



Unternehmen für Bildung.

IT - Berufe

Software

Modul:

**J – Netzwerk &
Protokolle Teil 2**

Version:

1.0

Januar 2019

Berufsfortbildungswerk GmbH (bfw)

Geschäftsbereich Ost

Berufsbildungsstätte Leipzig
Hohmannstraße 6
04129 Leipzig

Modul: **J – Netzwerke & Protokolle**

Version, Datum: 1.0 Januar 2019

Berufsfortbildungswerk GmbH (bfw)
Geschäftsbereich Ost

Berufsbildungsstätte Leipzig
Hohmannstraße 6 04129 Leipzig

Alle Rechte vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung des Herausgebers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Die Modulunterlage und alle ihre Bestandteile wurden mit großer Sorgfalt erstellt und geprüft. Dennoch können Fehler nicht vollkommen ausgeschlossen werden. Der Herausgeber und die Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Literaturhinweis

Titel: **Computer-Netzwerke – Grundlagen, Funktionsweise, Anwendung**

ISBN: ISBN 978-3-8362-4323-0

Verlag: Rheinwerkverlag

Inhalt

Kapitel 7	6
Kommunikation und Sitzung	6
7.1 SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	6
7.1.1 Grundlagen.....	6
7.1.2 Freigaben von Verzeichnissen und Druckern unter Windows.....	7
7.1.3 »nmbd« und »smbd« unter Linux/FreeBSD.....	8
7.1.4 Die Samba-Konfigurationsdatei »smb.conf«	8
7.1.5 Testen der Konfiguration	11
7.1.6 Aufnehmen und Bearbeiten von Samba-Benutzern	11
7.1.7 Starten, Stoppen und Neustart der Samba-Daemons	12
7.1.8 Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10).....	12
7.1.9 Client-Zugriffe unter Linux/FreeBSD	13
7.1.10 Zugriffskontrolle mit »smbstatus«	15
7.1.11 Die »net«-Befehle für die Windows-Batchprogrammierung.....	16
7.2 Network File System (NFS)	16
7.2.1 Konfiguration des NFS-Servers.....	17
7.2.2 Konfiguration des NFS-Clients.....	19
7.3 HTTP für die Informationen im Internet	20
7.3.1 Grundlagen des HTTP-Protokolls	20
7.3.2 Serverprogramme	23
7.3.3 Client-Programme	24
7.3.4 Webbrowser und Sicherheit	25
7.4 Mail-Transport	26
7.4.1 Grundlagen des SMTP/ESMTP-Protokolls.....	26
7.4.2 Konfigurationshinweise.....	29
7.4.3 Anhänge von E-Mails, MIME, S/MIME	30
7.5 Secure Shell (SSH) und Secure Socket Layer (SSL),.....	33
Transport Layer Security (TLS)	33
7.5.1 Secure Shell (SSH).....	33
7.5.2 SSL und TLS.....	34
7.6 Praxisübungen.....	35
7.6.1 Konfiguration des Samba-Servers	35
7.6.2 NFS-Server.....	35
7.6.3 HTTP, Sicherheit	35
7.6.4 E-Mail	35

Kapitel 8	36
Standards für den Datenaustausch Tag 1 - 5	36
Kapitel 9 - Netzerkanwendungen.....	40
9.1 Datenübertragung.....	40
9.1.1 File Transfer Protocol (FTP), Server.....	41
9.1.2 File Transfer Protocol (FTP), Clients	41
9.1.3 Benutzerkommandos für FTP- und SFTP-Sitzungen.....	42
9.1.4 Datentransfer mit »netread« und »netwrite«	44
9.1.5 Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat«	46
9.1.6 Secure Copy (scp), Ersatz für Remote Copy (rcp).....	46
9.1.7 SSHFS: entfernte Verzeichnisse lokal nutzen	47
9.2 SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der	48
Sicherheit oder zur kennwortfreien Anmeldung	48
9.3 Aufbau eines SSH-Tunnels.....	50
9.4 Fernsitzungen	51
9.4.1 Telnet	51
9.4.2 Secure Shell (SSH), nur Textdarstellung	51
9.4.3 Display-Umleitung für X11-Sitzungen	52
9.4.4 SSH zur Display-Umleitung für X11	52
9.4.5 Virtual Network Computing (VNC)	53
9.4.6 X2Go (Server und Client)	55
9.5 Telefonie-Anwendungen über Netzwerke (VoIP)	66
9.5.1 Grundlagen.....	66
9.5.2 Endeinrichtungen und ihre Konfiguration.....	69
9.5.3 Besonderheiten der Netzwerkinfrastruktur für VoIP	70
9.5.4 Sonderfall Fax: T38.....	70
9.5.5 Sicherheit	70
9.5.6 Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP	71
9.5.7 Remote Desktop Protocol (RDP)	71
Kapitel 10	72
Netzwerkpraxis.....	72
10.1 Planung von Netzwerken	72
10.1.1 Bedarf ermitteln	72
10.1.2 Ermitteln des Ist-Zustands	74
10.1.3 Berücksichtigung räumlicher und baulicher Verhältnisse.....	74
10.1.4 Investitionssicherheit	74

10.1.5 Ausfallsicherheiten vorsehen.....	75
10.1.6 Zentrales oder verteiltes Switching.....	75
10.2 Netzwerke mit Kupferkabeln	77
10.2.1 Kabel (Cat. 5 und Cat. 7).....	77
10.2.2 Anforderungen an Kabeltrassen und Installationskanäle	77
10.2.3 Dosen und Patchfelder.....	79
10.3 Netzwerke mit Glasfaserkabeln	80
10.3.1 Kabeltrassen für LWL-Kabel	81
10.3.2 Dosen und Patchfelder.....	81
10.3.3 Medienkonverter	82
10.3.4 LWL-Multiplexer.....	82
10.4 Geräte für Netzwerkverbindungen und -dienste.....	82
10.4.1 Netzwerkkarten.....	82
10.4.2 WLAN-Router und -Sticks.....	83
10.4.4 Switches	100
10.4.5 Printserver.....	101
10.4.6 Netzwerkspeicher (NAS)	102
10.4.7 Modems für den Netzzugang.....	103
10.5 Einbindung externer Netzwerkteilnehmer	105
10.6 Sicherheit Tag 5 - 10.....	105
10.6.1 Abschottung wichtiger Rechner	106
10.6.2 Netzwerkverbindung mit einem Virtual Private Network (VPN)	108
10.6.3 WLAN sicher konfigurieren	113
10.6.4 SSH-Tunnel mit PuTTY aufbauen.....	113
10.6.5 Sichere Konfiguration von Printservern	116
10.6.7 Sicherer Internetzugang mit IPv6.....	121
10.6.8 Mit Portknocking Brute Force-Angriffe vermeiden	122
10.7 Prüf- und Diagnoseprogramme für Netzwerke.....	124
10.7.1 Rechtliche Hinweise	124
10.7.2 Verbindungen mit »netstat« anzeigen	124

Kapitel 7

Kommunikation und Sitzung

Mit dem reinen Übertragen von Daten schaffen Sie noch keine Kommunikation. Ihre Rechner brauchen hierfür Sende- und Empfangsprogramme. Der Transfer von Dateien und E-Mails, das Arbeiten am entfernten Arbeitsplatz oder einfach das Anschauen von Webseiten bilden die Kommunikation im Internet.

7.1 SMB/CIFS (Datei-, Druck- und Nachrichtendienste)

Das Netzwerk-Dateisystem SMB/CIFS begegnet Ihnen oft im Zusammenhang mit Bürocomputern. Damit können Sie schnell Daten zwischen PCs austauschen und Drucker gemeinsam nutzen.

SMB/CIFS

- ▶ **Einsatzbereich:** Büroumgebungen mit MS-DOS- und MS-Windows-PCs sowie Linux- und Unix-Rechnern, Datenaustausch und gemeinsame Druckernutzung
- ▶ **SMB:** *Server Message Block*
- ▶ **CIFS:** *Common Internet File System*
- ▶ **NetBIOS:** Programmierschnittstelle, die unter anderem eine eigene Namensauflösung (ohne DNS) beinhaltet (»NetBIOS-Name«)
- ▶ **Umsetzungen:** MS-DOS, Microsoft Windows, Samba (Unix, Linux), LAN-Server (IBM)
- ▶ **Port-Nummern ältere Version, NetBIOS über TCP:** 137 (NetBIOS-Namensauflösung), 138 (Datagramm-Service), 139 (Session Service)
- ▶ **Port-Nummer neuere Version, Plain SMB über TCP:** 445
- ▶ **Vorteile:** verbreitet, relativ unkompliziert in der Handhabung
- ▶ **Nachteile:** keine Verschlüsselung
- ▶ **RFCs:** 1001, 1002, 1088, 2097, Internet-Draft:
<http://datatracker.ietf.org/doc/draft-palanivelan-netbios-smb/>

Zudem finden Sie weitere Funktionen je nach Windows-Version:

- Domänen-Prinzip (ab Windows NT): zentrale Benutzerverwaltung und Anmeldung
- Active Directory: Verzeichnisdienst des Microsoft Windows Servers, ermöglicht die
- Abbildung von organisatorischen Einteilungen eines Betriebs auf Zugriffs- und Nutzungsrechte
- Arbeitsgruppe: Zusammenfassung mehrerer Rechner ohne zentrale Administration
- (Benutzer, Anmeldung)

7.1.1 Grundlagen

Am häufigsten werden Sie SMB im Zusammenhang mit der Arbeitsgruppen-Konfiguration antreffen. Aus diesem Grund behandle ich diese hier ausführlicher. NT-Domänen oder Active Directories werden Sie meist in reinen Windows-Umgebungen finden,

in denen der Server selbst durchaus mit Linux oder FreeBSD laufen kann. Das Samba-Paket beherrscht alle drei Verwaltungsmodi (Arbeitsgruppe, NT-Domäne, Active Directory).

Im Arbeitsgruppen-Modus wählen Sie zwischen zwei Freigabe-Modi: *Share* (Freigabe) und *User* (Benutzer). Geben Sie ein Share frei, vergeben Sie für das freigegebene Objekt (Verzeichnis oder Drucker) ein Kennwort. Dieses müssen Sie allen Benutzern mitteilen, die auf die Freigabe zugreifen sollen. Solange Sie nur wenige zentrale Rechner mit Freigaben vorhalten, können Sie dies übersichtlich administrieren.

Geben Sie auf User-Ebene frei, müssen Sie die Benutzer gegebenenfalls mehrfach auf verschiedenen Rechnern anlegen. Änderungen von Kennwörtern oder das Löschen von Benutzern müssen Sie dann ebenso auf allen betroffenen Geräten durchführen. Dieses Vorgehen eignet sich damit nur für kleine Netze. Alle Rechner müssen zudem derselben Arbeitsgruppe angehören.

7.1.2 Freigaben von Verzeichnissen und Druckern unter Windows

Damit Sie andere Benutzer auf eine Ressource (Verzeichnisse, Drucker) zugreifen lassen können, müssen Sie eine Freigabe erteilen. Unter Windows funktioniert das meist mit einem rechten Mausklick auf das Objekt (Eigenschaftenmenü) bzw. einem Klick in die Symbolleiste auf Freigeben für (Abbildung 7.1).

Anschließend können Sie genaue Einstellungen vornehmen. Klicken Sie auf den kleinen Auswahlpfeil, um die Ressource Benutzern oder einer Gruppe zuzuordnen. Sie legen fest, wer was mit dem Objekt machen darf (Abbildung 7.2).

