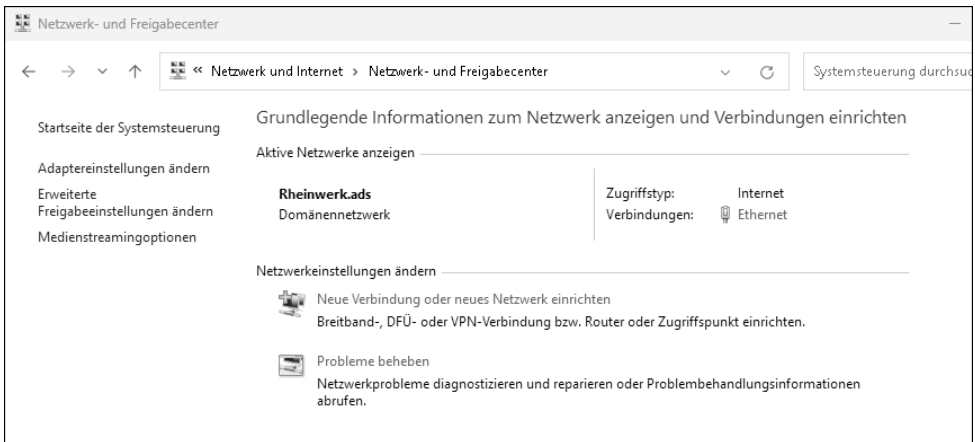


Abbildung 4.2: Netzwerk- und Freigabe, Menüpunkt »Ethernet« wählen



Abbildung 4.3: Eigenschaften von LAN-Verbindung

Egal, für welche IP-Version Sie sich entschieden haben, hier bestimmen Sie nun, ob sich der Rechner die Adresse von einem DHCP-Server abholt oder eine von Ihnen festgelegte Adresse bekommt (Abbildung 4.4).



Abbildung 4.4: Eintragen der IP-Adresse oder DHCP-Zugriff

Welchen Eintrag Sie in das Feld **Standardgateway** setzen müssen, erfahren Sie in Abschnitt 4.7.2, »Festlegen des Standard-Gateways«. Meist wird hier die Adresse des DSL-Routers eingetragen, zumindest bei kleinen Netzen. Windows bietet in dieser Maske auch den Nameserver-Eintrag an. Dies dient der Auflösung von Rechnernamen zu IP-Adressen. Was dies bedeutet, lesen Sie in Abschnitt 4.3, »Verwendung von Rechnernamen«.

Linux

Unter Linux bieten Ihnen die meisten Benutzeroberflächen direkten Konfigurationszugriff. Auch hier gelangen Sie über Systemmenüs zur Netzwerkkonfiguration, wobei Sie die Netzwerkschnittstelle auswählen können. Die Einträge für diese entsprechen meist denen von Abbildung 4.2 bis Abbildung 4.4.

Abseits des GUIs können Sie die Konfiguration direkt per Texteditor vornehmen. Damit können Sie bei Masseninstallationen sehr schnell diesen Teil der Konfiguration durchlaufen lassen, indem Sie nur noch per Skript oder Datenbank erzeugte Konfigurationsdateien am vorgesehenen Ort ablegen.

Das Beispiel bezieht sich auf Debian-Linux, bei anderen Distributionen können Abweichungen von der Beschreibung auftreten. Besonders konservative Linuxderivate, die anstelle des

`systemd` den klassischen `init.d` verwenden, konfigurieren die Netzwerkgeräte auf eine andere Art und Weise. Auch Netzwerkkarten verfügen über eine Gerätedatei. Deren Name ist aber logisch aufgebaut, Beispiel: `enp0s10`. Der Name setzt sich wie folgt zusammen:

- **en**: Ethernet
- **p0**: Nummer Bus
- **s10**: Steckplatz Bus

Debian verwendet den NetworkManager zur Netzwerkkonfiguration. Ob das am konkreten System so vorliegt, prüfen Sie mit der Abfrage `systemctl status NetworkManager.service`. Ist dies der Fall, lesen Sie in der Zeile **Active** die Begriffe **active** (**running**). In diesem Fall finden Sie die Konfigurationsdateien zur manuellen Bearbeitung unter `/etc/netplan`. Das Muster einer fest vergebenen IP-Adresse zeigt diese im YAML-Format gehaltene Datei:

```
network:
  version: 2
  ethernets:
    eth0:
      renderer: NetworkManager
      match: {}
      addresses:
        - "192.168.0.74/24"
      nameservers:
        addresses:
          - 192.168.0.1
      gateway4: 192.168.0.1
      dhcp6: true
      networkmanager:
        uuid: "75a1216a-9d1a-30cd-8aca-ace5526ec021"
        name: "netplan-eth0"
        passthrough:
          connection.timestamp: "1780058694"
          proxy._: ""
```

Abseits von Desktop-Rechnern bietet sich bei den Linuxderivaten statt des NetworkManager die direkte Verwendung von `systemd` an. Der Systemdienst `systemd-networkd.service` muss dabei aktiv sein.

Das erfahren Sie über die Abfrage: `systemctl status systemd-networkd.service`, Ergebnis: **Active: active(running)**. Die Konfigurationsdateien für die Netzwerkgeräte liegen unter `/etc/systemd/network/`. Die Beispielkonfiguration `static.network` enthält diesen Eintrag:

```
[Match]
Name=en*
```

```
[Network]
Address=192.168.0.42/24
Gateway=192.168.0.1
```

Mit `networkctl status enp0s25` (bei Ihrem System natürlich mit dem zutreffenden Netzwerkgerät) erhalten Sie eine umfangreiche Ausgabe, wie Listing 4.5 zeigt.

```
3: enp0s25
    Link File:
    /usr/lib/systemd/network/99-default.link
    Network File:
    /etc/systemd/network/20-wired.network
    State: routable (configured)
    Type: ether
    HW Address: 00:11:6b:62:93:2e
    MTU: 1500 (min: 68, max: 9000)
    Addresses:
    192.168.0.102/24 (DHCP4 via 192.168.0.1)
    fe80::211:6bff:fe62:932e/64
    Gateway: 192.168.0.1
    DNS: 192.168.0.1
```

Listing 4.5: Konfigurationsabfrage Netzwerkkarte mit networkctl

Ein anderes Abfragewerkzeug zeigt Listing 4.6. Mittels `ip addr show` erhalten Sie die Geräte und ihre Adressen aufgelistet.

```
hz@m01: ~$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP>
    mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP>
    mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:1e:33:0d:e9:f9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.234/24 brd 192.168.0.255 scope global
    dynamic enp0s10
```

```

    valid_lft 42828sec preferred_lft 42828sec
inet6 fda6:da5c:fcba::8fa/128 scope global
    valid_lft forever preferred_lft forever
inet6 fda6:da5c:fcba:0:70e7:9b9e:f380:e26e/64 scope
global temporary dynamic
    valid_lft 604432sec preferred_lft 85986sec
inet6 fda6:da5c:fcba:0:21e:33ff:fe0d:e9f9/64 scope
global mngtmpaddr noprefixroute
    valid_lft forever preferred_lft forever
inet6 2003:d3:93f1:1900:21e:33ff:fe0d:e9f9/64 scope
global mngtmpaddr noprefixroute dynamic
    valid_lft 13845sec preferred_lft 1245sec
inet6 fe80::21e:33ff:fe0d:e9f9/64 scope link
    valid_lft forever preferred_lft forever
3: wlp5s0: <BROADCAST,MULTICAST,UP,LOWER_UP>
    mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:22:5f:87:99:d0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.202/24 brd 192.168.2.255 scope global
dynamic wlp5s0
    valid_lft 42851sec preferred_lft 42851sec
inet6 fe80::fea6:abdc:9189:b898/64 scope link
    valid_lft forever preferred_lft forever

```

Listing 4.6: Ausgabe von »ip addr show«

Sehen Sie sich die Ausgabe in Listing 4.6 genau an. Beim Loopback-Gerät und `enp0s10` sehen Sie auch jeweils die IPv6-Adresse. Diese Adressen werden automatisch konfiguriert, weil bei der Installation des Systems die IPv6-Unterstützung aktiviert wurde. Wenn Sie hier eingreifen möchten, sollten Sie unbedingt auch das zutreffende Systemhandbuch zurate ziehen. Ferner sehen Sie in der Ausgabe die MAC-Adresse, die Menge bereits transportierter Pakete und weitere Konfigurationseinstellungen, die normalerweise aber nicht geändert werden müssen, z. B. die MTU-Größe.

Bei der IPv6-Adresse handelt es sich um eine Link-local Unicast-Adresse (Tabelle 3.19). Wenn Sie jetzt eine feste IPv6-Adresse (privat, Unique-local Unicast-Adresse) zusätzlich vergeben wollen, ergänzen Sie einfach den Eintrag in der jeweiligen Konfigurationsdatei des Netzwerkgerätes. Die IP-Konfiguration für Linux ist damit abgeschlossen.

FreeBSD

Unter FreeBSD nehmen Sie die Netzwerkeinstellungen in der zentralen Konfigurationsdatei `/etc/rc.conf` vor. Eine IPv4-Adresse benötigt folgende Einträge, wie Listing 4.7 zeigt.

```
ifconfig_re0="inet 192.168.0.25 netmask 255.255.255.0"  
defaultrouter="192.168.0.1"
```

Listing 4.7: »/etc/rc.conf«, Eintrag einer IPv4-Adresse

re0 bezeichnet dabei die jeweilige Netzwerkschnittstelle Ihres Systems (bei Ihnen gegebenenfalls anders benannt).

Eine Besonderheit unter FreeBSD sind die Jails. Sie können damit eigene, vom Rest des Systems abgeschottete Umgebungen einrichten. Damit diese Zugriff auf das Netzwerk erhalten, werden Aliase verwendet, wie Listing 4.8 zeigt.

```
# -- Aliase für Jails  
ifconfig_re0_alias0="inet 192.168.0.65 netmask 255.255.255.255"  
ifconfig_re0_alias1="inet 192.168.0.66 netmask 255.255.255.255"  
ifconfig_re0_alias2="inet 192.168.0.67 netmask 255.255.255.255"
```

Listing 4.8: »/etc/rc.conf«, Aliase für Jails

Jeder Alias erhält dabei mit der Netzmaske 255.255.255.255 eine eigene, einzelne IP-Adresse zusätzlich zur eigentlichen Interface-Adresse – passend für je eine Jail.

Den Adressbezug vom DHCP-Server fordern Sie mit der Zeile aus Listing 4.9 für eine Netzwerkkarte an:

```
ifconfig_rl0="DHCP"
```

Listing 4.9: »/etc/rc.conf«, Netzwerkkarte mit Adressbezug vom DHCP-Server

Eine IPv6-Adresse tragen Sie wie in Listing 4.10 gezeigt ein:

```
ipv6_enable="YES"  
ipv6_network_interfaces="ae0"  
ipv6_ifconfig_ae0="fd91:e4a5:5e03::dd04 prefixlen 64"  
ipv6_defaultrouter="fd91:e4a5:5e03::dd01"
```

Listing 4.10: »/etc/rc.conf«, IPv6-Adresse, statisch

Die erste Zeile aktiviert IPv6 grundsätzlich, die zweite legt fest, für welche Schnittstelle(n) IPv6 konfiguriert werden soll. Die dritte Zeile setzt die statische IPv6-Adresse mit Präfixlänge, die vierte den Standard-Gateway.

Nachdem Sie neue Einträge gesetzt oder bestehende geändert haben, werden sie nach dem Neustart des Netzwerks wirksam. Für IPv4-bezogene Einträge verwenden Sie:

```
/etc/rc.d/zentrale/netif restart
```

IPv6-Einstellungen geben Sie dem System durch den Aufruf

```
/etc/rc.d/network_ipv6 restart
```

bekannt. Anschließend kann es notwendig sein, auch

```
/etc/rc.d/routing restart
```

auszuführen. Wie unter Linux können Sie mit dem `ifconfig`-Kommando die aktuell geladenen Netzwerkeinstellungen abfragen. Dieses Kommando hilft Ihnen aber nicht nur bei der Abfrage von Netzwerkeinstellungen, sondern auch bei vielen Konfigurationsarbeiten bis hin zum WLAN.

macOS

Klicken Sie auf das Apple-Symbol, dann auf **Systemeinstellungen • Netzwerk**. Rechts sehen Sie die vorhandenen Netzwerkschnittstellen (Abbildung 4.5). Wählen Sie die Schnittstelle aus, die Sie konfigurieren möchten – in unserem Beispiel ist das der USB-Ethernet-Adapter **USB 10/100/1000 LAN 4**. Bei einem Mac mit eingebauter Ethernet-Buchse heißt der Eintrag **Ethernet**.