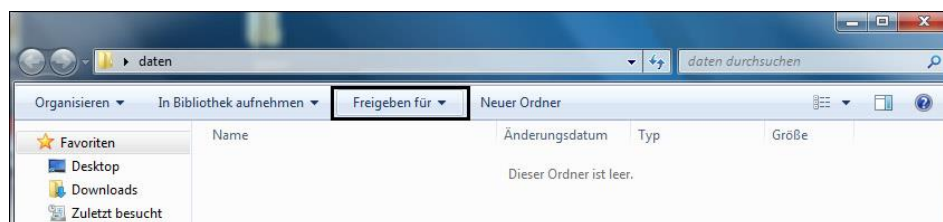


Abbildung 7.1 Menüpunkt »Freigeben für« wählen

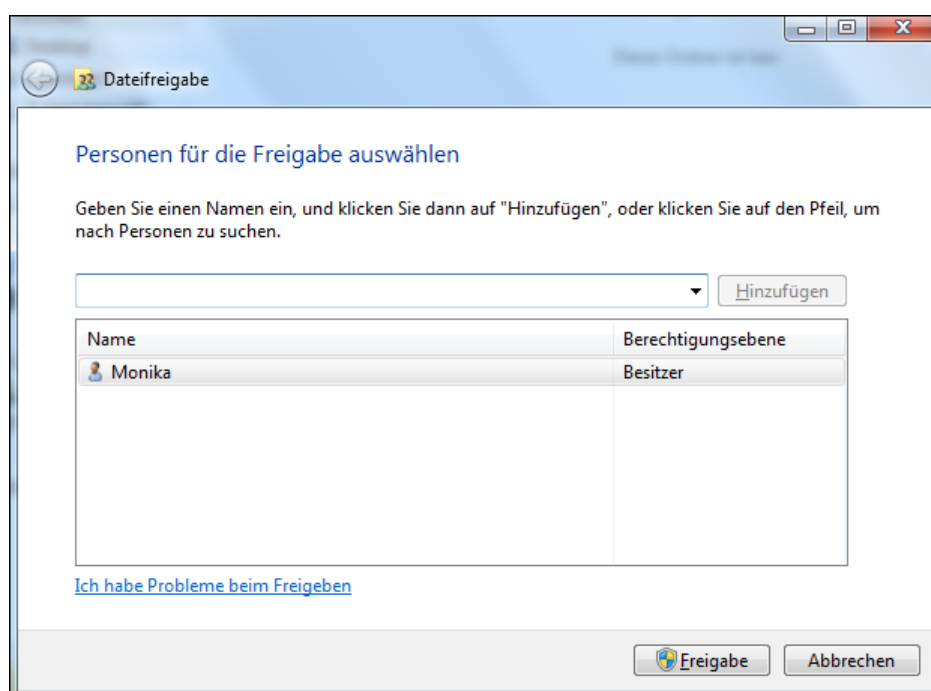


Abbildung 7.2 Das Freigabe-Menü

Drucker können Sie bereits bei der Installation freigeben. Achten Sie darauf, netzwerkweit eindeutige Namen auszuwählen. Die von Ihnen betreuten Anwender werden leichter mit den verschiedenen Bezeichnungen zurechtkommen.

7.1.3 »nmbd« und »smbd« unter Linux/FreeBSD

Das Samba-Paket bringt zwei Netzwerk-Daemons mit. Die Namensdienste und die interne Verwaltung sind die Aufgabe des `nmbd`. Für die Kommunikation mit den Clients nutzen Sie `smbd`. Die Konfigurationseinstellungen finden Sie in `/etc/smb.conf` oder `/usr/local/etc/smb.conf`. Die beiden Daemons sprechen Sie mit einem gemeinsamen RCSkript an.

7.1.4 Die Samba-Konfigurationsdatei »smb.conf«

Die Samba-Konfigurationsdatei `smb.conf` ist in verschiedene Sektionen unterteilt:

`global`: Einstellungen für die Benutzerauthentifizierung, Arbeitsgruppen- oder Domänenname, Netzwerkschnittstelle, Drucken
 - `homes`: Regeln für die Heimatverzeichnisse der Benutzer
 - `profiles`: Angabe der Regeln und des Ablageorts für die Benutzerprofile
 - `printers`: Festlegung des Druckerzugriffs
 - `shares`: Festlegung der Regeln und Ablageorte für Verzeichnisse, die für mehrere Benutzer vorgesehen sind. Das Schlüsselwort `shares` ersetzen Sie durch den Namen der Freigabe.

Zur Erläuterung habe ich die Konfigurationsdatei eines kleinen Arbeitsgruppen-Servers wiedergegeben:

```
[global]
workgroup = netzbuch
netbios name = netzi
server string = Samba %v
interfaces = lo, eth1
encrypt passwords = Yes
security = user
os level = 65
local master = Yes
wins support = No
printing = cups
printcap name = cups
[homes]
comment = Heimatverzeichnis
read only = no
create mask = 0600
directory mask = 0700
browseable = No
[printers]
comment = Drucker
browseable = no
path = /var/spool/samba
printable = yes
guest ok = no
read only = yes
create mask = 0700
```

Listing 7.1 »smb.conf« für Arbeitsgruppen

Die gezeigte Konfiguration reicht aus, um auf einer PC-Plattform ein »NAS« und einen Printserver für Windows-Clients einzurichten. Natürlich müssen Sie unter Linux den oder die Drucker installieren und die Benutzer aufnehmen. Reine Samba-Benutzer

legen Sie so an, dass diese keine Login-Shell bekommen (Sicherheitsgründe). In der Sektion `global` habe ich die notwendigen Eintragungen zum »Erscheinungsbild« des Servers im Netz, zu seinem Verhalten und zur Sicherheit festgelegt:

- ▶ `workgroup = netzbuch`: Name der Arbeitsgruppe
- ▶ `netbios name = netzi`: Windows-Name des Rechners. Dieser hat nichts mit dem Host-Namen gemeinsam. Der NetBIOS-Name erscheint in der Netzwerkumgebung.
- ▶ `server string = Samba %v`: zeigt Samba und seine Versionsnummer an
- ▶ `interfaces = lo, eth1`: Angabe der Netzwerkschnittstellen, über die Samba erreichbar sein soll (hier können Sie alternativ die IP-Adressen angeben). Diesen Eintrag müssen Sie im Zusammenhang mit der folgenden Zeile vornehmen.
- ▶ `bind interfaces only = yes`: Die beiden Daemons `nmbd` und `smbd` greifen nur auf diese in der oberen Zeile angegebenen Netzwerkschnittstellen zu.
- ▶ `encrypt passwords = yes`: Sie können verschlüsselte Kennwörter verwenden.
- ▶ `security = user`: Die Anmeldung erfolgt benutzerbezogen. Alternative: `share` (für freigabebezogene Anmeldung, unsicher)
- ▶ `os level = 65`: Prioritätsangabe für den Master-Browser
- ▶ `local master = yes`: Der Server agiert als Master-Browser. Ein Master-Browser regelt die Darstellung der Netzwerkumgebung (NetBIOS-Namen).
- ▶ `wins support = no`: Der Rechner agiert nicht als *Windows Internet Naming Service* (WINS), ein Nameserver für NetBIOS-Namen.
- ▶ `printing = cups`: Angabe des Drucksystems, hier `cups` (Alternativen: `bsd`, `lpng`). Im Anschluss könnten Sie hier Kommandos zum Anzeigen der Druckerwarteschlange oder zum Löschen von Druckaufträgen angeben. Unter Linux/FreeBSD wandelt das Drucksystem den Auftrag in ein für den Drucker brauchbares Datenformat um (Filter) und verwaltet die Warteschlangen (Spooler).
- ▶ `printcap name = cups`: Angabe der Druckereinträge

In der Sektion `homes` legen Sie die Einstellungen für die benutzereigenen Verzeichnisse ab:

- ▶ `comment = Heimatverzeichnis`: Kommentar, der zusätzlich zum Share-Namen ausgegeben wird
- ▶ `read only = no`: Damit ermöglichen Sie schreibenden Zugriff.
- ▶ `create mask = 0600`: Damit legen Sie die Rechte für Dateien fest. Hier werden das Lesen und das Schreiben nur für den Benutzer/Eigentümer erlaubt.
- ▶ `directory mask = 0700`: Festlegung der Rechte für Verzeichnisse. Hier werden das Lesen, Schreiben und das Ausführen nur für den Benutzer/Eigentümer erlaubt.
- ▶ `browseable = no`: Die benutzereigenen Verzeichnisse werden nicht allen Zugreifenden aufgelistet, nur das eigene Verzeichnis wird angezeigt.

Falls Sie nicht mit den Eigenheiten der Dateisysteme von Linux oder FreeBSD vertraut sind, hilft Ihnen vielleicht der folgende kleine Exkurs zu diesem Thema weiter: Die Rechte (Attribute) an Dateien und Verzeichnissen werden in drei Gruppen aufgeteilt: in den *Eigentümer*, die *Gruppe*, zu der der Eigentümer gehört, und alle anderen Benutzer am System. Es gibt die Rechte *Lesen*, *Schreiben* und *Ausführen*. Die weiteren möglichen Attribute sind hier nicht wichtig. Die Dateiattribute können Sie numerisch oder durch Buchstaben kennzeichnen. Anhand der Position erkennen Sie, für wen die Rechte gelten (Tabelle 7.1).

Eigentümer			Gruppe			Andere		
Lesen	Schr.	Ausf.	Lesen	Schr.	Ausf.	Lesen	Schr.	Ausf.
r	w	x	r	w	x	r	w	x

Tabelle 7.1 Dateiattribute in Symbolschreibweise für Linux/FreeBSD

Eine nach der Definitionen in der *smb.conf* erzeugte Datei trägt die Attribute

`-rw-----`

und ein Verzeichnis hat folgende Attribute:

`drwx-----`

Das erste Bit kennzeichnet die Sonderattribute, beim Verzeichnis ist das ein »d«. Anschließend folgen die Einträge für den Benutzer (Datei: Schreiben und Lesen, Verzeichnis: Schreiben, Lesen, Ausführen), für die Gruppe (keine Rechte) und für die anderen Benutzer (keine Rechte).

In der *smb.conf* (und auch bei vielen anderen Konfigurationsdateien und Programmen) werden die Dateiattribute numerisch ausgedrückt (Tabelle 7.2).

Attribut/Recht	Wert
Ausführen	1
Schreiben	2
Lesen	4

Tabelle 7.2 Dateiattribute in numerischer Schreibweise für Linux/FreeBSD

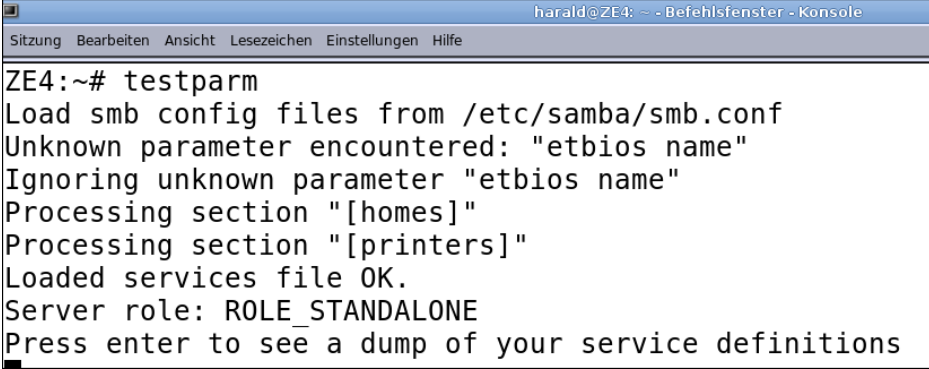
Für jeden »Akteur« (Eigentümer, Gruppe, andere) geben Sie die Rechte in einer einzigen Zahl an. Dazu addieren Sie die einzelnen numerischen Werte der Attribute. In der *smb.conf* finden Sie die Attribute für Dateien mit `0600` angegeben. Das bedeutet: keine Sonderattribute, Lesen (4) und Schreiben (2) für den Eigentümer, keine (0) für die Gruppe und andere. Verzeichnisse tragen die Rechtemaske `0700`: Alle Rechte (1 + 2 + 4) für den Eigentümer, jeweils 0 für die Gruppe und für die anderen. Die Sektion `printers` aus Listing 7.1 legt den Zugriff auf die vom Samba-Rechner verwalteten Drucker fest:

- ▶ `comment = Drucker`: Kommentar, der jedoch kaum angezeigt wird. Anstelle dessen sehen Sie beim Zugriff meist den Warteschlangennamen des Druckers.
- ▶ `browseable = no`: Die Drucker werden nicht allgemein angezeigt.
- ▶ `path = /var/spool/samba`: Pfad für die Ablage der Druckdaten
- ▶ `printable = yes`: Der Drucker kann benutzt werden.
- ▶ `guest ok = no`: kein Gastzugriff möglich
- ▶ `read only = yes`: Das Druckerobjekt kann nicht geändert oder gelöscht werden.
- ▶ `create mask = 0700`: Rechtengewährung (alle) für den Benutzer

Meist wird eine gut kommentierte Muster-Konfigurationsdatei (*smb.conf.sample* o. Ä.) mitgeliefert. In dieser finden Sie oft auch alle Erläuterungen, um Samba als Domain-Controller einzusetzen.

7.1.5 Testen der Konfiguration

Melden Sie sich als Benutzer `root` (Systemverwalter) auf der Shell (Terminal) an. Geben Sie den Befehl `testparm` ein. Sie erhalten gegebenenfalls Fehlerhinweise auf falsche und ungültige Parameter. Ändern Sie diese fehlerhaften Einträge (Abbildung 7.3) ab, und führen Sie den Test erneut durch.