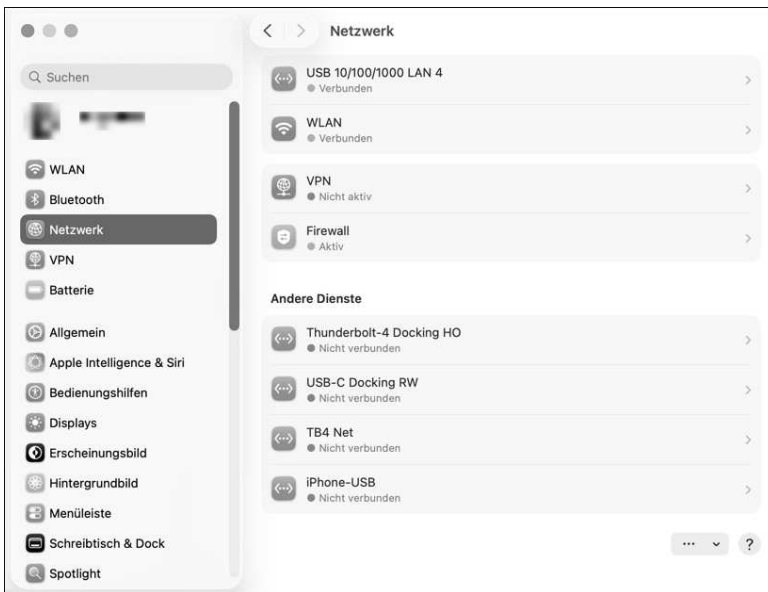


Abbildung 4.5: Auswahl der Netzwerkschnittstelle in den Systemeinstellungen

Die Detailseite der Schnittstelle zeigt den Verbindungsstatus mit IPv4-Adresse, Teilnetzmaske, Router und DNS-Server (Abbildung 4.6). Hier ist die Adressvergabe per **DHCP** eingetragen. Für Änderungen klicken Sie auf **Details**

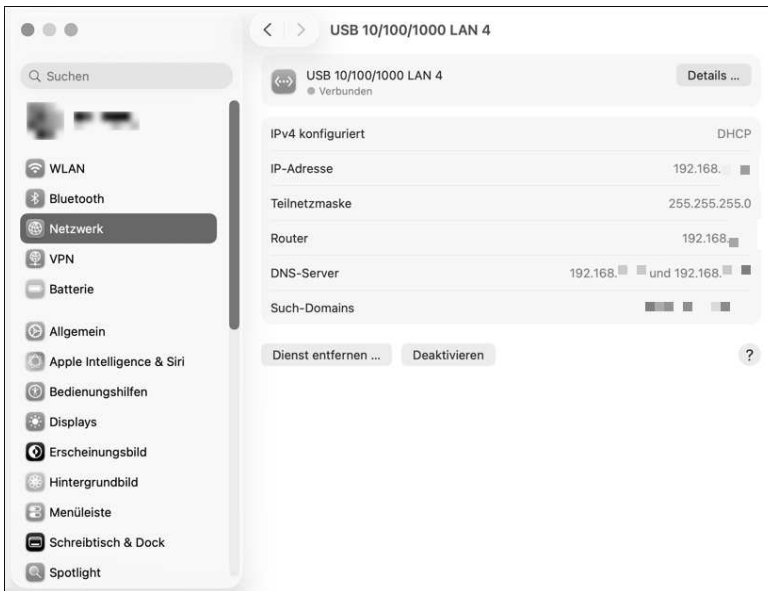


Abbildung 4.6: Status und IPv4-Konfiguration der gewählten Schnittstelle

Auf der Karteikarte **TCP/IP** wählen Sie im Punkt **IPv4 konfigurieren** die gewünschte Variante aus, zum Beispiel **DHCP** oder **Manuell**. Hier können Sie weitere Verfeinerungen vornehmen und im Punkt **IPv6 konfigurieren** auch die IPv6-Adresse festlegen (Abbildung 4.7).

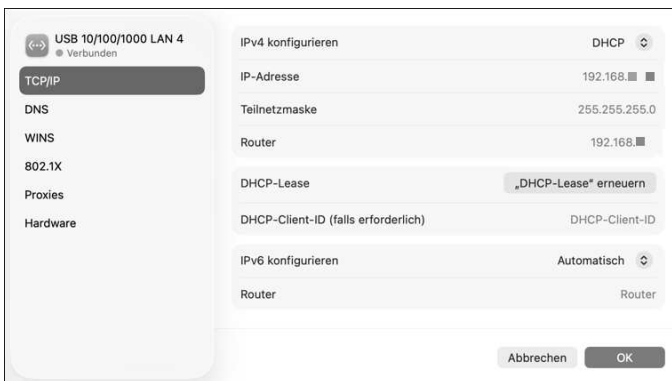


Abbildung 4.7: Feinkonfiguration der TCP/IP-Adressen

Die MAC-Adresse und andere physikalische Einstellungen sehen Sie, wenn Sie die Karteikarte **Hardware** auswählen. Stellen Sie den Punkt **Konfigurieren** von **Automatisch** auf **Manuell** um, können Sie Geschwindigkeit, Duplex und MTU selbst festlegen (Abbildung 4.8).

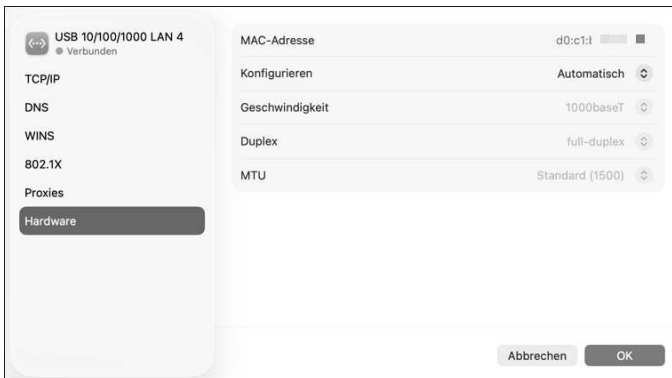


Abbildung 4.8: Einstellungen der Netzwerkschnittstelle

4.2.2 IP-Adresskonfiguration von weiteren Netzwerkgeräten

Im Netzwerk finden Sie weitere Geräte vor, denen Sie eine IP-Adresse zuweisen müssen: Konfigurationszugänge von managebaren Switches und Routern, Printservern, Kameras, NAS-Boxen bis hin zu Telefonanlagen und Heizungssteuerungen.



Abbildung 4.9: Netzwerkconfiguration eines »Kyocera Mita FS-1370DN« über das Bedienfeld

Speziell bei den Printservern begegnen Ihnen eingebaute und externe Modelle. Wenn der Drucker über ein Bediendisplay verfügt, wie es in Abbildung 4.9 gezeigt wird, können Sie die Adresse direkt hierüber setzen.

Bei allen anderen Geräten (nicht nur bei den Printservern) hilft Ihnen nur ein Blick in die Installationsanleitung. Sie erfahren daraus die voreingestellte IP-Adresse oder erhalten einen Hinweis darauf, ob das Gerät per DHCP seine Adresse bezieht. Manchmal müssen Sie sogar

ein spezielles Konfigurationsprogramm unter Windows bemühen, damit Sie erstmals eine Adresse auf dem neuen Gerät setzen können. Alle diese Geräte bieten Ihnen auch eine Web-Oberfläche zur weiteren Einstellung. In Abbildung 4.10 sehen Sie die Netzwerkconfiguration eines Printservers, der beide IP-Protokollversionen benutzen kann.

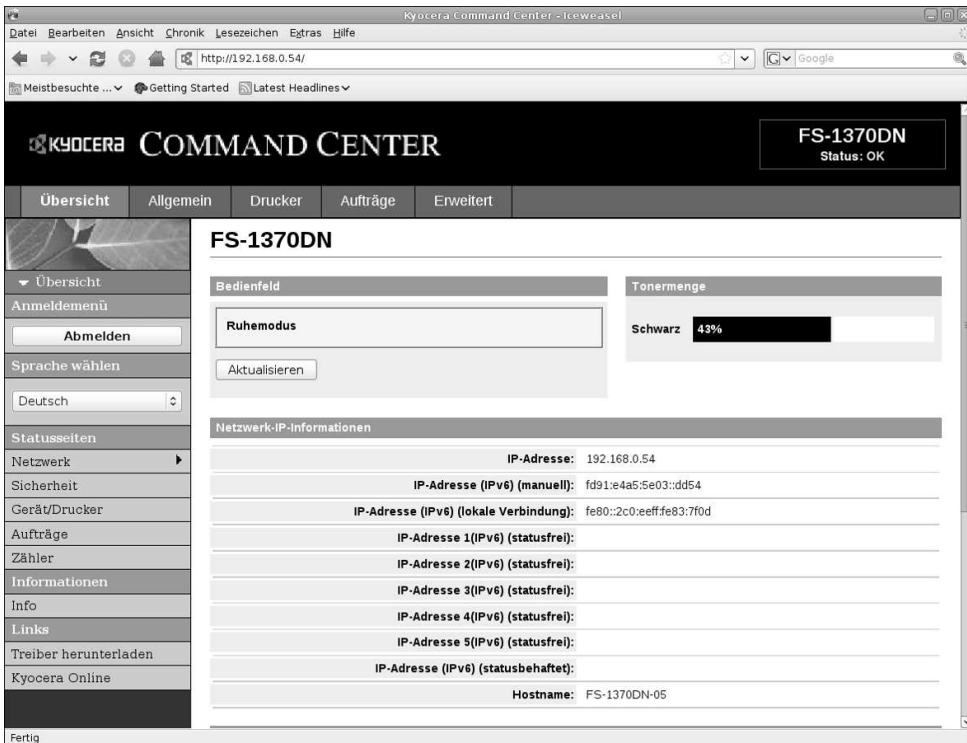


Abbildung 4.10: Konfiguration des Printservers eines »Kyocera Mita FS-1370DN« für IPv4 und IPv6

Ändern Sie im Rahmen dieser Erstkonfiguration in jedem Fall das Standardkennwort, das der Hersteller vergeben hat! »Offene« Netzwerkgeräte stellen ein großes Sicherheitsproblem dar und gefährden Ihr Netzwerk.

Sie werden bei einer Umstellung Ihres Netzwerks von IPv4 auf IPv6 auf die »Netzwerkkleingeräte« Rücksicht nehmen oder diese durch neue ersetzen müssen. Falls Sie sowieso mit einem »Schattennetz« zur Verwaltung der Switches, Router und anderer Netzwerkkomponenten arbeiten, belassen Sie dort einfach IPv4, solange die vorhandenen Geräte ihren Dienst verrichten.

4.2.3 Zentrale IP-Adressverwaltung mit dem DHCP-Server

Mit dem *Dynamic Host Configuration Protocol (DHCP)* können Sie über einen zentralen Rechner (fast alle) Netzwerkgeräte konfigurieren.

An DHCP-Servern kommt niemand im täglichen Internetleben vorbei. Die meisten Internet-Service-Provider teilen Ihnen bei der Einwahl für die Zeit der Verbindung eine IP-Adresse aus einem Pool zu. Meist darf Ihr Rechner oder Router diese Adresse für maximal 24 Stunden behalten – dann vergibt der Dienstleister eine neue Adresse.

Auch für Ihre lokalen Netzwerke bietet DHCP einige Vorteile:

- zentrale Netzwerkadministration, auch mit datenbankbasierter Inventarverwaltung
- einfache Konfiguration der Clients: Sie müssen nur die Einstellung **IP-Adresse automatisch beziehen** setzen.
- Zusammen mit dem *Bootstrap Protocol (BOOTP)* können Sie sogar plattenlose Rechner betreiben – hier müssen Sie am Client fast nichts mehr konfigurieren (Sie müssen nur die Bootreihenfolge im BIOS einstellen).

Diesen Vorteilen stehen aber auch einige Nachteile gegenüber, die nicht verschwiegen werden sollen. Fällt Ihr DHCP-Server aus, bekommen später hinzukommende Clients keine IP-Adresse mehr. Ein zusätzlicher, böswillig an das Netz angeschlossener DHCP-Server kann zudem Adressen für einen Angriff auf das Netzwerk vergeben (*Rogue DHCP*); eine verwandte Angriffsmethode ist, den DHCP-Server so lange um Adressvergaben zu bitten, bis der komplette Pool belegt ist – dann bekommen Clients ebenfalls keine Adresse mehr zugewiesen.

Auch eine feste Zuordnung von MAC- zu IP-Adresse erhöht die Netzwerksicherheit entgegen der Erwartung nicht wirklich: Böswillige Personen ändern entweder die eigene MAC-Adresse passend ab oder setzen gleich eine feste IP-Adresse. Schließlich benötigen Sie für jedes Subnetz einen eigenen DHCP-Server, da sich dieser innerhalb derselben Broadcast-Domäne befinden muss; soll er stattdessen über das Subnetz hinweg erreichbar sein, müssen Sie den verbindenden Router als DHCP-Relay konfigurieren, der Anfragen und Antworten dann als Unicast-Nachricht über die Netzwerkgrenze hinweg weiterleitet.