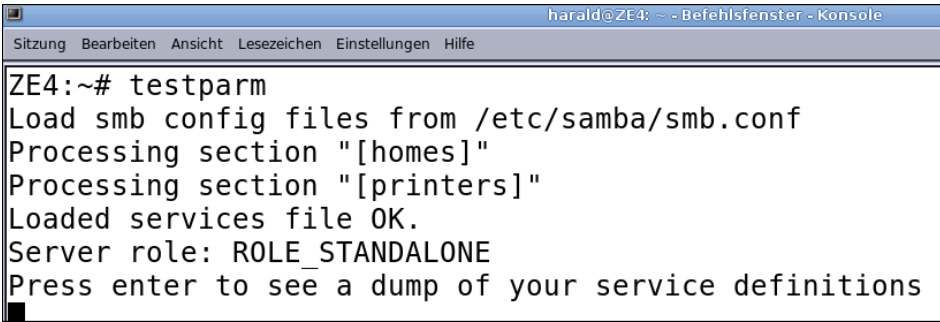
```

ZE4:~# testparm
Load smb config files from /etc/samba/smb.conf
Unknown parameter encountered: "etbios name"
Ignoring unknown parameter "etbios name"
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

```

Abbildung 7.3 »testparm«: Fehler in »smb.conf«

Eine fehlerfreie *smb.conf* hat in Abbildung 7.4 die Testprozedur durchlaufen. Am Schluss zeigt `testparm` eine gestraffte Ausgabe von *smb.conf* an.



```

ZE4:~# testparm
Load smb config files from /etc/samba/smb.conf
Processing section "[homes]"
Processing section "[printers]"
Loaded services file OK.
Server role: ROLE_STANDALONE
Press enter to see a dump of your service definitions

```

Abbildung 7.4 »testparm«: fehlerfreie »smb.conf«

7.1.6 Aufnehmen und Bearbeiten von Samba-Benutzern

Nach dem Neueinrichten des Samba-Dienstes müssen Sie die Benutzer aufnehmen. Gänzlich neue legen Sie zunächst für Linux/FreeBSD an. Für jene Benutzer, die auf dem System ausschließlich nur ihre Daten speichern sollen, lassen Sie die Login-Shell weg. Für Samba müssen Sie auch schon bestehende Linux-Benutzer explizit aufnehmen. Dies nehmen Sie unter der Benutzerkennung `root` vor. Geben Sie hierzu

```
smbpasswd -a <BENUTZERNAME>
```

ein. Hat der Benutzer sein Kennwort vergessen, kann er es selbst ändern, sofern er Shell-Zugriff hat. Andernfalls gibt `root` den folgenden Befehl ein:

```
smbpasswd <BENUTZERNAME>
```

Anschließend geben Sie das neue Kennwort zweifach ein. In Tabelle 7.3 finden Sie die wichtigsten Optionen von `smbpasswd` zur Benutzerverwaltung.

Aktion	smbpasswd
Benutzer anlegen	-a <BENUTZER>
Benutzer sperren	-d <BENUTZER>
Benutzer freigeben	-e <BENUTZER>
Benutzer löschen	-x <BENUTZER>

Tabelle 7.3 Optionen von »smbpasswd«

7.1.7 Starten, Stoppen und Neustart der Samba-Daemons

Wenn Sie Änderungen oder Ergänzungen an der Konfiguration vorgenommen haben, müssen Sie die beiden Daemons anhalten und neu starten. Sie brauchen Linux oder FreeBSD *nicht* neu zu starten! Sie rufen dazu das `init`-Skript der beiden Daemons auf. Unter Linux finden Sie es meist im Verzeichnis `/etc/init.d/` mit dem Namen `samba`, unter FreeBSD liegt es unter `/usr/local/etc/rc.d`. Sie müssen als `root` angemeldet sein, um einen Samba-Daemon zu starten oder zu stoppen, wie in Abbildung 7.5 gezeigt. Je nach Linux-Version können Sie alternativ die Option `reload` für den Neustart benutzen. Wenn Sie das Samba-Paket installieren, sorgen die Installationsroutinen meist automatisch dafür, dass bei jedem Hochfahren des Rechners die beiden Daemons mit gestartet werden.

```

ZE4:~# /etc/init.d/samba stop
Stopping Samba daemons: nmbd smbd.
ZE4:~# /etc/init.d/samba start
Starting Samba daemons: nmbd smbd.
ZE4:~# █

```

Abbildung 7.5 Anhalten und Starten der Samba-Daemons

7.1.8 Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10)

Unter Microsoft Windows gelangen Sie mit folgenden Schritten zur gewünschten Verbindung (wenn nicht anders angegeben, ist immer der linke Mausklick gemeint):

Öffnen Sie den Windows-Explorer (z. B. unter Windows 7 per Startmenü und Suche nach »explorer«).

Klicken Sie im Windows-Explorer die linke Spalte Netzwerk per Rechtsklick an.

Im neuen Fenster im Windows-Explorer klicken Sie (unter Windows 10: Rechtsklick auf Dieser PC, und dann:) Netzlaufwerk verbinden an. Unter Windows 10 wird Ihnen eine Schaltfläche Durchsuchen angeboten. Hierauf setzen Sie einen Linksklick ab und wählen die gewünschte Freigabe aus.

Im Dialog Netzlaufwerk verbinden wählen Sie zunächst den Laufwerksbuchstaben aus und geben manuell die Freigabe in der Form `\\Rechnername (NetBIOSname) \Freigabe` ein. Klicken Sie auf Fertigstellen.

Oder Sie gehen folgendermaßen vor:

Im Dialog Netzlaufwerk verbinden wählen Sie zunächst den Laufwerksbuchstaben aus und geben manuell die Freigabe in der Form `\\Rechnername (NetBIOSname) \Freigabe`

ein, setzen ein Häkchen bei Verbindung mit anderen Anmeldeinformationen herstellen und klicken schließlich auf Fertigstellen.

Windows-Sicherheit: Geben Sie Benutzername und Kennwort manuell ein, und klicken Sie auf OK.

Anschließend können Sie auf die Daten zugreifen.

7.1.9 Client-Zugriffe unter Linux/FreeBSD

Sie können mit Shell-Mitteln und Werkzeugen aus den verschiedenen grafischen Benutzeroberflächen auf Windows-Freigaben zugreifen.

Wenn Sie zunächst in Ihrem lokalen Netz Rechner finden wollen, die Windows-Freigaben anbieten, verwenden Sie `findsmb` (Abbildung 7.6). Geben Sie dabei unbedingt die Netzwerkadresse an. Mit der Option `-r` zeigt das Programm den Host-Namen anstelle des NetBIOS-Namens an. Meist unterscheiden sich bei Linux- und FreeBSD-Hosts die Host-Namen vom NetBIOS-Namen.

```

harald@ZE4:~$ findsmb 192.168.0.0

                                *=DMB
                                +=LMB
IP ADDR      NETBIOS NAME      WORKGROUP/OS/VERSION
-----
192.168.0.103  NETZI          +[NETZBUCH] [Unix] [Samba 3.2.5]
harald@ZE4:~$
harald@ZE4:~$ findsmb -r 192.168.0.0

                                *=DMB
                                +=LMB
IP ADDR      NETBIOS NAME      WORKGROUP/OS/VERSION -B 192.168.0.0
-----
192.168.0.103  ZE4.local
harald@ZE4:~$

```

Abbildung 7.6 »findsmb«

Das Programm `smbclient` dient zur Verbindung mit SMB-Freigaben. Mit der Option `-L <Netbios-Hostname>` erhalten Sie eine Liste der für Sie erreichbaren Freigaben (Abbildung 7.7). In dieser Abbildung sehen Sie auch die Angabe des Master-Browsers für die NetBIOS-Namen.

```

harald@ZE4:~$ smbclient -L netzi
Enter harald's password:
Domain=[NETZI] OS=[Unix] Server=[Samba 3.2.5]

      Sharename      Type      Comment
      -----
      IPC$           IPC       IPC Service (Samba 3.2.5)
      lp            Printer   FS-1370ND
      epson          Printer   Epson LQ-670
      harald         Disk      Heimatverzeichnis
Domain=[NETZI] OS=[Unix] Server=[Samba 3.2.5]

      Server          Comment
      -----
      Workgroup       Master
      -----
      NETZBUCH        NETZI
harald@ZE4:~$

```

Abbildung 7.7 »smbclient«: Auflistung der Freigaben

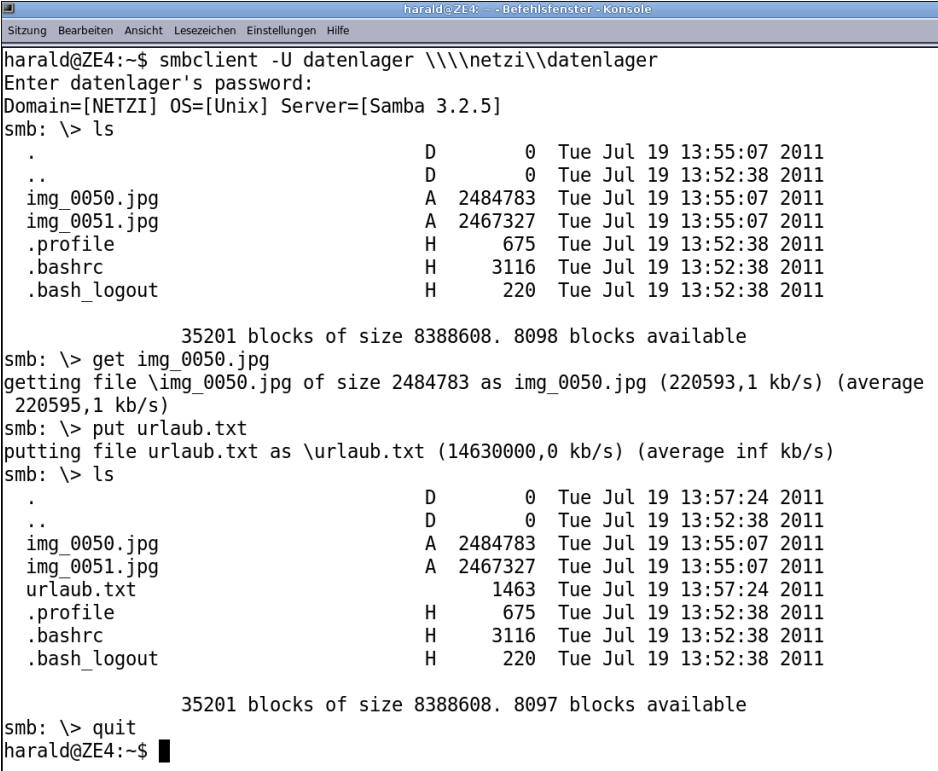
Das Verbinden mit einer Freigabe erfolgt in der Form

```
smbclient \\\<WINDOWSRECHNER>\<FREIGABE>
```

Dabei werden Sie je nach Shell-Version auch mit einem kleinen Problem konfrontiert: »\« ist ein Entwerterzeichen. So sehen Sie in Abbildung 7.8, dass dadurch die Zahl dieser Zeichen doppelt so hoch ist, wie gerade in der Syntax angegeben wurde. Mit der Option -U <BENUTZERNAME> geben Sie den Samba-Benutzer an.

In Abbildung 7.8 sehen Sie zunächst die Verbindungsaufnahme. Der Client zeigt nach erfolgreichem Anmelden die Arbeitsgruppe, das Betriebssystem und den Server-String an. Beachten Sie den Prompt des Clients. Sie erkennen daran eine bestehende Verbindung.

Mit `ls` lassen Sie sich den Verzeichnisinhalt anzeigen. Mit `get <DATEINAME>` holen Sie Dateien auf Ihr lokales Verzeichnis. Mit `put <DATEINAME>` senden Sie eine Datei aus dem lokalen Verzeichnis zur Freigabe. Mit `quit` beenden Sie die Sitzung.



```

harald@ZE4: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

harald@ZE4:~$ smbclient -U datenlager \\\netzi\datenlager
Enter datenlager's password:
Domain=[NETZI] OS=[Unix] Server=[Samba 3.2.5]
smb: \> ls
.                D            0 Tue Jul 19 13:55:07 2011
..               D            0 Tue Jul 19 13:52:38 2011
img_0050.jpg     A    2484783 Tue Jul 19 13:55:07 2011
img_0051.jpg     A    2467327 Tue Jul 19 13:55:07 2011
.profile         H        675 Tue Jul 19 13:52:38 2011
.bashrc          H       3116 Tue Jul 19 13:52:38 2011
.bash_logout     H        220 Tue Jul 19 13:52:38 2011

35201 blocks of size 8388608. 8098 blocks available
smb: \> get img_0050.jpg
getting file \img_0050.jpg of size 2484783 as img_0050.jpg (220593,1 kb/s) (average
220595,1 kb/s)
smb: \> put urlaub.txt
putting file urlaub.txt as \urlaub.txt (14630000,0 kb/s) (average inf kb/s)
smb: \> ls
.                D            0 Tue Jul 19 13:57:24 2011
..               D            0 Tue Jul 19 13:52:38 2011
img_0050.jpg     A    2484783 Tue Jul 19 13:55:07 2011
img_0051.jpg     A    2467327 Tue Jul 19 13:55:07 2011
urlaub.txt       A       1463 Tue Jul 19 13:57:24 2011
.profile         H        675 Tue Jul 19 13:52:38 2011
.bashrc          H       3116 Tue Jul 19 13:52:38 2011
.bash_logout     H        220 Tue Jul 19 13:52:38 2011

35201 blocks of size 8388608. 8097 blocks available
smb: \> quit
harald@ZE4:~$

```

Abbildung 7.8 Datenzugriff auf eine Freigabe

Normalerweise werden Sie `smbclient` nur für Shell-Skripte verwenden. Für die Arbeit am Arbeitsplatz werden Sie den Zugriff sicher über die grafische Benutzeroberfläche vornehmen. In Abbildung 7.9 sehen Sie den Verbindungsaufbau in der GNOME-Oberfläche.

Klicken Sie hierzu auf Orte und mit Server verbinden. In dem Dialog, der nun erscheint, wählen Sie bei Dienste-Typ • Windows-Freigabe und tragen den Freigabe und den Benutzernamen ein. Sie werden vom Rechner sodann zur Eingabe Ihres Kennworts aufgefordert. Am Schluss erhalten Sie das Fenster vom Dateimanager mit der Freigabe.

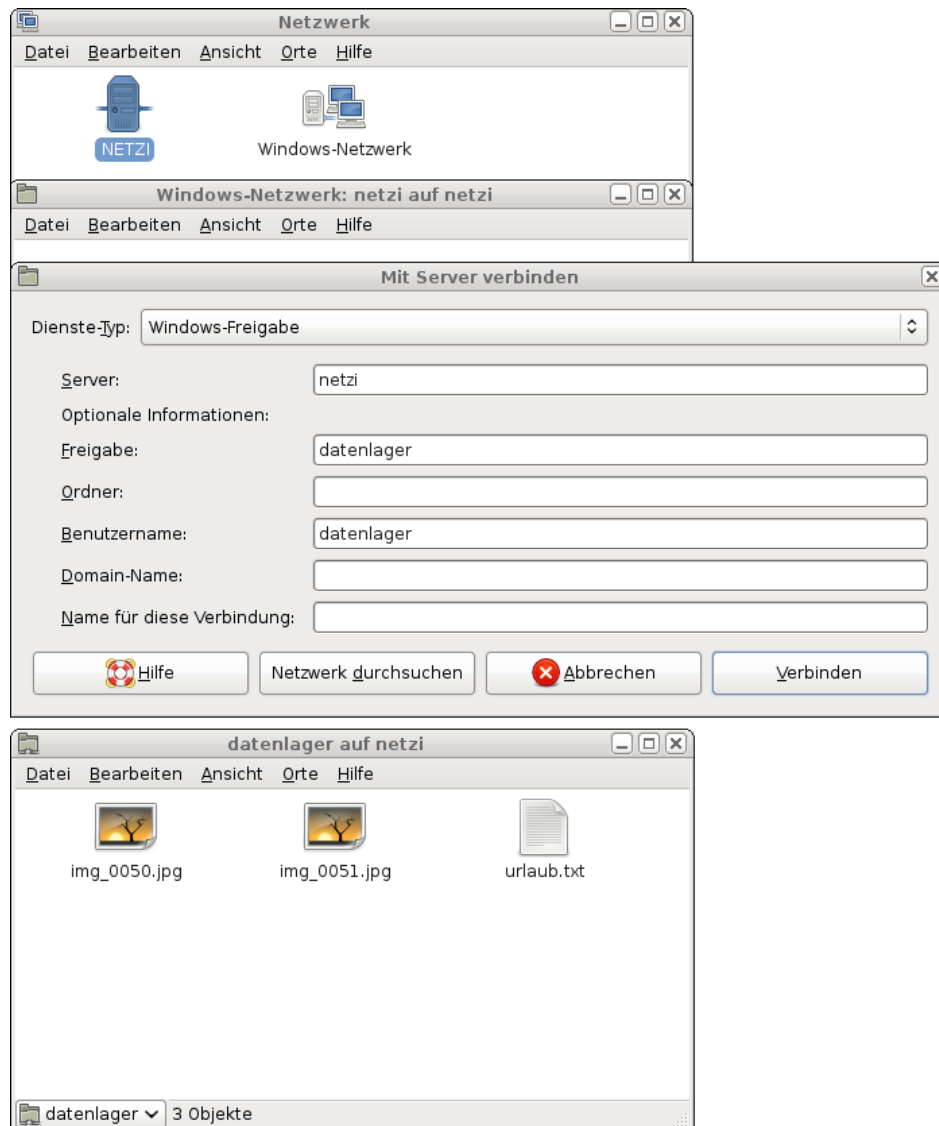


Abbildung 7.9 Zugriff auf eine Freigabe unter GNOME

7.1.10 Zugriffskontrolle mit »smbstatus«

Sie können mit der Benutzererkennung `root` die Belegung des Samba-Servers mittels `smbstatus` abrufen. Sie sehen dann, welche Benutzer auf welche Ressourcen aktuell zugreifen (Abbildung 7.10).

```

harald@ZE4: ~ - Befehlsfenster - Konsole
Sitzung Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe

harald@ZE4:~$ su -
Passwort:
ZE4:~# smbstatus

Samba version 3.2.5
PID      Username      Group         Machine
-----
25135    datenlager    datenlager    monikamobil   (192.168.0.102)
25136    datenlager    datenlager    monikamobil   (192.168.0.102)
25133    datenlager    datenlager    monikamobil   (192.168.0.102)
25126    datenlager    datenlager    monikamobil   (192.168.0.102)
24842    datenlager    datenlager    netzi         (192.168.0.103)

Service  pid          machine      Connected at
-----
IPC$     24838        netzi        Tue Jul 19 20:19:01 2011
datenlager 24842        netzi        Tue Jul 19 20:19:03 2011
datenlager 25133        monikamobil  Tue Jul 19 20:28:02 2011
datenlager 25135        monikamobil  Tue Jul 19 20:28:05 2011
IPC$     25049        monikamobil  Tue Jul 19 20:24:56 2011
datenlager 25126        monikamobil  Tue Jul 19 20:27:45 2011
datenlager 25136        monikamobil  Tue Jul 19 20:28:05 2011
IPC$     25042        monikamobil  Tue Jul 19 20:24:46 2011
IPC$     25046        monikamobil  Tue Jul 19 20:24:51 2011

No locked files

ZE4:~# █

```

Abbildung 7.10 Ausgabe von »smbstatus«

7.1.11 Die »net«-Befehle für die Windows-Batchprogrammierung

Mit den `net`-Befehlen können Sie auf die Netzwerkumgebung zugreifen und z. B. kleine Datensicherungsroutrinen erstellen.

Aktion	»net«-Befehl
Netzlaufwerk verbinden	<code>net use n: \\<RECHNERNAME>\<FREIGABE></code>
Netzlaufwerk verbinden mit Benutzer- angabe	<code>net user n: \user: <BENUTZER> \\<RECHNERNAME>\>FREIGABE></code>
Anzeige bestehender Netzlaufwerke	<code>net use</code>
Nachrichten an andere Rechner, Domänen oder Benutzer senden	<code>net send <EMPFÄNGER> <NACHRICHT></code>
Netzwerkumgebung anzeigen	<code>net view</code>
Freigaben eines Rechners anzeigen	<code>net view \\<RECHNERNAME></code>

Tabelle 7.4 Die »net«-Befehle für die Windows-Batchprogrammierung

Ich zeige hier nur eine kleine Auswahl der Befehle auf (Tabelle 7.4). Mit `<RECHNERNAME>` meine ich immer den NetBIOS-Namen. Als Laufwerksbuchstaben verwende ich in den Beispielen `N`.

7.2 Network File System (NFS)

Das *Network File System* begegnet Ihnen im Linux-, FreeBSD- und Unix-Umfeld. Mit NFS stellen Sie Freigaben von Verzeichnissen ähnlich wie mit Samba anderen Rechnern zur Verfügung. Beim NFS-Client hängen Sie diese Freigaben in den lokalen Verzeichnisbaum ein. Die so gemounteten NFS-Freigaben (*Exports*) werden wie ein lokales Verzeichnis

oder Plattengerät behandelt.

Mit NFS verwirklichen Sie z. B. folgende Konfigurationen:

zentrales Programmverzeichnis für mehrere Rechner; nur eine Programminstallation für viele zugreifende Geräte notwendig

Vorhalten eines kompletten Dateisystems für plattenlose Thin-Clients

Einrichtung eines zentralen Datensicherungsrechners

Vorhalten von Verzeichnissen mit von vielen gemeinsam genutzten Ressourcen, wie Vorlagen, Archivmaterial usw.

Hier im Buch beschreibe ich die aktuelle NFS-Version 4. Diese ist leichter administrierbar und sicherer als die Vorgängerversion. Sie benutzt TCP. Nachteilig bei jeder NFS-Version ist der jeweilige Umfang der Konfigurationsarbeiten. Es gibt andere, unkompliziertere und flexiblere Verfahren, um Daten für andere Rechner bereitzustellen.

Weitere Informationen finden Sie in den RFCs 3530 (NFS Version 4) und 1813 (NFS Version 3) sowie in den Manual-Seiten zu `exports`, `nfsd` und `portmap`.

7.2.1 Konfiguration des NFS-Servers

Vor der Installation müssen Sie in Ihrem Netz noch einige Dinge regeln:

Damit Sie beim Zugriff keine Probleme und Fehlermeldungen bekommen, müssen die Benutzer-IDs auf allen beteiligten Rechnern identisch sein (ausgenommen beim reinen Lesezugriff).

Dazu setzen Sie am besten eine zentrale Benutzerverwaltung wie LDAP, NIS oder Kerberos ein.

Legen Sie anschließend, falls es noch notwendig ist, die zu exportierenden Verzeichnisse auf dem Server an. Führen Sie die Programminstallation mit den Werkzeugen Ihrer Linux-Distribution durch.

Am Beispiel eines Debian-Linux-Servers zeige ich Ihnen die fälligen Konfigurationsschritte:

Editieren Sie die Datei `/etc/fstab`:

Fügen Sie die Zeile

```
/home /export/home none bind 0 0
```

an. Damit wird das `home`-Verzeichnis zusätzlich nach `/export/home` gemountet.

Editieren Sie die Datei `/etc/defaults/nfs-kernel-server`:

Setzen Sie die Variable (zwecks Übersicht und Ordnung):

```
# exports. Valid alternatives are "yes" and "no"; the default is #
"no".
```

```
NEED_SVCGSSD=no
```

Setzen Sie `no`, wenn Sie nicht mit Kerberos zur Benutzerauthentifizierung arbeiten.

Editieren Sie die Datei `/etc/defaults/nfs-common`:

Setzen Sie die beiden folgenden Variablen:

```
# Do you want to start the idmapd daemon? It is only needed for
# NFSv4.
```

```
NEED_IDMAPD=yes
```

```
# Do you want to start the gssd daemon? It is required for
# Kerberos mounts.
```

```
NEED_GSSD=no
```

Da hier die NFS Version 4 gewünscht wird, setzen Sie die erste Variable mit `yes`.
Nachdem hier im Beispiel Kerberos nicht verwendet wird, setzen Sie für die zweite Variable `no`.

Ergänzen Sie die Datei `/etc/exports` um Ihre NFS-Exports, wie im Beispiel gezeigt wird (jede Freigabe in einer Zeile):

```
/export 192.168.0.0/24(rw, fsid=0, insecure,  
no_subtree_check, async)  
/export/home 192.168.0.0/24(rw, nohide, insecure,  
no_subtree_check, async)
```

Für die Einträge in der `exports`-Datei können Sie verschiedene Optionen nutzen, die in Tabelle 7.5 erläutert werden.