Sehen Sie sich den Leistungsumfang des DHCP-Protokolls an. Mit DHCP können Sie noch mehr zuweisen, als nur IP-Adressen:

- IP-Adresse
- Netzwerkmaske (Subnetzmaske)
- Default-Gateway
- DNS-Server (Nameserver)
- Zeit- und NTP-Server
- Proxykonfiguration über WPAD

Dabei belegt DHCP die Ports UDP 67 (Server) und UDP 68 (Client). Die wichtigsten RFCs zum Nachlesen sind **2131**, **2132**, 3396, 3442, 3942, 4361, 4833, 4862, 5494, 6221, 6422, 6842, 7084, 7227, 7527, 8981, 9096, 9686, 9762, 9818 und **9915**.

Bei der Adresszuweisung unterscheiden Sie zwei Verfahren: Bei der *manuellen Adresszuweisung* wird für eine angegebene MAC-Adresse immer dieselbe IP-Adresse vergeben. Dies ist für alle Netzwerkgeräte von Vorteil, deren Dienste von anderen genutzt werden, wie z. B. Printserver. Bei der *dynamischen Zuordnung* bekommt ein anfragender Client dagegen eine beliebige Adresse aus einem festgelegten Adressbereich für eine bestimmte Zeit zugewiesen. Die Zuweisung selbst nennt man *Lease*, die Zeitspanne der Gültigkeit *Leasetime*.

Im Vorgriff auf Kapitel 5, »Internet Control Message Protocol (ICMP): Steuer- und Fehlercodes übertragen«, und Kapitel 6, »Datentransport mit TCP und UDP«, sehen Sie in Tabelle 4.5 speziell den Aufbau eines DHCP-Pakets dargestellt.

Byte	Feld
1	Anforderung (1) Antwort (2) (op)
1	Netzwerktyp (1 für Ethernet) (htype)
1	Länge Hardware-Adresse (6 Byte bei MAC-Adresse) (hlen)
1	Zahl der DHCP-Relay-Agenten (hops)
4	Transaktions-ID (xid)
2	abgelaufene Zeit seit Client-Start in Sekunden (secs)
2	Gültigkeit der IP-Adresse beim Client, Byte 2 reserviert (flags)
4	IP-Adresse des Clients, falls schon vorhanden (alte Adresse) (ciaddr)
4	zugeteilte IP-Adresse (yiaddr)
4	IP-Adresse des DHCP-Servers (siaddr)
4	IP-Adresse des DHCP-Relays (Router) (giaddr)
16	Client-MAC-Adresse (chaddr)
64	Host-Name des DHCP-Servers, Angabe optional (sname)
128	Boot-Image (Dateiname, wenn TFTPboot verwendet wird) (file)
312	Optionen (options)

Tabelle 4.5: Aufbau eines DHCP-Pakets

DHCP-Server finden Sie auch in DSL- und WLAN-Routern. Hier steht Ihnen eine komfortable Weboberfläche für Ihre Einträge zur Verfügung (Abbildung 4.11). Mit wenigen Angaben erhalten Sie für ein kleines Netz den DHCP-Komfort.

LAN IP Setup

☐ Enable UPnP

LAN TCP/IP Setup

IP Address

192

168

0

1

IP Subnet Mask

255

255

255

0

RIP Direction

None

RIP Version

Disabled

MTU Size

☐ Default (1500)
☒ Custom

1492

LAN IP Address Management

☐ Disable DHCP Server
☐ Use External DHCP Server
☒ Use Router as DHCP Server

DHCP Server Info

Starting IP Address

192

168

0

102

Ending IP Address

192

168

0

110

DNS Server Address
☒ Router is DNS Proxy
☐ Use These DNS Servers

Primary DNS

Secondary DNS

WINS Server

Lease Time (hours)

24

Reserved IP Table

	#	IP Address	Mac Address	Device Name

Abbildung 4.11: Webkonfigurationsoberfläche mit DHCP-Einrichtung eines DSL-Routers

Die Konfiguration eines DHCP-Servers finden Sie in der Datei `dhcpd.conf`. Bei Linux und FreeBSD finden Sie die Datei im Verzeichnis `/etc` bzw. `/usr/local/etc`. Die wichtigsten Punkte finden Sie hier mit Kommentaren (#) in der Muster-Konfiguration dargestellt.

```
# Gültigkeit der Zuweisung (Standard- und Maximalwert)
# in Sekunden
default-lease-time 600;
max-lease-time 7200;
```

```
# Der Server ist für das lokale Netz der alleinig
# zuständige:
authoritative;
# Angaben der Subnetzmaske, der Broadcast-Adresse, der
# Router, des Nameservers und des Domain-Namens

option subnet-mask 255.255.255.0;
option broadcast-address 192.168.5.255;
option domain-name-servers 192.168.5.1;
option domain-name "DOMAINNAME.TLD";

# Dynamisch zu vergebender Adressbereich

subnet 192.168.5.0 netmask 255.255.255.0 {
range 192.168.5.50 192.168.5.99;
}

# Feste Adresszuweisung für MAC-Adresse
# Die Adresse liegt außerhalb des Bereichs
# dynamisch zu vergebender Adressen

host schulung1 {
hardware ethernet 01:02:03:1a:1b:1c;
fixed-address 192.168.5.100;
}
```

Listing 4.11: Muster-Konfiguration der »dhcpd.conf«

Sie finden weitere Optionen in der Dokumentation, die Sie unter Linux oder FreeBSD mit `man dhcpd.conf` abrufen können. Windows-Benutzer lesen die dem Programm beiliegende Information. Falls Sie eine Datenbanklösung für Ihre Geräteverwaltung erstellen, binden Sie die `dhcpd.conf` gleich mit ein. Ihr Skript sollte den Kopf dieser Datei inklusive der `subnet-`Anweisung aus einer eigenen Datei mit der Datenbankabfrage zusammenführen, die die festen Zuweisungen ausgibt. Das ist unkomplizierter zu programmieren als die Lösungen, die explizit Zeileneinträge ändern. Nach jeder Neuerstellung der `dhcpd.conf`-Datei sollten Sie (oder das Skript) den DHCP-Server neu starten.

Für die Fehlersuche hilft Ihnen ein Packet-Sniffer wie `tcpdump`. Die (kommentierte Ausgabe) finden Sie in Listing 4.12. Es zeigt eine funktionierende Adresszuweisung:

```
# Aufruf tcpdump:
tcpdump -i NETZWERKGERÄT -n port 67 and port 68
```

```
# Adressanforderung durch den Client
10:59:31.592136 IP 0.0.0.0.68 > 255.255.255.255.67:
BOOTP/DHCP, Request from a8:13:74:28:2d:b4, length 293
# Antwort vom DHCP-Server
10:59:31.593451 IP 192.168.23.1.67 > 192.168.23.222.68:
BOOTP/DHCP, Reply, length 548
```

Listing 4.12: Ausgabe von »tcpdump«

Speziell für die Fehlersuche können Sie `dhcpcdump` benutzen. Dessen Ausgabe ist ausführlicher (Listing 4.13). Auch hier sehen Sie eine funktionierende Zuweisung:

```
# Aufruf: dhcpcdump -i NETZWERKGERÄT

## Suchen DHCP-Server ##
TIME: 2026-07-11 11:07:37.857
  IP: 0.0.0.0 (a8:13:74:28:2d:b4) >
  0.0.0.0 (ff:ff:ff:ff:ff:ff)
  OP: 1 (BOOTPREQUEST)
.....
OPTION: 53 ( 1) DHCP message type          1 (DHCPCDISCOVER)
.....
# Adresse anfordern
TIME: 2026-07-11 11:08:10.745
  IP: 192.168.23.1 (1c:ed:6f:ef4:a1:4e) >
  192.168.23.1 (a8:13:74:28:2d:b4)
  OP: 2 (BOOTPREPLY)
.....
OPTION: 53 ( 1) DHCP message type          2 (DHCPOFFER)
.....
# Adresse beziehen
TIME: 2026-07-11 11:08:10.745
  IP: 192.168.23.1 (1c:ed:6f:ef4:a1:4e) >
  192.168.23.1 (a8:13:74:28:2d:b4)
  OP: 2 (BOOTPREPLY)
YIADDR: **192.168.23.222**
SIADDR: **192.168.23.1**
.....
OPTION: 53 ( 1) DHCP message type          5 (DHCPACK)
OPTION: 54 ( 4) DHCP Server identifier      192.168.23.1
.....
```

Listing 4.13: Ausgabe von »dhcpcdump«

Wenn Sie ein lokales Netz mittels DHCP verwalten, sollten Sie sich über aktuelle Sicherheitsprobleme auf dem Laufenden halten. Als zentraler Dienst ist DHCP auch Ziel von Schadsoftware, die die Störung oder Ausforschung Ihres Netzwerkverkehrs bezweckt.

Automatische Adressvergabe für IPv6

Ein Verfahren für die automatisierte IPv6-Adressvergabe stellt die *Stateless Address Auto-configuration* (SLAAC) dar. Die Adresse wird dabei weder zentral im Netzwerk vergeben noch gespeichert. Das betreffende Gerät erzeugt die Adresse vielmehr selbst und zieht dabei die MAC-Adresse mit heran. Mit diesem Verfahren ist es möglich, sowohl eine link-lokale als auch eine globale IPv6-Adresse zu erzeugen.

Nachdem aufgrund der Adresse auf das Gerät (MAC-Adresse) Rückschlüsse gezogen werden können, ist dieses Vorgehen an sich unsicher. Mit den *Privacy Extensions* zusammen werden zufällige MAC-Adressen erzeugt, die wiederum für die Erzeugung der IP-Adresse verwendet werden. Die so erzeugten IP-Adressen unterliegen einer Verfallszeit, sind damit temporärer Natur und wechseln regelmäßig, was eine Profilbildung zumindest erschwert. Diese Adressen werden für die Dauer ihrer Benutzung vorgehalten. Wird eine neue in der Zwischenzeit erzeugt, erhält die vorherige die Kennzeichnung *temporary deprecated* und wird nur noch für die eingehenden Pakete genutzt. Die neue Adresse wird sofort nach deren Erstellung für die danach folgenden abgehenden Verbindungen angewendet.

Um die globale IPv6-Adresse zu erstellen, erfragt das Gerät den Präfix, der vom Provider des Internetzugangs zugeteilt wird, beim nächsten Gateway (Router) ab. Für Geräte, die vom Internet her erreichbar sein müssen, eignet sich dieses Verfahren nicht.

Alternativ erfolgt die Adressvergabe im lokalen Netz per DHCP. Das Endgerät erzeugt zunächst mittels SLAAC eine link-lokale Adresse. Damit erreicht es den nächsten Router. Dieser sendet sein Router Advertisement mit *managed* zurück und signalisiert damit dem Endgerät, dass es einen DHCP-Server kontaktieren muss.

Es wird zwischen *Stateful* und *Stateless* DHCPv6 unterschieden. Erstere Version teilt die IP-Adresse, gegebenenfalls auch vorherbestimmt und mit weiteren Konfigurationsparametern (Zeitserver, Nameserver), zu (ähnlich dem DHCP-Server im IPv4). Beim *Stateless* DHCPv6 bekommt das Endgerät seine IPv6-Adresse per SLAAC, der Server teilt nur die weiteren Konfigurationsparameter mit.

Die Grundlagen dazu finden Sie in den RFCs **4862**, **7527**, **8981**, **9762** und **9915**.

4.2.4 Zeroconf

Für *Zeroconf* finden Sie keine einheitliche Einbindung in die verschiedenen Betriebssysteme:

- **Microsoft Windows:** Ist der Windows-Rechner für den Adressbezug über DHCP eingerichtet, versucht er mehrmals einen DHCP-Server zu erreichen. Schlägt dies fehl, weist er sich eine IP-Adresse aus dem für Zeroconf reservierten Bereich zu (*APIPA*).
- **Apple:** Von Apple wird die Implementierung *bonjour* genannt.
- **Linux, FreeBSD:** Hier finden Sie Zeroconf unter dem Namen *avahi*. Viele Distributionen installieren den dazugehörigen Daemon mit. Dessen Konfigurationsdatei *avahi-daemon.conf* finden Sie unter */etc/avahi*. Meist genügen die Voreinstellungen für den Betrieb. Genaue Ausführungen zu den Einträgen dieser Datei erhalten Sie mit `man avahi-daemon.conf`.