Option	Option-Schlüsselwort
Lesen und Schreiben ist erlaubt.	<code>rw</code>
Nur Lesen ist erlaubt.	<code>ro</code>
Port-Nummer über 1024 verwenden	<code>insecure</code>
Datentransfer läuft im asynchronen Modus.	<code>async</code>
Das exportierte Verzeichnis gehört auf den Server <code>root</code> . Am Client werden diese Verzeichnisse auf den Benutzer <code>nobody</code> gemappt, Sie können sie deshalb nur lesen. Mit dieser Option umgehen Sie diese Sicherheitseinstellung.	<code>no_root_squash</code>
Betrachten Sie das <code>exports</code> -Beispiel. Hier werden die Verzeichnisse <code>/export</code> und <code>/export/home</code> als eigenständige Freigaben behandelt. Mit <code>nohide</code> sieht Ihr NFS-Client die beiden Freigaben nicht als verschiedene, sondern als hierarchisch miteinander verknüpft an.	<code>nohide</code>
Prüft, ob in einem einzelnen freigegebenen Verzeichnis eine angeforderte Datei liegt.	<code>subtree_check</code>
Unterlässt diese Prüfung. Dies ist eine empfehlenswerte Einstellung, wenn der gesamte Verzeichnisbaum exportiert wird. Damit steigern Sie die Zugriffsgeschwindigkeit.	<code>no_subtree_check</code>

Tabelle 7.5 Optionen in »/etc/exports«

Ergänzen Sie die Datei `/etc/hosts.deny` um folgende Einträge:

```
portmap: ALL  
mountd: ALL  
statd: ALL
```

In dieser Datei werden Angaben darüber gemacht, wer oder was nicht über das Netz auf den Rechner zugreifen darf.

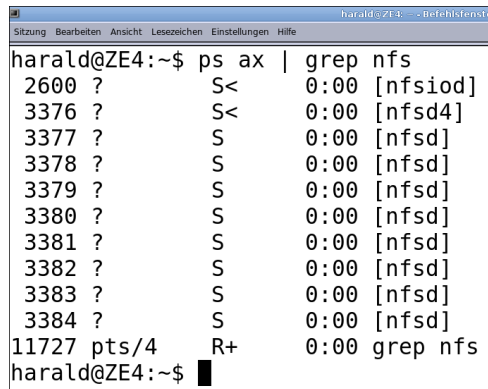
Ergänzen Sie die Datei `hosts.allow` um diese Einträge:

```
portmap: 192.168.0.0/24  
mountd: 192.168.0.0/24  
statd: 192.168.0.0/24
```

In dieser Datei finden Sie Angaben darüber, wer oder was über das Netzwerk auf den Rechner zugreifen darf. Zunächst wurde in `hosts.deny` alles verboten, und hier in der Datei `hosts.allow` werden Zugriffe eingeschränkt erlaubt.

Führen Sie das Kommando `/etc/init.d/nfs-kernel-server restart` aus. Sie sollten nun die Meldungen erhalten, dass der NFS-Server und der `mountd` gestartet wurden.

Überprüfen Sie, ob NFS jetzt aktiv ist. Fragen Sie dazu die Prozesstabelle ab: `ps ax | grep nfs` sollte eine Anzeige wie in Abbildung 7.11 ergeben.



```

harald@ZE4:~$ ps ax | grep nfs
2600 ?        S<        0:00 [nfsiod]
3376 ?        S<        0:00 [nfsd4]
3377 ?        S         0:00 [nfsd]
3378 ?        S         0:00 [nfsd]
3379 ?        S         0:00 [nfsd]
3380 ?        S         0:00 [nfsd]
3381 ?        S         0:00 [nfsd]
3382 ?        S         0:00 [nfsd]
3383 ?        S         0:00 [nfsd]
3384 ?        S         0:00 [nfsd]
11727 pts/4    R+        0:00 grep nfs
harald@ZE4:~$

```

Abbildung 7.11 Prozessstatusabfrage

7.2.2 Konfiguration des NFS-Clients

Beim Client-Rechner können Sie mit der Benutzerkennung `root` die NFS-Freigaben im Verzeichnisbaum einhängen. Hierzu müssen Sie das Einhängeverzeichnis anlegen und anschließend die Freigabe mounten. Hier im Beispiel wurde als Einhängeverzeichnis `/usr/nfszugriff` gewählt:

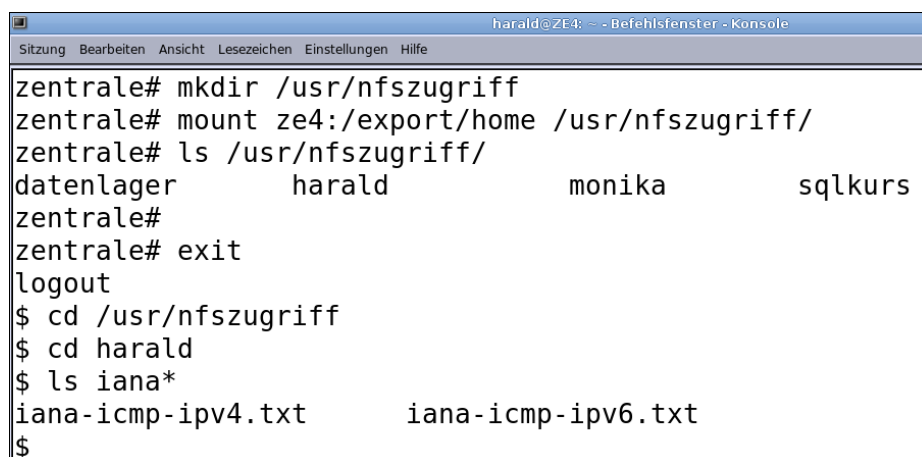
Anlegen des Verzeichnisses:

```
mkdir /usr/nfszugriff
```

Einhängen der Freigabe in den Verzeichnisbaum:

```
mount ze4:/export/home /usr/nfszugriff/
```

Zur Verdeutlichung sehen Sie den Vorgang in Abbildung 7.12. Sie finden darin auch den (funktionierenden) Datenzugriff als normaler Benutzer dargestellt.



```

zentrale# mkdir /usr/nfszugriff
zentrale# mount ze4:/export/home /usr/nfszugriff/
zentrale# ls /usr/nfszugriff/
datenlager      harald          monika          sqlkurs
zentrale#
zentrale# exit
logout
$ cd /usr/nfszugriff
$ cd harald
$ ls iana*
iana-icmp-ipv4.txt  iana-icmp-ipv6.txt
$

```

Abbildung 7.12 Manuelles Einhängen der Freigabe und Funktionstest

Sollen die NFS-Freigaben dauerhaft nach jedem Rechnerstart automatisch in den Verzeichnisbaum eingehängt werden, müssen Sie in der Datei `/etc/fstab` eine Zeile anfügen (hier auf das Beispiel bezogen):

```
192.168.0.34:/export/home /usr/nfszugriff nfs rw,soft 0 0
```

Die Option `soft` verhindert ein Einfrieren von Anwendungen, die auf die Freigaben zugreifen.

7.3 HTTP für die Informationen im Internet

Mit dem *Hypertext Transfer Protocol* (HTTP) übertragen Sie Texte, Bilder und andere Inhalte, die in der *Hypertext Markup Language* (HTML) erstellt oder darin eingebettet sind. Die Verteilung der Datenmengen ist dabei sehr ungleich: Der anfragende Client übermittelt im Allgemeinen nur wenige Zeichen, während der Server (fast) beliebig viel als Antwort senden kann.

Die Client-Programme, die sogenannten *Webbrowser*, müssen von jedem Benutzer bedient werden können. Gleiches gilt aber auch für die anzuzeigenden Webseiten, die Sie erstellen. Lassen Sie diese übersichtlich und klar im Aufbau erscheinen.

7.3.1 Grundlagen des HTTP-Protokolls

Mit dem HTTP-Protokoll transportieren Sie HTTP-Nachrichten. Diese enthalten Texte, Skripte, Bilder und andere Multimedia-Inhalte.

Übersicht über die HTTP-Protokolle

Allgemeine Eigenschaften: HTTP ist ein zustandsloses Protokoll und benutzt TCP. Die Zuordnung von Statusinformationen (Formulare, Warenkörbe ...) wird durch Cookies (Datenschnipsel, die der Zuordnung dienen) ermöglicht.

Versionen: HTTP/1.0 und HTTP/1.1

HTTP/1.0: Bei jeder Anfrage eines Clients baut der Server eine neue, eigene TCP-Verbindung auf, die nach erfolgreicher Übertragung der Antwort wieder geschlossen wird.

HTTP/1.1: Sie können eine bestehende Verbindung zum »Nachladen« benutzen (z. B. Grafiken). Damit erzielen Sie eine höhere Übertragungsgeschwindigkeit und eine verminderte Netzlast. In dieser Protokollversion können Sie Daten zum Server transportieren. Das Verfahren WebDAV ist damit möglich.

HTTP-Nachrichten sind unverschlüsselt.

HTTPS-Nachrichten sind verschlüsselt. Für diese Erweiterung müssen Sie entsprechende Server- und Client-Programme nutzen.

Standard-Port: 80, alternativ: 8080, verschlüsselt (HTTPS): 443

Serverprogramme: thttp, apache, tomcat, Internet Information Services (IIS)

Client-Programme: Firefox, Opera, Iceweasel, Galeon, Internet Explorer, w3m, links, lynx

RFCs: 1945, 2295, 2774, 2817, 4918, 5689, 5785, 6266, 6585, 7230, 7231, 7232, 7233, 7234, 7235

Die verschiedenen Anfragemethoden (HTTP-Requests) finden Sie in Tabelle 7.6. Sie können bei einigen dieser Requests Argumente übergeben. Argumente trennen Sie mit dem Zeichen »&« ab. Mit Werten gefüllte Parameter bauen Sie in der Form `?ARGUMENT=WERT` auf.

Methode	Name
Anforderung einer Datei (Abruf einer Webseite)	get
Anforderung zur Übersendung des Headers, nicht aber des Inhalts einer HTML-Datei. Sie überprüfen damit, ob eine Datei im Cache des Clients noch aktuell ist.	head
Senden weiterer Daten an den Server	post
Prüfen, ob eine Anfrage verändert wurde. Der Webserver gibt die Anfrage anstelle einer Webseite zurück.	trace

Tabelle 7.6 HTTP-Requests

Methode	Name
Anfrage nach vom Server angebotenen Methoden	options
Weitere Methoden von RESTful Webservices	
Senden einer Datei	put
Löschen einer Datei	delete
Zusätze von WebDAV (Dateiserver unter dem HTTP-Protokoll)	
Kopieren einer Datei oder eines Verzeichnisses	copy
Verschieben einer Datei oder eines Verzeichnisses	move
Abfragen einer Objekteigenschaft oder Anzeigen eines Verzeichnisbaums	propfind
Ändern von Objekteigenschaften	proppatch
Setzen einer Zugriffssperre für ein Objekt, während Sie es bearbeiten	lock
Aufheben einer Zugriffssperre	unlock

Tabelle 7.6 HTTP-Requests (Forts.)

HTTP-Server beantworten Requests mit einem Statuscode und gegebenenfalls mit weiteren Daten. Der Statuscode gibt Ihnen Auskunft darüber, wie der Request Ihres Clients abgearbeitet wurde. Sie finden die Festlegungen teilweise in den RFCs (siehe Kasten) und den Handbüchern und Manual-Seiten der Serverprogramme. Manche Server geben zusätzliche, nicht in den RFCs beschriebene Statuscodes ab.

Anhand der ersten Ziffer der Statuscodenummer erkennen Sie schon, ob die Anfrage erfolgreich war oder nicht. Die 1 zeigt Ihnen an, dass die Bearbeitung der Anfrage noch andauert. Die 2 meldet Ihnen Erfolg. Die 3 teilt Ihnen mit, dass die Anfrage umgeleitet wurde. Die 4 weist Sie auf Fehler in der Anfrage hin, und die 5 deutet auf Serverfehler hin.

Die wichtigsten dieser Codes finden Sie in Tabelle 7.7 zusammengefasst.

Code	Text	Bedeutung
Gruppe 1 – Informationen		
100	CONTINUE	Fortsetzung der Anfrage
101	SWITCHING PROTOCOLS	Protokollwechsel (Zustimmung durch den Server)

Tabelle 7.7 HTTP-Statuscodes

Code	Text	Bedeutung
102	PROCESSING	Bearbeitung dauert an. Diesen Code gibt der Server bei längerer Bearbeitungsdauer an, damit ein Time-out verhindert wird.
Gruppe 2 – erfolgreiche Anfragen		
200	OK	OK, Anfrage erfolgreich bearbeitet; Daten werden in dieser Antwort an den Client übermittelt.
201	CREATED	Ein Request wurde mit Erfolg bearbeitet. Die vom Client angefragten Daten wurden vor der Übermittlung der Antwort zusammengestellt.
202	ACCEPTED	Die Anfrage wurde vom Server angenommen, aber noch nicht ausgeführt.
204	NO CONTENT	Antwort auf erfolgreiche Anfrage, in der mit Absicht keine weiteren Daten übermittelt werden
205	RESET CONTENT	Nach dieser erfolgreichen Anfrage soll der Client die Seite neu darstellen. Eventuelle Daten in Formularfeldern werden gelöscht.
Gruppe 3 – Umleitungen, Änderungen und Rückfragen		
300	MULTIPLE CHOICE	Sie können wählen, in welcher Form die angeforderten Daten abgerufen werden.
301	MOVED PERMANENTLY	Umleitung; der Server stellt zur Darstellung der neuen Adresse das Location-Header-Feld bereit.
303	SEE OTHER	Der Server gibt das Location-Header-Feld mit der Adresse aus, unter der die Antwort abgelegt wurde.
304	NOT MODIFIED	Gegenüber der letzten Antwort hat sich deren Inhalt nicht geändert, deshalb überträgt der Server keine Daten.
305	USE PROXY	Der Server gibt das Location-Header-Feld mit der Adresse des Proxys aus. Die Antwort ist nur hierüber erreichbar.
Gruppe 4 – fehlerhafte Anfragen		
400	BAD REQUEST	syntaktischer Fehler im Request

Tabelle 7.7 HTTP-Statuscodes (Forts.)

Code	Text	Bedeutung
401	UNAUTHORIZED	Request ohne gültige Authentifizierung (fehlerhafte oder fehlende Anmeldedaten)
403	FORBIDDEN	Request ohne gültige Authentifizierung
404	NOT FOUND	Aufruf einer nicht vorhandenen Webseite oder Webressource
423	LOCKED	Die angeforderte Seite ist gesperrt.
451	UNAVAILABLE FOR LEGAL REASONS	zensiert aus politischen Gründen oder wegen urheberrechtlicher Einschränkungen
Gruppe 5 – Fehler im Bereich des Servers		
500	INTERNAL SERVER ERROR	allgemeine Fehlermeldung
501	NOT IMPLEMENTED	Die Anfrage enthielt eine vom Server nicht unterstützte Methode.
503	SERVICE UNAVAILABLE	Der Server beantwortet (zeitweise) keine Requests.

Tabelle 7.7 HTTP-Statuscodes (Forts.)

Betrachten Sie nun den Auszug aus einem Mitschnitt des Netzwerkverkehrs. Dies dient als anschauliches Beispiel, wie die Protokolle der verschiedenen Schichten verschachtelt sind. Auf die Darstellung der Ethernet-Frames habe ich verzichtet.

Der Rechner `ze4` mit der IP-Adresse `192.168.0.34` stellt eine Anfrage an den HTTP-Server `netzbuch` mit der IP-Adresse `192.168.0.67`. Die Anfrage wird erfolgreich beendet. Sie können hier gut erkennen, wie zunächst auf TCP-Ebene die Verbindung aufgebaut wird (Zeilen 1, 2). Bei der Anfrage übermittelt der Client den Antwort-Port 35029. Dieser gilt, solange die Verbindung besteht.

Gut sehen Sie hier auch, dass das HTTP-Protokoll als Nutzlast des TCP transportiert wird. In Zeile 3 wird zunächst der Transport der Anfrage selbst per TCP geregelt, in Zeile 4 wird die HTTP-Anfrage angezeigt.

Zeile 5 zeigt Ihnen die Antwort des Servers mit dem HTTP-Statuscode (200, OK). In Zeile 6 bestätigt der Client-Rechner das Paket. Der Server-Rechner hat nichts mehr zu übermitteln und leitet mit dem `FIN`-Flag die Aufhebung der Verbindung ein (Zeile 7). Der Client bestätigt dies durch gleichzeitiges Übersenden eines `FIN`-Flags seinerseits (Zeile 8). Dessen Erhalt quittiert der Server-Rechner in Zeile 9, die Verbindung ist damit endgültig abgebaut.

Netzwerkverkehr bei einer HTTP-Anfrage

```

192.168.0.34 192.168.0.67 TCP 35029 > http [SYN] Seq=0
192.168.0.67 192.168.0.34 TCP http > 35029 [SYN, ACK] Seq=0 Ack=1
192.168.0.34 192.168.0.67 TCP 35029 > http [ACK] Seq=1 Ack=1
192.168.0.34 192.168.0.67 HTTP GET / HTTP/1.1
192.168.0.67 192.168.0.34 HTTP HTTP/1.1 200 OK (text/html)
192.168.0.34 192.168.0.67 TCP 35029 > http [ACK] Seq=202 Ack=919
192.168.0.67 192.168.0.34 TCP http > 35029 [FIN, ACK] Seq=919 Ack=202
192.168.0.34 192.168.0.67 TCP 35029 > http [FIN, ACK] Seq=202 Ack=920
192.168.0.67 192.168.0.34 TCP http > 35029 [ACK] Seq=920 Ack=203

```

7.3.2 Serverprogramme

Für jeden Einsatzbereich können Sie einen passenden Webserver verwenden. Die Programme

unterscheiden sich hinsichtlich ihres Leistungsvermögens und ihrer Ausstattungsdetails, wie der Einbindung diverser Skriptsprachen. Hier finden Sie eine kleine Übersicht von HTTP-Serverprogrammen:

thttpd: für kleine Projekte, z. B. auch Embedded-Anwendungen. Informationen erhalten Sie unter www.acme.com/software/thttpd/.

lighthttpd: ebenfalls für kleine Projekte geeignet, beherrscht mehrere Skriptmodule und Verschlüsselung. Die URL der Projektseite lautet <http://redmine.lighttpd.net/projects/lighttpd>.

Apache: ein weit verbreiteter Webserver mit vielen Erweiterungsmöglichkeiten, sehr leistungsfähig. Die URL des Apache-Projekts lautet www.apache.org.

Internet Information Services (IIS): Der IIS läuft im Gegensatz zu den anderen hier aufgeführten Programmen ausschließlich unter Microsoft-Windows-Betriebssystemen. Informationen über dieses kostenpflichtige Closed-Source-Produkt erhalten Sie unter www.microsoft.com/de-de/default.aspx.

Allen Webservern gemeinsam ist, dass die Webdokumente für Server, Administrator und gegebenenfalls Anwendungen zugänglich abgelegt werden. Je mehr Module und Plug-ins installiert werden, desto mehr belasten die Serverprozesse das Rechnersystem. Nicht nur in der Serversoftware selbst, auch in den Modulen und Plug-ins können sich Sicherheitslücken verbergen. Manche Erweiterungen können auch von ihrer Art her schon ein Sicherheitsproblem beinhalten, wenn es um Prozesse und Dateizugriffe geht.

Wenn es möglich ist, installieren Sie deshalb den Webserver in einer abgesicherten Umgebung (Linux: chroot; FreeBSD: chroot, Jail; allgemein: System in virtueller Maschine).

7.3.3 Client-Programme

Mit den HTTP-Servern kommunizieren Sie normalerweise per Webbrowser. Diese Programme unterscheiden sich hinsichtlich ihrer Bedienung und ihres Leistungsumfangs. HTTP-Clients arbeiten überwiegend im grafischen Modus. Dadurch können sie Bilder, Videos und andere Multimedia-Inhalte darstellen. Bekannte Programme sind:

- Firefox (www.mozilla.org)
- Opera (www.opera.com)
- Chrome (www.google.de/chrome)
- Internet Explorer (<https://support.microsoft.com/de-de/help/17621/internet-explorerdownloads>)
- Edge (www.microsoft.com/de-de/windows/microsoft-edge)
- Safari (www.apple.com/de/safari)

Auch für die reine Textdarstellung finden Sie HTTP-Clients (Abbildung 7.13). Diese können Sie für Verbindungen über sehr langsame Telefon- und Funkverbindungen, für reine webgestützte Wartungszugänge oder auch für Sehbehinderten-Arbeitsplätze einsetzen. In letzterem Fall führen Sie deren Ausgabe mit einer Braille-Zeile oder einer Sprachausgabe zusammen. Reine »Textbrowser« belasten zudem den PC kaum. So können Sie damit auch ältere Terminal-Arbeitsplätze oder Computerkassen mit einer Warenwirtschaftslösung verbinden. Aktive Inhalte kann keines dieser Programme darstellen (Flash, Video usw.).

Drei Vertreter dieses Programmtyps sind:

w3m: mit Mausbedienung

lynx: ohne Mausbedienung, dafür mit umfangreichem Menü

elinks: mit Mausbedienung

Alle Programme werden mit der Syntax

`<PROGRAMM> http://<URL>`

aufgerufen. Navigiert wird per Tastatur (Pfeiltasten, TAB, ENTER Taste) und teilweise (w3m, elinks) auch per Maus. Sie beenden diese Programme durch Druck auf die Taste Q (für quit)

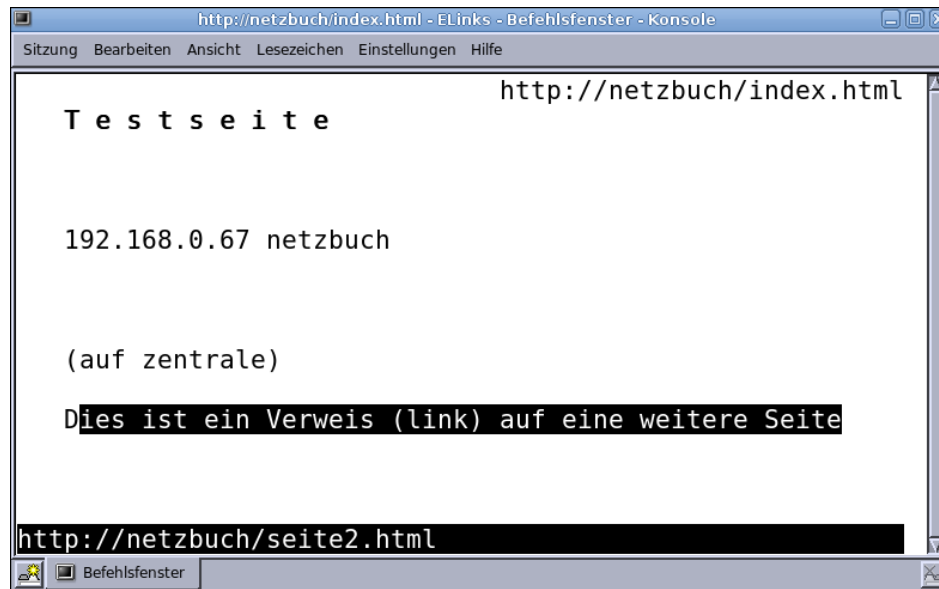


Abbildung 7.13 Darstellung einer Webseite mit »elinks«

Die genaue Funktionsbeschreibung der Webbrowser für den Textmodus entnehmen Sie den Manual-Seiten.

7.3.4 Webbrowser und Sicherheit

Moderne Webbrowser können durch Plug-ins zu Multimedia-Zentralen aufgerüstet werden. Die Programme dienen gerade bei Privatleuten mehr der Unterhaltung als dem Abrufen von reinen Informationen.

Werbeleute, die Seitenbetreiber selbst und auch die dunkle Seite der IT interessieren sich für den »Surfer« im Internet. Ältere Browser oder Plug-ins mit Sicherheitslücken bilden oftmals das Einfallstor für Angriffe vom Internet her. Von solchen Sicherheitsproblemen erfahren Sie ziemlich zeitnah z. B. auf www.heise.de.

Relative Sicherheit bietet Ihnen das folgende Vorgehen:

Verfolgen Sie Meldungen zu Sicherheitslücken.

Halten Sie Programme und Plug-ins aktuell.

Stellen Sie den Browser so ein, dass er keine Auskunft über die zuletzt besuchten Seiten gibt (Referrer).

Unterbinden Sie das Anlegen einer Historie und eines Caches. In der Historie lassen sich von Ihnen besuchte Seiten auslesen, im Cache lagern Daten (Bilder, Skripte usw.) davon.

Lassen Sie keine Cookies von Drittanbietern zu, und löschen Sie die vorhandenen beim Verlassen des Programms. Damit verhindern Sie, dass Ihre Verbindungen nachvollzogen werden.
Stellen Sie den Browser so ein, dass er keine Formulardaten speichert.
Benutzen Sie kein »Masterpasswort«, und lassen Sie das Speichern von Kennwörtern nicht zu.