In der täglichen Netzwerkpraxis begegnet Ihnen Zeroconf, wenn etwas nicht funktioniert. Außer bei Apple-Systemen wird es meist als Notfalloption eingerichtet. Wenn Sie einen PC für DHCP-Adressbezug konfigurieren und eine Adresse aus dem Zeroconf-Bereich vorfinden, ist entweder der DHCP-Server nicht gestartet oder die Verbindung zu ihm ist gestört.

In der täglichen Arbeit können Sie Zeroconf nutzen, um ein Mini-Netzwerk mit zwei Rechnern über ein Crosskabel schnell in Betrieb zu nehmen. Aber auch hier sind Sie manchmal mit festen IP-Adressen schneller ...

4.3 Verwendung von Rechnernamen

Bei Ihrer täglichen Arbeit sprechen Sie einen Rechner selten direkt mit der IP-Adresse an, sondern über seinen Namen. Sie tippen nur noch bei Konfigurationsarbeiten im Lokale Netzwerk IP-Adressen in den Webbrowser ein. Ihr Rechner oder ein Nameserver löst mehr oder weniger unauffällig im Hintergrund die Namen in die IP-Adressen auf.

4.3.1 Der Urtyp: Adressauflösung in der »hosts«-Datei

Bevor es den Nameserver gab, pflegten die Systembetreuer eine mehr oder weniger lange *hosts-Datei*. Sie finden darin eine Tabelle, die Namen und IP-Adressen gegenüberstellt.

Sie finden die Datei bei Windows-Rechnern unter

```
%SystemRoot%\system32\drivers\etc\
```

und bei Linux und FreeBSD unter

```
/etc
```

abgelegt.

Für jede IP-Adresse dürfen Sie in die gleiche Zeile mehrere Namen eintragen. Meist finden Sie hier einen kompletten Namen (Name mit Domain und Top-Level-Domain) und anschließend den lokalen Kurznamen. Die Datei wird von oben nach unten gelesen. Beim ersten passenden Eintrag wird die dort gefundene IP-Adresse verwendet.

Die Einrichtung und Pflege einer lokalen *hosts*-Datei hat vor allem den Nachteil, dass Sie selbst die Einträge verwalten müssen. Die Verwendung dieser Datei bringt Ihnen aber auch große Vorteile:

- Rechner fragen stets zuerst die lokale *hosts*-Datei vor einem Nameserver-Zugriff ab. Wenn Sie hier oft benötigte Adressen hinterlegen, können Sie auch bei einer Störung des DNS-Servers wie gewohnt mit den Namen weiterarbeiten.
- Zusammen mit fest vergebenen lokalen Adressen erhalten Sie ein recht robustes, gegen Störungen und Angriffe gewappnetes Netz, da keine aktiven Dienste (DHCP, DNS) benötigt werden.
- Testen von Webserveranwendungen: Leiten Sie auf den Localhost (127.0.0.1) um. Sie müssen später beim Echteininsatz am Code nichts mehr ändern.
- Setzen privater »Web Sperren«. Durch die Umleitung auf die 127.0.0.1 kommen ausforschende Webseiten, Trojaner und Viren(-schleudern) nicht mehr zum Zug. Aber: Sollten Sie diese Einstellung auf den Arbeitsplätzen Ihrer Arbeitnehmer (oder Kollegen) vornehmen, achten Sie auf die aktuell gültige Rechtslage und auf Betriebsvereinbarungen! Listen mit obskuren Seiten schon im *hosts*-Format erhalten Sie im Internet.

In der Muster-*hosts*-Datei finden Sie lokale und nicht lokale Adressen sowie auf den Localhost umgeleitete Rechnernamen. Sie können daraus Ihr eigenes Muster ableiten, mit dem Sie Ihre lokalen Rechner ausstatten.

Definition localhost, zwingend

```
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Rechner lokal und Internet

```
192.168.0.34 ze4.example.com ze4
192.168.0.25 zentrale.example.com zentrale
192.168.0.54 lp
fd91:e4a5:5e03::dd05 ze4-6.example.com ze4-6
fd91:e4a5:5e03::dd54 lp-6
```

```
fd91:e4a5:5e03::dd04 zentrale-6.example.com zentrale-6
192.0.32.8      www.iana.org ia
```

Bewirkt Sperre nach außen