Lassen Sie sogenannte *Add-ons* nicht automatisch installieren.

Internet-Café: Bringen Sie Ihren Browser auf einem USB-Stick mit. Benutzen Sie nicht den vom Surf-PC. Deaktivieren Sie Java/JavaScript wenigstens für unbekannte Seiten. Viele Browser lassen hier Ausnahmeregelungen und Sondereinstellungen für einzelne Seiten zu.
Damit unterbinden Sie die Ausführung aktiver Inhalte.

Weitere Hinweise finden Sie in Abschnitt 10.6, »Sicherheit«.

7.4 Mail-Transport

Ihre E-Mails können Sie auf verschiedene Arten senden und empfangen. Der Transport erfolgt im Hintergrund durch den *Mail Transport Agent (MTA)*, während Sie selbst den *Mail User Agent (MUA)* benutzen (Outlook, K-Mail, Evolution, Mutt, Alpine ...).

7.4.1 Grundlagen des SMTP/ESMTP-Protokolls

Ihre E-Mails werden mit dem *Simple Mail Transport Protocol (SMTP)* bzw. dem *Extended Simple Mail Transport Protocol (ESMTP)* übertragen. Oft hören Sie den Begriff *SMTP*, gemeint ist aber die neuere Version *ESMTP*. Der MTA benutzt das (E)SMTP-Protokoll.

Übersicht über das SMTP/ESMTP-Protokoll und den Mail-Transport

- ▶ Funktionsschema Mail-Transport: siehe [Abbildung 7.14](#)
- ▶ Wichtige Befehle: siehe [Tabelle 7.8](#)
- ▶ Statuscodes: siehe [Tabelle 7.9](#)

Sie können aus verschiedenen MTAs wählen:

- ▶ **exim**: leistungsfähig, ressourcenschonend, einfache Konfiguration (www.exim.org)
- ▶ **postfix**: für mittlere und größere E-Mail-Aufkommen, umfangreiche Ausstattung (www.postfix.org)
- ▶ **qmail**: für ISPs und sehr große E-Mail-Aufkommen (<http://cr.yp.to/qmail.html>)
- ▶ **MS EXCHANGE**: für Microsoft Windows (www.microsoft.com)
- ▶ Ports: 25/TCP, 465/TCP mit Verschlüsselung, 587/TCP
- ▶ RFCs zum Nachlesen: 1845, 1870, 1985, 2034, 2047, 2184, 2231, 2505, 2852, 2920, 3030, 3207, 3461, 3463, 3464, 3798, 3885, 3886, 4468, 4865, 4954, 5248, 5321, 5322, 5335, 5336, 5337, 6152, 6409, 6531, 6532, 6533, 6854, 7100, 7504, 7817

Der Absender einer E-Mail muss sich bei »seinem« SMTP-Server authentifizieren. Verlangt der Server keine Anmeldung, fungiert er als »Open-Relay« und damit als Verbreitungswerkzeug für unerwünschte E-Mails (Spam). Beim Einsatz des *SMTP-Auth* zur Authentifizierung können Sie folgende Verfahren einsetzen:

CRAM-MD5: *Challenge-Response Authentication Mechanism, Message Digest 5*; ein relativ sicheres Anmeldeverfahren, da keine Kennwörter im Klartext übertragen werden (siehe RFCs 2104, 2195 und 6151)!

LOGIN: Benutzername und Kennwort werden in zwei Schritten unverschlüsselt

übertragen. Die verwendete Base64-Codierung ist keine Verschlüsselung im eigentlichen Sinne.

NTLM: *NT-LAN-Manager*, ein proprietäres Anmeldeverfahren von Microsoft.

PLAIN: Benutzername und Kennwort werden in einem Schritt unverschlüsselt übertragen.

Die verwendete Base64-Codierung ist keine Verschlüsselung im eigentlichen Sinne (siehe RFC 4616).

SCRAM-SHA-1: *Salted Challenge Response Authentication Mechanism*, relativ sichere Anmeldemethode mit Verschlüsselung (siehe RFC 5808).

Bevorzugen Sie auch im Intranet verschlüsselte Anmeldeverfahren. Moderne MTAs beherrschen eine oder mehrere Formen davon.

Gegen das unerwünschte Mitlesen von E-Mails während des Transports helfen verschiedene Verschlüsselungstechniken: für die Übertragung als solche (SSL/TLS) und auch für den Inhalt. Hier gibt es mehrere Standards. Sie müssen vorher mit dem Empfänger absprechen, welche Verschlüsselungsmethode er »versteht«.

Der Mail-Transport besteht aus mehreren Phasen. Sie senden von Ihrem PC aus mit Ihrem E-Mail-Programm eine Nachricht per SMTP ab. Ihr Programm authentifiziert sich beim SMTP-Server Ihres Providers. Dieser Server verfügt über einen eigenen SMTPClient. Dieser leitet die Nachricht ebenfalls per SMTP an den Mail-Server beim Provider des Empfängers weiter. Der empfangende Server gleicht möglicherweise die Adresse des sendenden SMTPs mit einer »Blacklist« (hier werden Spam-Server geführt) ab.

Hierzu muss der DNS-Zugriff funktionieren. Der Empfänger der E-Mail kann auf die E-Mail aber nicht mittels SMTP zugreifen. Für das Abholen muss er Protokolle wie POP3 oder IMAP benutzen, wenn er die Mails auf seinen lokalen Rechner übertragen möchte. Alternativ bieten viele Provider Webmail-Lösungen an. Hier greifen Sie mittels Webbrowser mit HTTPS auf Ihre E-Mails auf dem Server (Schreiben und Lesen) zu.

In Abbildung 7.14 zeige ich Ihnen schematisch den Lauf einer E-Mail. Die Webmail-Lösung habe ich dabei nicht dargestellt.

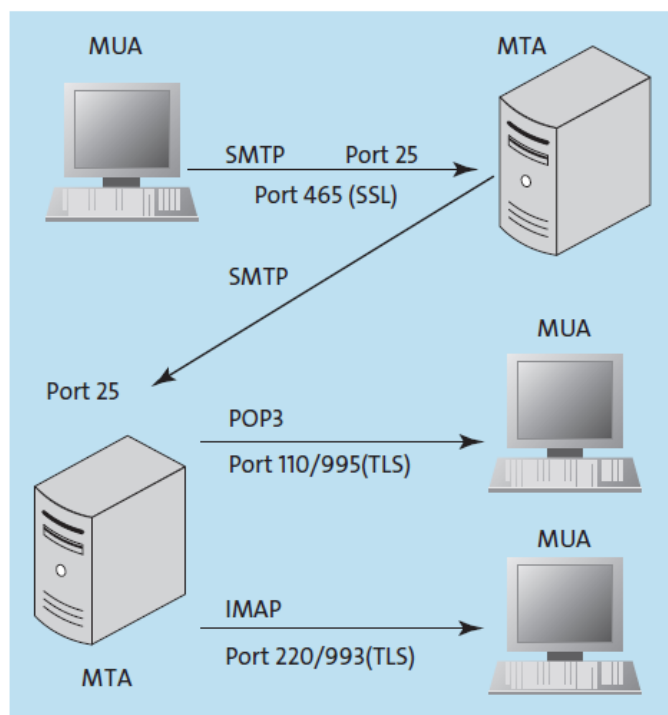


Abbildung 7.14 Schema des Transportwegs einer E-Mail

Der SMTP-Client sendet im Dialog mit dem Server verschiedene Kommandos. Eine Auswahl finden Sie in Tabelle 7.8.

Kommando	Aktion
EHLO <RECHNERNAME>	Beginn der SMTP-Sitzung; der Server teilt Ihnen mit, welche SMTP und ESMTP-Kommandos er anbietet.
HELO <RECHNERNAME>	Beginn der SMTP-Sitzung

Tabelle 7.8 Auswahl an SMTP-Kommandos

Kommando	Aktion
MAIL FROM <ABSENDER>	Beginn der E-Mail-Übertragung mit Angabe der Absenderadresse
NOOP	Beim Leerlauf in der Sitzung bekommen Sie damit eine Antwort vom Server. Damit verhindern Sie einen Abbruch wegen Zeitüberschreitung (Time-out).
QUIT	Beenden der SMTP-Sitzung
RCPT TO <EMPFÄNGER>	Angabe der oder des Empfängers (mehrfach je Nachricht möglich)
RSET	Abbruch einer bereits eröffneten E-Mail-Übertragung, ohne die bestehende Verbindung zu beenden
VRFY	Überprüfung der Empfängeradresse

Tabelle 7.8 Auswahl an SMTP-Kommandos (Forts.)

Der SMTP-Server sendet Ihnen bzw. Ihrem E-Mail-Client während der Verbindung Statuscodes als Antwort auf die einzelnen Aktionen. In Tabelle 7.9 finden Sie eine Auswahl.

Code	Text	Bedeutung
220	SERVICE READY	Der Server ist bereit, Anweisungen entgegenzunehmen.
221	CLOSING CHANNEL	Der Server trennt die Sitzung.
250	OK	Das Kommando wurde erfolgreich ausgeführt.
354	START MAIL INPUT	Aufforderung zur Übermittlung der E-Mail
421	<DOMAIN> SERVICE NOT AVAILABLE. CLOSING TRANSMISSION CHANNEL	Die Domain ist nicht verfügbar, die Verbindung wird getrennt.
500	SYNTAX ERROR, COMMAND UNRECOGNISED	Fehler im Kommando
501	SYNTAX ERROR, NO PARAMETERS ALLOWED	Fehler im Kommando, keine weiteren Parameter zulässig
502	COMMAND NOT IMPLEMENTED	Das Kommando ist entweder unbekannt oder nicht verfügbar.

Tabelle 7.9 SMTP-Statuscodes

Code	Text	Bedeutung
503	BAD SEQUENCE OF COMMANDS	falsche Reihenfolge der übermittelten Kommandos
504	COMMAND PARAMETER NOT IMPLEMENTED	Dieser Parameter im Kommando nicht möglich.
554	TRANSACTION FAILED	Übermittlung fehlgeschlagen oder kein SMTP-Service verfügbar

Tabelle 7.9 SMTP-Statuscodes (Forts.)

7.4.2 Konfigurationshinweise

Wenn Sie selbst einen SMTP-Server für Ihr Netz installieren, können Sie verschiedene Einsatzbereiche festlegen:

Der Server dient nur netzinternem E-Mail-Verkehr. Er verweigert E-Mails mit Adressen »von außerhalb« die Weiterleitung, und er leitet keine E-Mails »nach außen«.

Der Server dient dem netzinternen E-Mail-Verkehr und sendet ausgehende E-Mails in das Internet.

Der Server sendet ausschließlich ausgehende E-Mails weiter.

Testen Sie vor dem Echteininsatz Ihres SMTP-Servers, ob

Sie keine E-Mails mit beliebigem Absender darüber versenden können (Spam-Relay!),

abgehende E-Mails eine vollständige und richtige Absenderadresse aufweisen und ob

die Verbindung zu einem SMTP-Relay Ihres Internet-Providers verschlüsselt funktioniert.

Die ersten Funktionsprüfungen können Sie übrigens mit dem `telnet`-Client vornehmen. Mit einem E-Mail-Client (MUA) als Testobjekt laufen Sie Gefahr, dass falsche oder zu allgemeine Fehlermeldungen ausgegeben werden. Dies würde die Nachkonfiguration erschweren. Allerdings können Sie mit dieser Methode nur unverschlüsselte E-Mail-Übertragungen prüfen. Sie bauen die Verbindung in der Form

```
telnet <RECHNERNAME> 25
```

oder

```
telnet <IPADRESSE> 25
```

auf. Zwischen `<RECHNERNAME>` oder `<IP-ADRESSE>` und der Port-Angabe 25 steht ein Leerzeichen.