```
127.0.0.1      www.facebook.de
127.0.0.1      www.google-analytics.com
127.0.0.1      googleads.g.doubleclick.net
127.0.0.1      pagead.googleadsyndication.com
```

Listing 4.14: Muster für »etc/hosts«

4.3.2 Der Domain Name Server (DNS) und seine Konfiguration

Für ein umfangreicheres Netz können Sie einen Nameserver (DNS) verwenden. Mit diesem schaffen Sie sich einen zentralen Konfigurationspunkt. Im Zusammenhang mit einem DHCP-Server und einer Datenbank für die Geräteverwaltung automatisieren Sie viele einzelne Arbeitsschritte.

Für Privatanutzer und kleine Firmennetze, die die Namen ihrer wenigen Rechner in der *hosts*-Datei auflösen, reicht die Weiterleitung der DNS-Anfragen zum Internet-Provider über den DSL-Router im Normalfall aus.

Sehen Sie sich die Zusammenfassung der Vor- und Nachteile einmal an:

- Zentraler Konfigurationspunkt; Clients müssen nur einmal für den DNS-Zugriff eingestellt werden.
- Ein eigener Nameserver verhindert, dass Sie bei einer erfolglosen Anfrage auf einer »Meinten Sie ...«-Seite des Internet-Providers landen.
- Beim Ausfall des DNS-Servers des Internet-Providers können Sie trotzdem Anfragen an übergeordnete Nameserver stellen.
- Aber: Der Nameserver ist ein beliebtes Ziel für Angriffe und Ausspähungen. Sie müssen das Programm deshalb stets in der aktuellen Version betreiben.
- Anfall zusätzlichen Netzwerkverkehrs

Grundlagen des DNS

Zunächst lesen Sie hier in Kurzform alles Wichtige zum DNS: Der Nameserver führt IP-Adresse und Rechnername zusammen – weltweit wie lokal, wobei die Suche sowohl mit dem Host-Namen als auch mit der IP-Adresse möglich ist. Als Zusatznutzen unterdrückt DNS über die umgekehrte Namensauflösung unerwünschte Werbe-Mails (Spam) und ermöglicht das Setzen von Websperren und -umleitungen (analog zur *hosts*-Datei). Belegt sind die Ports UDP/TCP 53; die grundlegenden RFCs dazu sind **1034** und **1035** (Updates in RFCs 1101, 1183,

Inhalt

Geleitwort des Fachgutachters	15
Vorwort	17
1 Grundlagen moderner Netzwerke	19
1.1 Definition und Eigenschaften von Netzwerken	19
1.2 Die Netzwerkprotokollfamilie TCP/IP	22
1.3 OSI-Schichtenmodell und TCP/IP-Referenzmodell	23
1.4 Räumliche Abgrenzung von Netzwerken	26
1.5 Regel- und Nachschlagewerk für TCP/IP-Netze (RFCs)	26
1.6 Prüfungsfragen	28
2 Netzwerktechnik	29
2.1 Elektrische Netzwerkverbindungen und -standards	29
2.1.1 Netzwerke mit Koaxialkabeln	31
2.1.2 Netze mit Twisted-Pair-Kabeln	34
2.1.3 Aufbau, Bezeichnung und Kategorien von Twisted-Pair-Kabeln	35
2.1.4 Stecker- und Kabelbelegungen	39
2.1.5 Anschlusskomponenten für Twisted-Pair-Kabel	42
2.1.6 Herstellung von Kabelverbindungen mit der Schneid-Klemmtechnik (LSA)	44
2.1.7 Montage von RJ45-Steckern	47
2.1.8 Prüfen von Kabeln und Kabelverbindungen	51
2.1.9 Kennzeichnen, Suchen und Finden von Kabelverbindungen	55
2.1.10 Power over Ethernet (PoE)	58
2.2 Lichtwellenleiter, Kabel und Verbinder	59
2.2.1 Übersicht über die Netzwerkstandards mit Glasfaserkabel	61
2.2.2 Aufbau und Funktion von Glasfaserkabeln	64
2.2.3 Dauerhafte Glasfaserverbindungen	68
2.2.4 Steckverbindungen für Lichtwellenleiter	69
2.2.5 Unterschiedliche Formen der Ferrulen am Steckerende	73

2.2.6	Umgang mit der LWL-Technik	75
2.2.7	Aufbau eines einfachen Leitungs- und Kabeltesters	77
2.2.8	Prüfen von LWL-Kabeln und -Verbindungen	78
2.3	Datenübertragung per Funktechnik	79
2.3.1	WLAN (Wireless LAN, Wi-Fi)	79
2.3.2	Datenübertragung über öffentliche Funknetze	82
2.3.3	Powerline Communication (PLC)	83
2.4	Technische Anbindung von Rechnern und Netzen	84
2.5	Weitere Netzwerkkomponenten	85
2.6	Zugriffsverfahren	85
2.6.1	CSMA/CD, Kollisionserkennung	85
2.6.2	CSMA/CA, Kollisionsvermeidung	86
2.7	Prüfungsfragen	86
3	Adressierung im Netzwerk – Theorie	87
3.1	Physikalische Adresse (MAC-Adresse)	87
3.2	Ethernet-Pakete (Ethernet-Frames)	89
3.3	Zusammenführung von MAC- und IP-Adresse	91
3.3.1	Address Resolution Protocol (ARP), IPv4	91
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	93
3.4	IP-Adressen	95
3.5	IPv4-Adressen	97
3.5.1	Netzwerkklassen im IPv4	97
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	98
3.5.3	Berechnungen	101
3.5.4	Private Adressen des IPv4	104
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	104
3.5.6	Localnet und Localhost	106
3.5.7	Weitere reservierte Adressen	107
3.6	IPv6-Adressen	107
3.6.1	Adresstypen des IPv6	110
3.6.2	IPv6-Loopback-Adresse	113
3.6.3	Unspezifizierte Adresse	114
3.6.4	IPv4- in IPv6-Adressen und umgekehrt	114
3.6.5	Übergangsszenario	114
3.6.6	Kryptografisch erzeugte Adressen (CGA)	115

3.6.7	Lokale Adressen	115
3.6.8	Übersicht der Präfixe von IPv6-Adressen	116
3.6.9	Adresswahl und -benutzung	117
3.7	Internetprotokoll	117
3.7.1	Der IPv4-Header	119
3.7.2	Der IPv6-Header	120
3.8	Prüfungsfragen	122
3.8.1	Berechnungen	122
3.8.2	IP-Adressen	122
4	MAC- und IP-Adressen in der Praxis	123
4.1	MAC-Adressen	123
4.1.1	Ermitteln der MAC-Adresse	123
4.1.2	Ändern der MAC-Adresse	125
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«	126
4.1.4	ARP-Spoofing erkennen	126
4.2	IP-Adressen setzen	126
4.2.1	Netzwerkconfiguration von PCs	128
4.2.2	IP-Adressconfiguration von weiteren Netzwerkgeräten	137
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	139
4.2.4	Zeroconf	145
4.3	Verwendung von Rechnernamen	145
4.3.1	Der Urtyp: Adressauflösung in der »hosts«-Datei	145
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	147
4.3.3	Einstellungen beim Client	156
4.4	Überprüfung der Erreichbarkeit und Namensauflösung von Hosts	160
4.4.1	Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6« ...	160
4.4.2	Werkzeuge für Nameserver-Abfragen (»nslookup«, »host«, »dig«, »resolvectl query«)	162
4.4.3	DNS-Abfragen mit Netzwerkdiagnoseprogrammen mitschneiden	166
4.4.4	DNS-Caching, DNS und Sicherheitsprobleme	168
4.4.5	DNSSEC und verschlüsselte Übertragung	169
4.4.6	Einstellungen für mehr Sicherheit bei DNS-Abfragen	173

4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	175
4.5.1	Bridges – Verbinden von Netzwerkteilen	175
4.5.2	Hubs – die Sammelschiene für TP-Netze	176
4.6	Switches – Verbindungsknoten ohne Kollisionen	177
4.6.1	Funktionalität	177
4.6.2	Schleifen – Attentat oder Redundanz?	178
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)	181
4.6.4	Virtuelle Netze (VLAN)	182
4.6.5	Switch und Sicherheit	184
4.6.6	Geräteauswahl	185
4.6.7	Anzeigen und Anschlüsse am Switch	186
4.6.8	Konfiguration eines Switchs allgemein	188
4.6.9	Spanning Tree am Switch aktivieren	189
4.6.10	VLAN-Konfiguration von Switches	190
4.6.11	Konfigurationszugriff auf Switches per serieller Schnittstelle	193
4.6.12	Konfiguration von Rechnern für tagged VLANs	195
4.7	Routing – Netzwerkgrenzen überschreiten	198
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	201
4.7.2	Festlegen des Standard-Gateways	202
4.7.3	Routing-Tabelle abfragen (»netstat«)	202
4.7.4	Routenverfolgung mit »traceroute«	203
4.7.5	Route manuell hinzufügen (»route add«)	204
4.7.6	Route löschen (»route«)	206
4.8	Multicast-Routing	207
4.9	Praxisübungen	208
4.9.1	Glasfasern	208
4.9.2	TP-Verkabelung	208
4.9.3	Switches	209
4.9.4	MAC- und IP-Adressen	209
4.9.5	Namensauflösung	209
4.9.6	Routing	209
4.9.7	Sicherheit im lokalen Netz	210

5	Internet Control Message Protocol (ICMP): Steuer- und Fehlercodes übertragen	211
5.1	ICMP-Pakete (IPv4)	212
5.2	ICMPv6-Pakete	213
6	Datentransport mit TCP und UDP	217
6.1	Transmission Control Protocol (TCP)	217
6.1.1	Das TCP-Paket	217
6.1.2	TCP: Verbindungsaufbau	221
6.1.3	TCP: Transportkontrolle	222
6.1.4	TCP: Verbindungsabbau	223
6.1.5	Mit oder gegen den Datenstau: Congestion-Control-Algorithmen	224
6.1.6	Verfeinerungen für TCP	226
6.2	User Datagram Protocol (UDP)	227
6.2.1	UDP: Der UDP-Datagram-Header	227
6.3	QUIC	228
6.4	Nutzung von Services mittels Ports und Sockets	230
6.4.1	Sockets und deren Schreibweise	231
6.4.2	Übersicht über die Port-Nummern	232
6.4.3	Ports und Sicherheit	233
6.5	Die Firewall	236
6.5.1	Integration der Firewall in das Netzwerk	238
6.5.2	Regeln definieren	239
6.6	Der Proxyserver	244
6.6.1	Lokaler Proxyserver	245
6.6.2	Proxyserver als eigenständiger Netzwerkteilnehmer	245
6.6.3	Squid, ein Proxyserver	246
6.7	Port and Address Translation (PAT), Network Address Translation (NAT)	247
6.8	Praxis	249
6.8.1	Verbindungsaufbau mit geänderter Port-Nummer	249
6.8.2	Portscans zum Austesten von Sicherheitsproblemen	250
6.8.3	Schließen von Ports	251

6.9	Prüfungsfragen	252
6.9.1	TCP-Protokoll	252
6.9.2	Ports und Sockets	252
6.9.3	Firewall	253
7	Kommunikation und Sitzung	255
7.1	Dateidienste	255
7.1.1	SMB/CIFS	255
7.1.2	Grundlagen	256
7.1.3	Freigaben von Verzeichnissen und Druckern unter Windows	257
7.1.4	Samba unter Linux/FreeBSD	258
7.1.5	Die Samba-Konfigurationsdatei »smb.conf«	258
7.1.6	Testen der Konfiguration	262
7.1.7	Aufnehmen und Bearbeiten von Samba-Benutzern	263
7.1.8	Starten, Stoppen und Neustart der Samba-Dienste	263
7.1.9	Netzlaufwerk unter Windows verbinden	263
7.1.10	Client-Zugriffe unter Linux/FreeBSD	264
7.1.11	Zugriffskontrolle mit »smbstatus«	267
7.1.12	Die »net«-Befehle unter Windows	268
7.1.13	Cloud-Speicher als Ergänzung	268
7.2	Network File System (NFS)	269
7.2.1	Konfiguration des NFS-Servers	269
7.2.2	Konfiguration des NFS-Clients	271
7.3	HTTP für die Informationen im Internet	272
7.3.1	Grundlagen des HTTP-Protokolls	272
7.3.2	Serverprogramme	277
7.3.3	Client-Programme	278
7.3.4	Webbrowser und Sicherheit	279
7.4	Mail-Transport	280
7.4.1	Grundlagen des SMTP/ESMTP-Protokolls	280
7.4.2	Konfigurationshinweise	284
7.4.3	Anhänge von E-Mails, MIME, S/MIME	286
7.5	Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)	290
7.5.1	Secure Shell (SSH)	290
7.5.2	SSL und TLS	292
7.5.3	Quantensichere Verschlüsselung	293

7.5.4	Konfiguration des SSH-Servers	296
7.5.5	Konfiguration des SSH-Clients	298
7.6	Praxisübungen	298
7.6.1	HTTP, Sicherheit	298
7.6.2	E-Mail	299
7.6.3	SSH, TLS/SSL	299
8	Netzwerkanwendungen	301
8.1	Datenübertragung	301
8.1.1	File Transfer Protocol (FTP), Server	301
8.1.2	File Transfer Protocol (FTP), Clients	302
8.1.3	Benutzerkommandos für FTP- und SFTP-Sitzungen	303
8.1.4	Datentransfer mit »netread« und »netwrite«	305
8.1.5	Öffentlichen Schlüssel für SSH-Anwendungen zum Server übertragen	307
8.1.6	Secure Copy (scp), Ersatz für Remote Copy (rcp)	310
8.1.7	SSHFS: entfernte Verzeichnisse lokal nutzen	310
8.2	Aufbau eines SSH-Tunnels	313
8.3	Fernsitzungen	314
8.3.1	Telnet	314
8.3.2	Secure Shell (SSH), nur Textdarstellung	315
8.3.3	Display-Umleitung für X11-Sitzungen	315
8.3.4	SSH zur Display-Umleitung für X11	316
8.3.5	Virtual Network Computing (VNC)	318
8.3.6	X2Go (Server und Client)	320
8.3.7	Remote Desktop Protocol (RDP)	324
8.4	Telefonie-Anwendungen über Netzwerke (VoIP)	327
8.4.1	Grundlagen	327
8.4.2	Endeinrichtungen und ihre Konfiguration	331
8.4.3	Besonderheiten der Netzwerkinfrastruktur für VoIP	332
8.4.4	Sonderfall Fax: T38	333
8.4.5	Sicherheit	334
8.4.6	Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP	334
8.5	Kleiner Einstieg in Nextcloud	335
8.6	Fernwartung mit RustDesk	340

9	Netzwerkpraxis	345
9.1	Planung von Netzwerken	345
9.1.1	Bedarf ermitteln	345
9.1.2	Ermitteln des Ist-Zustands	347
9.1.3	Berücksichtigung räumlicher und baulicher Verhältnisse	348
9.1.4	Investitionssicherheit	348
9.1.5	Ausfallsicherheiten vorsehen	349
9.1.6	Zentrales oder verteiltes Switching	350
9.2	Netzwerke mit Kupferkabeln	352
9.2.1	Kabel (Cat. 5 und Cat. 7)	353
9.2.2	Anforderungen an Kabeltrassen und Installationskanäle	353
9.2.3	Dosen und Patchfelder	354
9.3	Netzwerke mit Glasfaserkabeln	356
9.3.1	Kabeltrassen für LWL-Kabel	357
9.3.2	Dosen, Stecker und Patchfelder	358
9.3.3	Medienkonverter	359
9.3.4	LWL-Multiplexer	361
9.4	Geräte für Netzwerkverbindungen und -dienste	362
9.4.1	Netzwerkarten	362
9.4.2	WLAN-Router und -Sticks	363
9.4.3	Router	364
9.4.4	Switches	370
9.4.5	Printserver	373
9.4.6	Netzwerkspeicher (NAS)	375
9.4.7	Modems für den Netzzugang	376
9.5	Einbindung externer Netzwerkteilnehmer	380
9.6	Sicherheit	380
9.6.1	Abschottung wichtiger Rechner	382
9.6.2	Netzwerkverbindung mit einem Virtual Private Network (VPN)	384
9.6.3	WLAN sicher konfigurieren	390
9.6.4	SSH-Tunnel mit PuTTY aufbauen	391
9.6.5	Sichere Konfiguration von Printservern	393
9.6.6	Sicherer E-Mail-Verkehr	395
9.6.7	Sicherer Internetzugang mit IPv6	396
9.6.8	Mit Portknocking Brute-Force-Angriffe vermeiden	397
9.6.9	Sichere DNS-Abfragen	398
9.6.10	Zero Trust – vertraue niemandem!	399

9.7	Prüf- und Diagnoseprogramme für Netzwerke	399
9.7.1	Rechtliche Hinweise	399
9.7.2	Verbindungen mit »netstat« anzeigen	400
9.7.3	Hosts und Ports mit »nmap« finden	403
9.7.4	MAC-Adressen-Inventur: netdiscover	407
9.7.5	Datenverkehr protokollieren (Wireshark, tcpdump)	408
9.7.6	Netzaktivitäten mit »darkstat« messen	410
9.7.7	Netzlast mit »fping« erzeugen	412
9.7.8	Weitere Einsatzmöglichkeiten von »fping«	412
9.7.9	Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen	415
9.7.10	Weitere Systemabfragen auf Linux-Systemen	416
9.7.11	Netzwerküberwachung im Terminal mit »NetWatch«	417
A	Fehlertafeln	421
B	Auflösungen zu den Prüfungsfragen	429
C	Glossar	435
Index		447

Index

/etc/nsswitch.conf	157
/etc/rc.conf	133
4G, LTE-Advanced	82
5G	82
5G-Stand alone, 5G-SA	83
6G	83
10 Gigabit Media Independent Interface → 10G-MII	
10Base-5	31, 33
10Base-FL	61
10GBase-ER	62
10GBase-LR	62
10GBase-LX4	62
10GBase-SR	62
10G-MII	84
100Base-FX;10G-MIIa	61
100Base-SX;10G-MIIb	61
1000Base-LX;10G-MIIId	61
1000Base-SX;10G-MIIe	61

A

Abmantler	44
Abschottung wichtiger Rechner	382
Active Directory	256
Address Resolution Protocol → ARP	
Adressierung	20, 87
<i>Hardware- und IP-Adressen</i>	87
<i>MAC-Adresse</i>	87
<i>Media Access Control</i>	87
<i>physikalische Adresse</i>	87
ADSL (Asymmetric Digital Subscriber Line)	376
All-Zero-Adresse	114
Anspleißen	70
Anwendungsschicht/Application Layer	24, 25
Anycast-Adressen	110, 111
AON (Active Optical Network)	377
Apache	277
APIPA	145
Arbeitsgruppen-Konfiguration	256

Arbeitsnetz	383
Architekturunabhängigkeit	22
ARP	91, 124
ARP-Broadcast	93
ARP-Cache	92
ARP-Spoofing	93
ARP-Spoofing, erkennen	126
Attachment Unit Interface → AUI	
Auflösungen zu den Prüfungsfragen	429
AUI	32, 84
Ausfallsicherheiten, Netzwerkplanung	349
Außenmantel	64
Auto-MDI(X)	41
Autonomes System	200
avahi	145

B

Backbone	41
BBR → Staukontrolle	
Beschaffung	
<i>Modems für den Netzzugang</i>	376
<i>NAS</i>	375
<i>Netzwerkfestplatte</i>	375
<i>Netzwerkspeicher</i>	375
<i>Printserver</i>	373
<i>Router</i>	364
<i>Switch</i>	370
Bestandsbauten, Netzwerkplanung	348
Bestandsnetze, Netzwerkplanung	353
Betriebssystemermittlung, nmap	405
Betriebsvereinbarung	382
bonjour	145
Border Gateway Protocol, BGP	200
BPDU	180
Brandabschnitt	353
Brandschott	353
Bridge	175
Bridge Protocol Data Unit → BPDU	
Bridgedevice	176

Broadcast-Domänen	98
Broadcast-MAC-Adresse	88
browseable	260
Brute-Force-Angriffe	397
Bündelader	64

C

Cache Poisoning	168
Caching Resolver	168
Canonical Format Indicator	184
Carrier Sense Multiple Access/ Collision Detection → CSMA/CD	
Carrier-Grade NAT (CGNAT)	114
Cat. 8	37
Cat. 8.1	35, 38
Cat. 8.2	35, 38
CGA	115
CheaperNet	33
Checkliste Netzwerkplanung	345
Chipsatz, Netzwerkkarte	362
Chrome	278
CIDR	98, 99
CIFS	255
Classless Inter-Domain Routing → CIDR	
Coatings	64
Codecs	329
Common Internet File System → CIFS	
Congestion-Control → Staukontrolle	
Cookies	280
create mask	260
Crimpzange	48
Cross-over-Kabel	41
CSMA/CA	86
CSMA/CD	32, 85
CUBIC → Staukontrolle	

D

darkstat	410
Darstellungsschicht/Presentation Layer	24
Datei-, Druck- und Nachrichtendienste	255
Dateiattribute	260
Datenpakete	19
Datenverkehr protokollieren	408

Default Router List	95
delv	171
Demilitarisierte Zone	237
Destination Cache	95
DHCP	139
dhcpd.conf	141
DHCP-Server	139, 141
dig	163
directory mask	260
Display-Umleitung für X11-Sitzungen	315
DMZ	237
DNS	147
DNS over HTTPS	169
DNS over TLS	169
DNS-Injection	168
DNSSEC	169
DNS-Spoofing	168
DoH	169
Domain Name Server → DNS	
Domain-Name	148
Domänen-Prinzip	256
Dosenkörper	43
DoT	169
dovecot	281
DSCP	119
Dual-Speed Hub	176
Duplicate Address Detection	93, 115
Dynamic Host Configuration Protocol → DHCP	
Dynamisches Routing	200

E

ECN	119
Edge	278
EIA/TIA T568 A	40
EIA/TIA T568 B	40
Eigenschaften von Netzwerken	
<i>Adressierung</i>	20
<i>Fehlererkennung</i>	20
<i>Fehlerkorrektur</i>	20
<i>Flusssteuerung</i>	20
<i>Netzwerkprotokoll</i>	20
<i>paketorientiert</i>	19
<i>transaktionssichernde Maßnahmen</i>	21
<i>transparent</i>	20

<i>übertragungssichernde Methoden</i>	21
<i>verbindungslos</i>	21
<i>verbindungsorientiert</i>	21
<i>Verbindungssteuerung</i>	20
Einbindung externer Netzwerkteilnehmer	380
E-Mail-Anhänge	286
Erreichbarkeit von Hosts prüfen	415
Ersatzverbindung, Switch	179
ESMTP	280
EternalBlue	256
Ethernet-Frames	89
Ethernet-Pakete	89
exim	281
Extended Simple Mail Transport Protocol → ESMTP	

F

Farbkennzeichnung/Adernfarbe	40
Fax	333
FCS	91
Fehlererkennung	20
Fehlerkorrektur	20
Fehlersuche	
1000Base-T	421
DHCP	421
Kupfernetz	421
LWL-Netz	421
Fehlertafeln	421
Fernwartung	340
Ferrule	69
File Transfer Protocol → FTP	
findsmb	264
Firefox	278
Firewall	236, 238, 382
Firewall-Regeln	239
allow	239
block	239
deny	239
drop	239
pass	239
reject	239
Flags	120
Flags in Multicast-Adressen	112
Flow Label	121
Flusssteuerung	20

fping	412
FQDN	148
Fragment-Offset	120
freeSSHd	290
Freigabe	256, 257, 266
Fremdes Wartungspersonal	381
FTP	301
aktiver Modus	302
passiver Modus	302
Verbindung beenden	304
FTP-Clients	302
FTP-Kommandos	303
FTP-Server	301
FTTB	377
FTTH	377
Fully Qualified Domain Name → FQDN	
fuser	416

G

GAN	26
Gefälschte Frames	184
Gemeinsame Nutzung einer IP-Adresse ...	201
Geräteauswahl, Switch	185
getmac	124
Gf-AP, ONT (Optical Network Termination)	378
G.fast	376
Gigabit Media Independent Interface → GMII	
Glasfaserabschnitte	75
Glasfaser-Steckverbindungen	69
Glasfasertechnik	75
Glasfaserverbindungen, dauerhafte	68
Glaskern	64
Glasmantel	64
Globale Unicast-Adressen	110
GMII	84
GPON (Gigabit Passive Optical Network)	377
Group Identifier	112

H

Halbduplex	34
Hardware-Firewall	236
Head of Line Blocking	229
Header-Prüfsumme	120

Herstellercode	87	ICMP Router Discovery	93
Hohlander	64	ICMPv6	211
Hop-Limit	121	<i>Nachrichten</i>	93
host	163	<i>Pakete</i>	213
Host to Network	25	Identifikation	120
Host-Anteil	98	IEEE 802.3at-2009	332
hosts-Datei	145	IEEE 802.3ck	35
HTML	272	IEEE-Standards	30
HTTP	272	IETF	26
<i>Apache</i>	277	IFP → Internet Fax Protokoll	
<i>Chrome</i>	278	IGMP	208
<i>Cookies</i>	280	IHL	119
<i>Edge</i>	278	Interface-ID	110, 115
<i>Firefox</i>	278	interfaces	260
<i>get</i>	273	Intermediate System to Intermediate System Protocol, IS-IS	200
<i>head</i>	273	Internet	26
<i>HTTP</i>	272	Internet Fax Protokoll	333
<i>HTTP/1.0</i>	272	Internet Group Management Protocol → IGMP	
<i>HTTP/1.1</i>	272	Internet Information Services (IIS)	278
<i>HTTP-Clients</i>	278	Internetanwendungsserver	384
<i>HTTP-Requests</i>	273	Internet-Café	280
<i>HTTPS</i>	272	Internetprotokoll	117
<i>HTTP-Statuscodes</i>	274	Internetschicht/Internet Layer	25
<i>Internet Information Services (IIS)</i>	278	Intranet	26, 236
<i>JavaScript</i>	280	Intranetzugang per Internet	380
<i>lighttpd</i>	277	Inventur-Scan	404
<i>links2</i>	279	Investitionssicherheit, Netzwerkplanung	348
<i>lynx</i>	279	ip	124
<i>Masterpasswort</i>	280	ip neigh	124
<i>nginx</i>	278	IP-Adressen	95
<i>post</i>	273	IP-Adressen setzen	
<i>Sicherheit für Webbrowser</i>	279	<i>/etc/rc.conf</i>	133
<i>Statuscode</i>	273	<i>Adresse zuweisen</i>	126
<i>trace</i>	273	<i>avahi</i>	145
HTTP-Serverprogramme	277	<i>bonjour</i>	145
Hub	85, 176	<i>Debian-Linux</i>	130
Hypertext Markup Language → HTML		<i>dhcpcd.conf</i>	141
Hypertext Transfer Protocol → HTTP		<i>DHCP-Server</i>	139
		<i>FreeBSD</i>	133
		<i>Linux</i>	130
		<i>macOS</i>	135
		<i>Netzwerkkonfiguration von PCs</i>	128
		<i>Netzwerkplanung</i>	126
		<i>Stateless Adress Autoconfiguration</i>	144
		<i>Subnetzmaske mit ipcalc</i>	127
ICMP	211		
<i>freischalten</i>	243		
<i>Meldungen</i>	211		
<i>Pakete</i>	211		
<i>Pakete (IPv4)</i>	212		

<i>weitere Netzwerkgeräten</i>	137
<i>Zeroconf</i>	145
IP-Adressen zuweisen	126
ipcalc	127
iperf3	225
IP-Protokoll	96
IPv4	91
IPv4-Adressen	97
IPv4-Header	119
IPv4-mapped IPv6-Adresse	114
IPv6	93
IPv6-Adressen	107
<i>Adresstypen</i>	110
<i>Bestandteile</i>	110
<i>Präfixe</i>	116
<i>Regeln zur Adressbenutzung</i>	117
<i>Schreibweisen</i>	108
IPv6-Header	120
IPv6-Kenndaten	108
IPv6-Loopback-Adresse	113

J

JavaScript	280
------------------	-----

K

Kabelbelegung	39
Kabelbeschriftung	55
Kabelrinne	353
Kabeltrassen für LWL-Kabel	357
Kabelverbindungen prüfen	51
Klebertechnik	70
Klimatisierung	349
Knoten	93
Koaxialkabel	31
Kollisionsbereich	177
Kollisionserkennung	85
Kollisionsvermeidung	86
Kommunikationsschicht/Session Layer	25
Kompaktader	64
Konfiguration, Switch	188
Kryptografisch erzeugte Adressen	115

L

L2TP	386
LACL	181
LACP	181
LAN	26
Laserstrahlen	75
Layer 2 Tunneling Protocol → L2TP	
LC-Stecker	71
Leitungssuchgerätesatz	56
Lichtwellenleiter	59
<i>anspleißen</i>	70
<i>Biegeradien</i>	77
<i>Bündelader</i>	64
<i>dauerhafte Glasfaserverbindungen</i>	68
<i>Eigenschaften</i>	59
<i>Ferrule</i>	69
<i>Glasfaser</i>	59
<i>Glasfaserkabel</i>	64
<i>Glasfaser-Steckverbindungen</i>	69
<i>Glaskern</i>	77
<i>Glasmantel</i>	77
<i>Gradientenindex</i>	66
<i>Hohlader</i>	64
<i>Kabel- und Leitungstester</i>	77
<i>Klebertechnik</i>	70
<i>Kompaktader</i>	64
<i>LC (LWL-Stecker)</i>	70
<i>Monomode-Faser</i>	64
<i>MTRJ (LWL-Stecker)</i>	70
<i>Multimode-Faser</i>	64
<i>Netzwerkstandards mit Glasfaserkabel</i>	61
<i>Primärcoating</i>	64
<i>Prüfen von LWL-Kabeln</i>	78
<i>SC (LWL-Stecker)</i>	70
<i>Schutz der Glasfasertechnik</i>	76
<i>Schutzmaßnahmen LWL-</i> <i>Netzwerkanlagen</i>	75
<i>ST (LWL-Stecker)</i>	70
<i>Stufenindex</i>	65
<i>Stufenindexfasern</i>	65
<i>Umgang mit LWL-Komponenten</i>	75
<i>Verletzungen durch Glasfaserteile</i>	76
<i>Vollader</i>	64
lighttpd	277
Link Aggregation	181

Link Aggregation Control Layer → LACL	
Link Aggregation Control Protocol → LACP	
Link-local Unicast-Adressen	110
links2	279
Local Internet Registry	96
local master	260
Localhost	106, 146
Logische Adressen	95
Lokale Adressen	115
Loopback-Adressen	106
LSA	43
LSA-Anlegewerkzeug	45
LSA-Verbindung herstellen	45
Isof	416
LWL-Kabel, Prüfen	78
LWL-Leitungstester	77
LWL-Multiplexer	361
LWL-Netzwerk-Anschlussdosen	358
LWL-Patchfelder	358
lynx	279

M

MAC- und IP-Adresse	91
MAC-Adressen	87, 123, 403
Absender	91
ändern	125
ARP	124
ARP-Spoofing erkennen	126
ermitteln	123
getmac	124
ip	124
ip neigh	124
manuell setzen und ändern	126
Ziel	91
macOS	135
MAC-Randomisierung	88
Mail Transport Agent → MTA	
Mail User Agent → MUA	
Mail-Transport	280
Codierungen	286
Content-Type-Eintrag	286
CRAM-MD5	281
dovecot	281
EHLO	283
E-Mail-Anhänge	286
ESMTP-Protokoll	280
exim	281
Funktionsprüfung SMTP-Server	284
HELO	283
LOGIN	281
MAIL FROM	283
MIME	286
MIME-Parts	286
MS EXCHANGE	281
MTA	280
MUA	280
multipart/mixed	287
NTLM	281
PLAIN	281
postfix	281
QUIT	283
RCPT TO	283
RSET	283
S/MIME	286
SCRAM-SHA-256	281
SMTP-Client	283
SMTP-Protokoll	280
SMTP-Relay	284
SMTP-Server	284
SSL	281
Statuscodes	283
text/html	287
text/plain	287
TLS	281
MAN	26
Masterpasswort	280
MAU	32
MDI	41
MDI-X	41
Media Access Control	87
Media Independent Interface → MII	
Medienkonverter	85, 359
Medium Attachment Unit → MAU	
Mehrfaktorauthentifizierung	399
Metrik	200
MII	84
MIME	286
MIME-Erweiterung	286
Mobilfunknetze	82
Monomode-Faser	64
MS EXCHANGE	281

MSTP	180
MTA	280
MTRJ-Stecker	71
MUA	280
Multicast-Adressen	110, 111
Multicast-Routing	207
Multimode-Faser	64, 65
Multiple Spanning Tree Protocol → MSTP	
Multiplex-Verbindungen	228

N

named.conf	150
Namensauflösung	160
Nameserver-Abfragen	162
NAPT	201
NAS-Box	137
NAT	201, 247
NAT/PAT	237
NAT64/DNS64	115
NDP	93
NDP-Caches	95
NDP-Nachrichtentypen	94
Neighbor Advertisement	93, 94
Neighbor Cache	95
Neighbor Discovery Protocol → NDP	
Neighbor Solicitation	93, 94
Neighbor Unreachability Detection	93
net-Befehle	268
NetBIOS	255
netbios name	259
NetBIOS über TCP	255
netread	305
netstat	202, 400
NetWatch	417
Network Address Port Translation → NAPT	
Network Address Translation → NAT	
Network File System (NFS)	
<i>Konfiguration des NFS-Servers</i>	269
<i>zentrale Benutzerverwaltung</i>	269
netwrite	305
Netz- und Subnetzmaske	98
Netzaktivitäten messen mit darkstat	410
Netzlast erzeugen mit fping	412
Netzlaufwerk verbinden	263
Netzmaske	97
Netzmaske berechnen	101
Netzwerk-Anschlussdosen	43, 354
Netzwerkanteil	98
Netzwerkanwendungen	301
<i>cd</i>	304
<i>Datenübertragung</i>	301
<i>Fernsitzungen</i>	314
<i>FTP</i>	301
<i>FTP- und SFTP-Sitzungen</i>	303
<i>get</i>	303
<i>lpwd</i>	304
<i>ls</i>	304
<i>mget</i>	303
<i>mput</i>	304
<i>put</i>	303
<i>pwd</i>	304
<i>RDP</i>	324
<i>scp</i>	310
<i>SSH</i>	315, 316
<i>SSHFS</i>	310
<i>SSH-Tunnel</i>	313
<i>VNC</i>	318
<i>Waypipe</i>	317
Netzwerkgrenzen überschreiten	198
Netzwerkkarten	362
Netzwerkklassen	97
Netzwerkkonfiguration von PCs	128
Netzwerkplanung	126, 345
<i>Abhängigkeit von Kundendiensten</i>	349
<i>Anforderungen an Kabeltrassen</i> <i>und Installationskanäle</i>	353
<i>Ausfallsicherheiten vorsehen</i>	349
<i>Bausubstanz</i>	348
<i>Bedarf ermitteln</i>	345
<i>Berücksichtigung räumlicher</i> <i>und baulicher Verhältnisse</i>	348
<i>Bestandsnetz</i>	353
<i>BIDI-WDM</i>	361
<i>Brandabschnitte</i>	353
<i>Brandmeldeanlage</i>	348
<i>Brandschott</i>	353
<i>Brandschutz</i>	348
<i>CWDM</i>	361
<i>Daten- und Sabotageschutz</i>	350
<i>Denkmalschutz</i>	348
<i>Dosen und Patchfelder</i>	354, 358

DWDM	361	Arbeitsnetz	383
Ermitteln des Ist-Zustandes	347	Benutzerverfolgung	396
Fachpersonal	350	Betriebsvereinbarung	382
Funktionsausfall Switch	349	eigene Rechner	381
GBIC	359	E-Mail-Verkehr	395
Grundriss	348	Firewall	382
Installationskanäle	353	fremdes Wartungspersonal	381
Investitionssicherheit	348	Ignorieren von Firmware-Updates	381
Kabel (Cat. 5 und Cat. 7)	353	Internetanwendungen	382
Kabelrinnen	353	Internetanwendungsserver	384
Kabelschaden	349	IPSec	385
Kabeltrassen	353	Kennwörter	380
Kabeltrassen für LWL-Kabel	357	L2TP	386
Klimatisierung	348, 349	Mehrfaktorauthentifizierung	399
Leerrohre	349	OpenVPN	385
LWL-Kabel und Stromleitungen	356	Proxyserver	382
LWL-Multiplexer	361	Radius-Server	390
managebare Switches	352	Schadsoftware	381
Medienkonverter	359	Sicherheitsprobleme	380
minimale Biegeradien LWL	357	Sicherheitsregeln	380
Netzwerke mit Glasfaserkabeln	356	Sicherheits-Updates	381
Netzwerke mit Kupferkabeln	352	Soziale Netzwerke	381
Neuinstallation	353	SSH-Tunnel mit PuTTY	391
Notfallpläne	350	SSL	385
Potenzialunterschied	353	Tracking	396
Redundanter Internetzugang	350	Tunnel	385
SFP	359	Verteilen von Anwendungen	383
Sicherheit	348	VPN	384
Spleißbox	357	VPN-Router	385
Stromausfall	349	Wartungsnetz	383
Stromversorgung	348	WLAN sicher konfigurieren	390
Switching, zentral oder verteilt	350	WLAN-Verschlüsselung	390
Telefonnetz	348	Zero Trust	399
Trunking-Verbindungen	352	Zugriffsregelungen	381
verteilte Unterbringung der Switches	351	Netzwerkstandards	29
VoIP	349	10Base-2	33
WWDM	361	10Base-5	31
XFP	359	10Base-FL	61
Zutrittskontrolle	348	10GBase-ER	62
Netzwerkprobleme	211, 225	10GBase-LR	62
Netzwerkprotokollfamilie TCP/IP	22	10GBase-LX4	62
Netzwerkschrank	42	10GBase-SR	62
Netzwerksegment	89	100Base-FX	61
Netzwerksicherheit		100Base-SX	61
Abschottung wichtiger Rechner	382	1000Base-LX	61
allgemeine Maßnahmen	381	1000Base-SX	61

AUI	32
Auto-MDI(X)	41
BNC	33
Cheapernet	33
Cross-over-Kabel	41
CSMA/CD	32
EIA/TIA-568B	41
Farbkennzeichnung/Adernfarbe	40
Folienschirm	36
Geflechtsschirm	36
Glasfasernetzwerke	61
Halbduplex	34
IEEE-Standards	30
Kabelkategorien	37
Koaxialkabel	31
LSA-Verbindung herstellen	45
MAU	32
MDI	41
MDI-X	41
PoE	58
Quad Pair	37
RJ45	34
Thicknet	31
Thin Wire Ethernet	32
Transceiver	32
Twisted Pair	37
Twisted-Pair-Kabel	34
ungeschirmt	36
Verkabelungsbezeichnungen	30
Vollduplex	34
Western-Stecker	34
WLAN	31
Yellow Cable	31
Netzwerktester	52
Netzwerküberwachung mit NetWatch	417
Netzzugangsschicht/Link Layer	25
Netzzugriff	248
Next Header	121
Nextcloud	335
NFS → Network File System (NFS)	
NFS-Server	269
nginx	278
nmap	233, 250, 403
nmbd	258
nslookup	163
Nutzdaten	91

O

OLT (Optical Line Termination)	378
Open Shortest Path First, OSPF	200
OpenSSH	290
OpenVPN	385
oping	415
OSI-Schichtenmodell	23
Anwendungsschicht/Application Layer	24
Darstellungsschicht/Presentation Layer ..	24
Kommunikationsschicht/Session Layer ...	25
physikalische Schicht/Physical Layer	23, 25
Sicherheitsschicht/Data Link Layer	25
Transportschicht/Transport Layer	25
Vermittlungsschicht/Network Layer	25

P

Pad	91
Padding	120
Paketorientierung	19
PAN	26
PAT	201, 247
Patchfeld	42
Patchkabel	42
Payload Length	121
Personal Firewall	236
Physikalische Adresse	87
Physikalische Schicht/Physical Layer	25
ping	160, 211, 415
ping6	160, 415
Plain SMB über TCP	255
PLC	83
PoE	58, 332
Port and Address Translation → PAT	
Port Trunking	181
Portknocking	397
Port-Nummern	
abweichende	249
Übersicht	232
Ports	230
schließen	251
Sicherheit	233
Ports und Sockets	230
/etc/services	232

<i>geschlossener Port</i>	235
<i>netstat</i>	235
<i>offener Port</i>	235
<i>Port-Nummer</i>	230
<i>Ports und Sicherheit</i>	233
<i>Portscanner</i>	233
<i>Port-Unreachable-Meldung</i>	235
<i>registered Ports</i>	232
<i>Schreibweise Sockets</i>	231
<i>Standard-Port-Nummern</i>	230
<i>Übersicht über die Port-Nummern</i>	232
<i>UDP-Portscans</i>	235
<i>Well-known-Ports</i>	232
Portscanner	233, 250
Port-Unreachable-Meldung	235
postfix	281
Potenzialunterschied	353
Power over Ethernet → PoE	
Powerline-Communication → PLC	
Präambel	91
Präfix	110
Prefix List	95
Primary Nameserver	149
Printserver	137
Private IPv4-Adressen	104
Proxyserver	244, 382
<i>als eigenständiger Netzwerkteilnehmer</i>	245
<i>Dedicated Proxyserver</i>	244
<i>generischer</i>	244
<i>lokaler</i>	245
<i>Reverse Proxyserver</i>	245
<i>transparenter</i>	244
Prüf- und Diagnoseprogramme	399
Public-Key-Authentifizierung	290
PuTTY	290

Q

QoS	332, 333
Quality of Service → QoS	
Quantensichere Verschlüsselung	293
Quarantäneverzeichnis	384
QUIC	228, 277
<i>Head of Line Blocking</i>	229
<i>Multiplex-Verbindungen</i>	228

R

Radius-Server	390
Rapid Spanning Tree Protocol → RSTP	
RARP	92
Raspberry Pi	321
Raumanbindung	349
RDP	324
Rechnernamen	145
<i>\$ORIGIN</i>	153
<i>\$TTL</i>	153
<i>/etc/nsswitch.conf</i>	157
<i>A</i>	152
<i>AAAA</i>	152
<i>autoritativ</i>	149
<i>Caching-only-Nameserver</i>	149
<i>CNAME</i>	152
<i>DHCP-Server</i>	156
<i>dig</i>	163
<i>DNS</i>	147
<i>Domain-Name</i>	148
<i>Einstellungen beim Client</i>	156
<i>FQDN</i>	148
<i>host</i>	163
<i>IN</i>	153
<i>localhost</i>	146
<i>MX</i>	152
<i>Namensauflösung</i>	145, 160
<i>Nameserver-Abfragen</i>	162
<i>NS</i>	152
<i>nslookup</i>	163
<i>ping</i>	160
<i>ping6</i>	160
<i>Primary Nameserver</i>	149
<i>PTR</i>	152
<i>resolvectl</i>	165
<i>Reverse-Zone</i>	153
<i>Rückwärtssuche</i>	153
<i>Secondary Nameserver</i>	149
<i>Second-Level-Domain</i>	148
<i>Subdomain</i>	148
<i>tcpdump</i>	166
<i>TLD</i>	148
<i>Top-Level-Domain</i>	148
<i>Vorwärtssuche</i>	153
<i>Windows-Clients</i>	156

Rechtliche Hinweise	399
Redirect Message	94
Remote Desktop Protocol → RDP	
RENO → Staukontrolle	
Repeater	85
reservierte IPv4-Adressen	107
resolvectl	165
RESTful Webservices	273
RFC-Dokumentenstatus	26
RFCs	26
<i>Elective</i>	28
<i>Experimental</i>	27
<i>Informational</i>	27
<i>Internet Standard</i>	27
<i>Limited Use</i>	28
<i>May</i>	28
<i>Must</i>	27
<i>Must not</i>	27
<i>Not Recommended</i>	27
<i>Proposed Standard</i>	27
<i>Recommended</i>	27
<i>Required</i>	27
<i>Shall</i>	27
<i>Shall not</i>	27
<i>Should</i>	27
<i>Should not</i>	27
RG-58	33
RIPE NCC	96
RJ45	34
RJ45-Stecker montieren	47
Root-Bridge	180
Round Trip	229
route	204
Route löschen	206
Route manuell hinzufügen	204
Routenverfolgung	203
Router Advertisement	94
Router Solicitation	94
Routing	198
<i>Allgemeines</i>	200
<i>autonomes System</i>	200
<i>BGP</i>	200
<i>dynamisches Routing</i>	200
<i>gemeinsame Nutzung einer IP-Adresse</i>	201
<i>ICMP</i>	198
<i>IGMP</i>	198

IS-IS	201
Metrik	200
Multicast-Routing	207
NAPT	201
netstat	202
OSPF	201
PAT	201
RIP	201
route	204
Route löschen	206
Route manuell hinzufügen	204
Routenverfolgung mit traceroute	203
Routing-Tabelle abfragen	202
Standard-Gateway	200, 202
Standard-Route	200
Standard-Router	200
statisches Routing	200
Routing Information Protocol, RIP	200
Routing-Tabelle abfragen	202
RRSIG	170
RSTP	180
RTCP	327
RTP	327
Rückwärtssuche	153
RustDesk	340

S

S/MIME	286
Safari	278
Samba-Benutzer	263
Samba-Konfigurationsdatei	258
<i>global</i>	258
<i>homes</i>	258
<i>printers</i>	258
<i>profiles</i>	258
<i>shares</i>	258
Schadsoftware	381
Schirmgeflecht	44
Schleifen, Switch	178
Schleifstaub	75
Schluckwiderstand	31
Schneid-Klemmtechnik	43, 44
Schutz der Glasfasertechnik	76
Scope-Feld	112
scp	310

SC-Stecker	71	SMB	255
SDSL (Symmetric Digital Subscriber Line)	376	<i>smbclient</i>	264
Secondary Nameserver	149	<i>smb.conf</i>	258
Second-Level-Domain	148	<i>smbd</i>	258
Secure Copy → scp		<i>smbstatus</i>	267
Secure Neighbor Discovery	115	<i>Testen der Konfiguration</i>	262
Secure Shell → SSH		<i>testparm</i>	262
Serielle Schnittstelle, Switch	193	<i>User</i>	256
Server Message Block → SMB		<i>smbclient</i>	264
SFD	91	SMB-Client-Zugriffe unter Linux/FreeBSD	264
Share	256	<i>smb.conf</i>	258
Shell-Skript, fping	412	<i>smbd</i>	258
Sicherheitsprobleme	250, 380	<i>smbstatus</i>	267
Sicherheitsregeln	380	SMTP	280
Sicherheits-Updates	381	SMTP-Auth	281
Sicherungsschicht/Data Link Layer	25	SMTP-Client	283
Simple Mail Transport Protocol → SMTP		SMTP-Server, Konfiguration	284
Singlemode-Faser → Monomode-Faser		Sockets	230, 231
SIP	327	Soziale Netzwerke	381
SIPS	334	Spanning Tree	189
Site-local Unicast-Adressen	115	Spanning Tree Protocol → STP	
SLAAC	144	Squid	246
SMB	255	SRTP	334
SMB/CIFS	255	ss	402
<i>Active Directory</i>	256	SSH	290, 315
<i>Arbeitsgruppen-Konfiguration</i>	256	<i>Anwendung</i>	291
<i>Aufnehmen und Bearbeiten von</i>		<i>Display-Umleitung</i>	316
<i>Samba-Benutzern</i>	263	<i>Fernsitzung</i>	315
CIFS	255	SSH-Client	298
Client-Zugriffe unter Linux/FreeBSD	264	ssh-copy-id	307
Dateiattribute	260	SSHFS	310
Domänen-Prinzip	256	SSH-Key	290
<i>findsmb</i>	264	SSH-Server	296
<i>Freigaben von Verzeichnissen und</i>		SSH-Tunnel	313
<i>Druckern unter Windows</i>	257	SSH-Tunnel mit PuTTY aufbauen	391
GNOME-Oberfläche	266	SSL	292
Grundlagen	256	SSL Alert Protocol	292
Linux/FreeBSD	258	SSL Application Data Protocol	292
<i>net-Befehle für Windows</i>	268	SSL Change Cipher Specification Protocol	292
NetBIOS	255	SSL Handshake Protocol	292
NetBIOS über TCP	255	SSL Record Protocol	292
Netzlaufwerk verbinden	263	Standard-Gateway	200, 202
<i>nmbd</i>	258	Standard-Route	200
Plain SMB über TCP	255	Standard-Router	200
<i>Samba-Daemon</i>	263	Stateful-Packet-Inspection	237
<i>Samba-Konfigurationsdatei</i>	258	Statisches Routing	200
Share	256		

Statuscode	273
Staukontrolle	224
Store-and-Forward-Bridging	176
STP	179, 184
ST-Stecker	71
Stufenindexfasern	65
STUN	327
STUN-Server	330
Subdomain	148
Subnet-ID	110
Subnetzmaske berechnen	127
Switch	177
Angriffspunkte	184
Anzeigen und Anschlüsse	186
Beschaffung	370
CFI	184
dynamisches VLAN	184
Ersatzverbindung	179
Ersteinrichtung	188
Funktionalität	177
Geräteauswahl	185
Kollisionsbereich	177
Konfiguration	188
LACL	181
LACP	181
Link Aggregation	181
MSTP	180
paketbasiertes VLAN	183
Port Trunking	181
portbasiertes VLAN	182
Rechnerkonfiguration für tagged VLAN	195
Root-Bridge	180
RSTP	180
Schleifen	178
serielle Konfiguration	193
Spanning Tree aktivieren	189
statisches VLAN	184
STP	179
tagged VLAN	183
TPID	183
Verbindungsabbrüche	180
verteilte Unterbringung	351
VID	184

virtuelle Netze	182
VLAN	182
VLAN-Konfiguration	190, 195, 196, 198
zentrale Unterbringung	350
systemd-resolved	106

T

T38	333
Tag Protocol Identifier	183
tagged VLAN	183, 195
TCP	217
TCP/IP-Referenzmodell	23
Anwendungsschicht/Application Layer	25
Internetschicht/Internet Layer	25
Netzzugangsschicht/Link Layer	25
Transportschicht/Transport Layer	25
TCP-Datagramm	217
tcpdump	166, 408
TCP-Erweiterungen	226
TCP-Paket	217
ACK	219
Aufbau	217
CWR	219
ECE	219
FIN	220
Flags, Steuerungsbits	219
PSH	220
RST	220
SYN	220
URG	219
TCP-Transportkontrolle	222
TCP-Verbindungssabbau	221, 223
Technische Anbindung	84
Teilsegmente	101
Terminalserver-Projekt	320
testparm	262
Thicknet	31
Thin Wire Ethernet	32
TLD	148
TLS	292
Top-Level-Domain → TLD	
TP-Netze	
Crimpzange	48
Dosenkörper	43
Leitungssuchgeräte	56

LSA	43, 44
LSA-Anlegewerkzeug	45
Netzwerk-Anschlussdose	43
Netzwerktester	52
PoE	58
Prüfen der Kabelverbindung	51
RJ45-Stecker montieren	47
Schneid-Klemmtechnik	43, 44
traceroute	203
Traffic Class	121
Transaktionssicherung	21
Transceiver	32
Transmission Control Protocol → TCP	
Transportschicht/Transport Layer	25
Trunking-Port, ungesicherter	184
Trunking-Verbindungen	352
TTL	120
Tunnel	237, 334
Twisted-Pair-Kabel, Aufbau	35
Typ	91

U

Überlauf, Switch	184
Übertragungssicherung	21
UDP	227
UDP-Datagramm-Header	227
UDP-Lite	228
UDP-Portscans	235
Unicast-Adressen	110
Unique-local Unicast-Adressen	115
Unspezifizierte Adresse	114
USB-WLAN-Stick	363
User	256
User Datagram Protocol → UDP	

V

VDSL2 (Very High-Speed Digital Subscriber Line 2)	376
Verbindungslos	21
Verbindungsorientiert	21
Verbindungssteuerung	20
Verkabelungsbezeichnungen	30
Verkabelungstechnik	349

Vermittlungsschicht/Network Layer	25
Verschlüsselung	
Authentifizierung	290
SSH-Key	290
SSL	292
SSL Alert Protocol	292
SSL Application Data Protocol	292
SSL Change Cipher Specification	292
SSL Handshake Protocol	292
SSL Record Protocol	292
TLS	292
Verschlüsselungsarten	290
Version	119
Virtual Network Computing → VNC	
Virtual Private Network → VPN	
Virtuelle Netze	182
Vivaldi	278
VLAN	90, 182
dynamisches	184
paketbasiertes	183
portbasiertes	182
statisches	184
VLAN Identifier	184
VLAN-Konfiguration	190
FreeBSD	195
Linux	196
Windows	198
VLAN-Tag	90, 183
VNC	318
VoIP	327, 330
Vollader	64
Vollduplex	34
Vollduplex-Betrieb, Switch	177
Vorwärtssuche	153
VPN	334, 384
VPN-Router	385
VXLAN	198

W

w3m	279
WAN	26
WannaCry	256
Wartungsnetz	383
Waypipe	317
Webbrowser und Sicherheit	279

WebDAV	273
WebRTC	330
Wechsel der Benutzerkennwörter	381
Western-Stecker	34, 41
wins support	260
wireshark	408
WLAN	31, 79
WLAN sicher konfigurieren	390
WLAN-Router	363
WLAN-Standards	81
WLAN-Stick	363
WLAN-Zugangsgerät	176
workgroup	259

X

x2golistsessions_root	322
x2goterminate-session	323
XGS-GPON (10 Gigabit Passive Optical Network)	378

Y

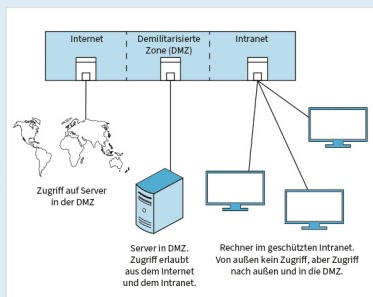
Yellow Cable	31
--------------------	----

Z

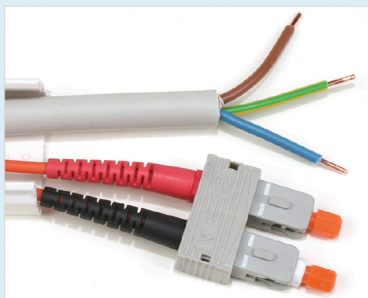
Zentrale Datenhaltung	375
Zero Trust	399
Zeroconf	104, 105, 145
Zugdosen	349
Zugriffsregelungen	381
Zugriffsverfahren	85
<i>Clear-to-Send-Signal</i>	86
CSMA/CA	86
CSMA/CD	85
JAM-Signal	85
Kollisionserkennung	85
Kollisionsvermeidung	86
Request-to-send-Signal	86

Alles, was Sie über Netzwerktechnik wissen sollten

Netzwerk-Praxis ist zentraler Bestandteil der IT-Ausbildung. Auch im Informatikstudium gehört das Wissen um OSI-Modell und Datentransfer zum Handwerk dazu. In diesem Standardwerk finden Sie alles Wichtige zu Planung, Aufbau und zum sicheren Betrieb von IT-Netzwerken.



Lernen und nachschlagen



Verkabelung, Stecker, Hardware

```
-> traceroute <www.rheinwerk-verlag.de>
HOST: DNSChecker.org
  1. |---| 100.0 3
  2. |---| 10.74.132.49 0.0% 3
  3. |---| 138.197.248.254 0.0% 3
  4. |---| 143.244.192.172 0.0% 3
  5. |---| 143.244.225.216 0.0% 3
  6. |---| 143.244.225.143 0.0% 3
  7. |---| nylx.retn.net (196.32.168.182) 0.0% 3
  8. |---| as2-11.it.ics.fht.de.xsln.net (87.245.232.253) 0.0% 3
  9. |---| ??? 100.0 3
 10. |---| fra11.ccl.ash8314.net (45.91.100.239) 0.0% 3
 11. |---| fra11.ccl.ash8314.net (45.91.100.22) 0.0% 3
 12. |---| 103.241.48.3 0.0% 3

-> ping 103.241.48.3
PING 103.241.48.3 (103.241.48.3) 56(84) bytes of data.
 64 bytes from 103.241.48.3: icmp_seq=1 ttl=58 time=15.1 ms
 64 bytes from 103.241.48.3: icmp_seq=2 ttl=58 time=14.5 ms
 64 bytes from 103.241.48.3: icmp_seq=3 ttl=58 time=14.3 ms
 64 bytes from 103.241.48.3: icmp_seq=4 ttl=58 time=14.2 ms
```

Praxiswissen und Beispiele

Netzwerktechnik: Theorie und Praxis

Alle Grundlagen in einem Buch: von MAC-, IPv4- und IPv6-Adressen über Netzmasken, DNS und Adressumsetzungen bis zu Datentransport mit TCP und UDP, Protokollen, Ports oder Sockets.

Netzwerke planen, aufbauen und betreiben

Ist Glasfaser oder Kupfer für Ihr Szenario besser geeignet? Wie konfigurieren Sie Switches oder Router? Was müssen Sie bei der Planung von Kabeltrassen beachten und wie sorgen Sie umfassend für Sicherheit in Ihrem Netzwerk? Hier finden Sie konkrete Lösungen.

Für Ausbildung und Selbststudium

Praxisbeispiele, Anleitungen, Fehlertafeln, Netzwerk-Glossar, RFCs und Übungsaufgaben mit Lösungen: Zahlreiche Hilfsmittel unterstützen Fachinformatiker, Administratorinnen und IT-Fachleute im Selbststudium, in der Ausbildung und im Beruf.



Harald Zisler ist seit über 30 Jahren in der IT tätig und beschäftigt sich in Theorie und Praxis mit Computer-Netzwerken. Regelmäßig publiziert er zu Themen aus der IT sowie Kommunikationstechnik und befasst sich mit FreeBSD, Linux, Datenschutz und Datensicherheit.

Auf einen Blick

Wichtige Grundlagen

TCP/IP, Ports, MAC-Adressen
IPv4- und IPv6-Adressen
Internetprotokolle
DHCP, Routing, Adressierung
Virtuelle Netze (VLAN)
Datei-, Druck- und Nachrichtendienste, PAT/NAT

Netzwerktechnik

Lichtwellenleiter, Kabel und Verbinder
Funktechnik, WLAN, VoIP
Switches, Bridges, Hubs, Router
Netzwerkarten, Printserver, Netzwerkspeicher

Praxis

Netzwerkplanung und -aufbau
Firewall und Proxies