Zunächst sehen Sie in Abbildung 7.15 die Abfrage allgemeiner Einstellungen und angebotener Kommandos.

```

harald@ZE4:~$ telnet 192.168.0.67 25
Trying 192.168.0.67...
Connected to 192.168.0.67.
Escape character is '^]'.
220 netzbuch.example.com ESMTP Exim 4.74 Sun, 24 Jul 2011 08:58:09 +0000
ehlo ze4
250-netzbuch.example.com Hello ze4 [192.168.0.34]
250-SIZE 52428800
250-PIPELINING
250 HELP
help
214-Commands supported:
214 AUTH HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
quit
221 netzbuch.example.com closing connection
Connection closed by foreign host.
harald@ZE4:~$

```

Abbildung 7.15 Abfrage verfügbarer Kommandos

In Abbildung 7.16 sehen Sie den kompletten Ablauf einer E-Mail-Lieferung an den SMTPServer.

```

harald@ZE4:~$ telnet 192.168.0.67 25
Trying 192.168.0.67...
Connected to 192.168.0.67.
Escape character is '^]'.
220 netzbuch.example.com ESMTP Exim 4.74 Sun, 24 Jul 2011 08:54:00 +0000
helo ze4
250 netzbuch.example.com Hello ze4 [192.168.0.34]
mail from: harald@example.com
250 OK
rcpt to: harald@netzbuch.example.com
250 Accepted
data
354 Enter message, ending with "." on a line by itself
Das ist eine Testmail.
.
250 OK id=1QkuSF-0000s1-Ke
quit
221 netzbuch.example.com closing connection
Connection closed by foreign host.
harald@ZE4:~$

```

Abbildung 7.16 Manueller Test einer E-Mail-Übertragung

7.4.3 Anhänge von E-Mails, MIME, S/MIME

E-Mails können nur Text transportieren. Der Text muss zudem im *ASCII-Code* (*American Standard Code for Information Interchange*) vorliegen. Damit Sie in Ihren E-Mails auch Umlaute benutzen und Dateien anhängen können, gibt es Erweiterungen (*Multipurpose Internet Mail Extensions*, *MIME*, und für die Verschlüsselung von E-Mails *Secure MIME*, *S/MIME*).

Die MIME-Erweiterungen codieren Nicht-ASCII-Texte und Anhänge (Binärcode, Bilder, Multimedia-Dateien) in ASCII-Zeichenfolgen um. Nur mit diesen kann das E-Mail-System umgehen. Beim Empfänger werden diese Anhänge wieder in das Originalformat zurückverwandelt.

MIME-Erweiterung, Codierungen

Codierungen:

7bit: nur ASCII

8bit: ASCII und einzelne Sonderzeichen

Nicht-ASCII-Texte: *Quoted-Printable*-Verfahren. Sie codieren alle Bytes außerhalb des ASCII-Zeichensatzes. Das umgewandelte Zeichen trägt als Kennzeichnung das »=«-Zeichen. Der Zeichenwert in hexadezimaler Form schließt sich daran an.

Binäre Anhänge und zum Teil Texte: Sie codieren alle Nicht-Text-Anhänge (Binärdaten aller Art) mittels *Base64* in ASCII-Text.

MIME-Parts: Die MIME-Spezifikation ist in mehrere Sektionen unterteilt:

Part 1: Erweiterungen des Mail-Headers

Part 2: Typ des Inhalts

Part 3: Mail-Header-Erweiterungen für Nicht-ASCII-Text

Part 4: Registrierungsprozedur von neuen Erweiterungen bei der IANA

Part 5: Mindestanforderungen an MUAs

RFCs: 1847, 2045, 2046, 2047, 2049, 2131, 2184, 2231, 2822, 3023, 3396, 3548, 3676, 3798, 4288, 4289, 4361, 4648, 4829, 5147, 5322, 5335, 5336, 5494, 6532, 6657, 6842

MIME kennt derzeit nur die Version 1.0. Sie verwenden diesen Eintrag ohne Änderung.

MIME kennt verschiedene Inhaltstypen. Diese finden Sie als Content-Type-Eintrag im Kopfbereich der E-Mail:

application: angehängte Datei mit Zuordnung zu einer Anwendung

audio: Audiodatei

image: Grafikdatei

multipart: Daten sind mehrteilig.

text: Textdatei

video: Videodatei

Am Content-Type-Eintrag finden Sie eine weitere Beschreibung des Inhalts. Bei Texten finden Sie Hinweise zum Zeichensatz (`Text/Plain charset="<ZEICHENSATZ>"`). In Tabelle 7.10 finden Sie eine kleine Übersicht häufig vorkommender Content-Type-Einträge.

Content-Type (MIME-Type)	Inhalt
text/plain	blanker Text
text/html	HTML-Text
multipart/mixed	mehrteilige Daten in verschiedenen Formaten (Text, Bilder ...)

Tabelle 7.10 Inhaltsbeschreibungen

Nach der Inhaltsbeschreibung enthalten E-Mails einen weiteren Eintrag über die Art der Codierung (siehe den vorherigen Kasten »MIME-Erweiterung, Codierungen«).

Betrachten Sie zunächst in Listing 7.2 das Beispiel einer reinen Text-Mail, deren Inhalt im heute weitverbreiteten Zeichensatz `utf8` abgefasst ist:

```
From: Harald Zisler <harald@example.com>
To: harald@example.com
Subject: Test Umlaute =?utf-8?b?w5bDhMOcw58=?=
Date: Mon, 25 Jul 2016 23:06:38 +0200
User-Agent: KMail/1.13.5 (Linux/2.6.32-5-amd64; KDE/4.4.5; x86_64; ; )
MIME-Version: 1.0
Content-Type: Text/Plain;
charset="utf-8"
Content-Transfer-Encoding: base64
.....
VGZvdCBVbWxhdXRIL1NvbmlRlcnplaWNoZW46CgrDpMO2w7zDn8OEw5bDnED
```

Listing 7.2 E-Mail mit Umlauten

Im Folgenden zeige ich Ihnen ein weiteres Beispiel. Diesmal handelt es sich um eine E-Mail mit dem Content-Type `multipart`. In der E-Mail befinden sich eine Grafik- und eine HTML-Datei, etwas Text und ein ZIP-Archiv. Die einzelnen Anhänge einer E-Mail des Typs `multipart` werden durch die `boundary`-Einträge voneinander getrennt. Sie bilden eine Art »Zwischenüberschrift«, in der unter anderem der Content-Type der folgenden Daten angegeben wird. Ein weiterer `boundary`-Eintrag mit zwei Strichen am Ende seiner Zeichenkette schließt die Reihe der Anhänge ab.

```

From: Harald Zisler <harald@example.com>
To: harald@example.com
Subject: Mehrere =?iso-8859-1?q?Anh=E4nge?=
Date: Tue, 26 Jul 2016 20:35:52 +0200
User-Agent: KMail/1.13.5 (Linux/2.6.32-5-amd64; KDE/4.4.5; x86_64; ; )
MIME-Version: 1.0
Content-Type: Multipart/Mixed;
boundary="Boundary-00=_lkwLOSj9eA6z3cS"
--Boundary-00=_lkwLOSj9eA6z3cS
Content-Type: Text/Plain;
charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Diese Mail hat mehrere Anh=E4nge!
--Boundary-00=_lkwLOSj9eA6z3cS
Content-Type: image/jpeg;
name="img_0604.jpg"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="img_0604.jpg"
/9j/4TP+RXhpZgAASUkqAAgAAAAKAA4BAgAgAAAAhgAAAA8BAgAGAAAApg
.....
fy7eUvGo34wT61ZXxC8tmbZ1yq/dNFrk2OfMki3CurYH1pbiVpiSRk+tWg
--Boundary-00=_lkwLOSj9eA6z3cS
Content-Type: text/html;
charset="UTF-8";
name="index.html"
Content-Transfer-Encoding: 7bit
Content-Disposition: attachment;
filename="index.html"
<html>
<head><meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<style>
.Normal
.....
</body>

</html>
--Boundary-00=_lkwLOSj9eA6z3cS
Content-Type: application/x-compressed-tar;
name="modern.tgz"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
filename="modern.tgz"
H4slCKORFEwAA21vZGVtLnRhcgDsvGVsHc+/5nmOmZmZ2Y6Z7ZiZmZmZ2c
.....
+bCMTAGn65n/o59AN27cuHHjxo0bN27cuHHjxo0bN27cuHHjxo0bN27cuH
--Boundary-00=_lkwLOSj9eA6z3cS—

```

Listing 7.3 E-Mail mit mehreren Anhängen

In Abbildung 7.17 sehen Sie die in Listing 7.3 gezeigte E-Mail im MUA.

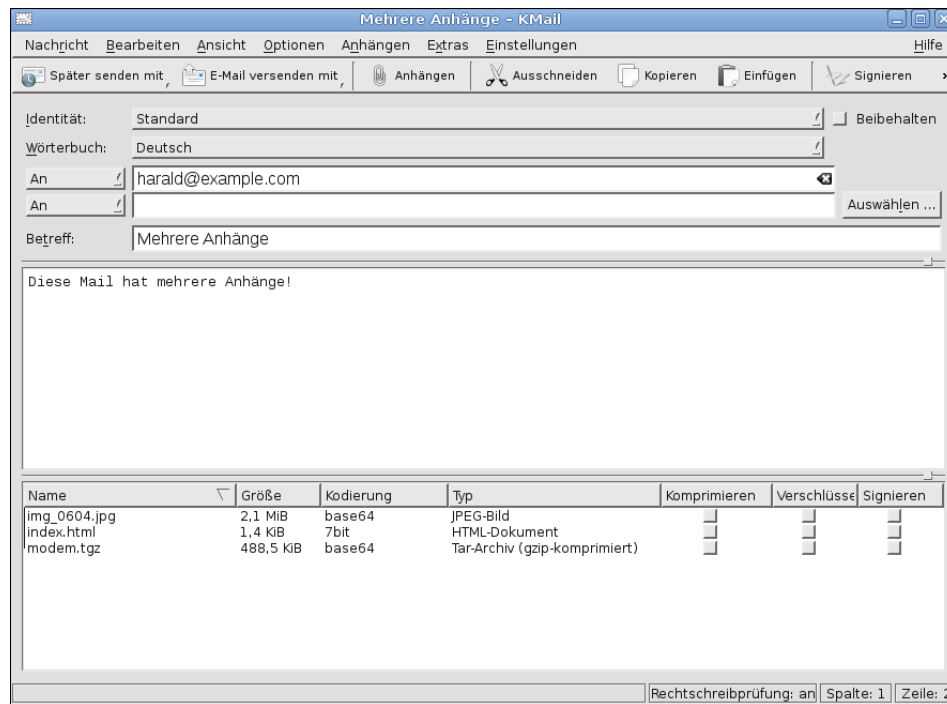


Abbildung 7.17 Multipart-E-Mail

7.5 Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)

In diesem Abschnitt stelle ich Ihnen Verschlüsselungsmöglichkeiten für Datenübertragungen und Fernsitzungen vor.

7.5.1 Secure Shell (SSH)

Mit SSH können Sie gleichermaßen verschlüsselte Fernsitzungen als auch Datenübertragungen vornehmen. Wenn Sie zwei Rechner über das Internet kommunizieren lassen, können Sie mit SSH einen Tunnel einrichten. Dieser schützt dann auch unverschlüsselte Daten vor Mitlesern.

Allgemeines über SSH

- ▶ Ersetzt unter anderem die unverschlüsselt übertragende Anwendungen rcp und rlogin sowie ftp
- ▶ Einbettungen in weiteren Protokollen (X11, verschlüsselte grafische Fernsitzung)
- ▶ Angewandte Version: 2
- ▶ Port: 22 (Standard, beliebig anders konfigurierbar)
- ▶ SSH-Key: Sie benötigen einen privaten und einen öffentlichen Schlüssel. Diese erzeugen Sie mit dem OpenSSH-Programmpaket selbst.
- ▶ Authentifizierung: mit RSA-Zertifikat, siehe SSH-Key
- ▶ Verschlüsselungsarten: Standard: AES 128 Bit, möglich: 3DES, Blowfish, Twofish, CAST, IDEA, Arcfour, SEED und AES mit anderer Schlüssellänge
- ▶ Implementierungen: SSH (kommerziell), OpenSSH (Linux, FreeBSD, Unix), PuTTY (Client-Programm) mit sftp und scp (Windows, Linux, FreeBSD), freeSSHd (Windows)
- ▶ RFCs: 4250, 4251, 4252, 4253, 4254, 4256, 4335, 4419, 4432, 4462, 4716, 4819, 5656, 6187, 6668, 6797

Sie haben für SSH-Verbindungen zwei Möglichkeiten der Authentifizierung:

Anmeldung per Kennwort: Sie müssen bei der Verbindungsaufnahme immer ein Kennwort eingeben.

Anmeldung per Public-Key-Authentifizierung: Hier müssen Sie kein Kennwort eingeben.
 Ihr Client-Programm übermittelt einen privaten Schlüssel an das Zielsystem.
 Den öffentlichen Schlüssel Ihres Systems haben Sie zuvor auf diesem Zielsystem hinterlegt.
 Damit können Sie SSH auch für Skripte einsetzen, die ohne Benutzereingriff laufen.

Die praktische Anwendung von SSH wird in den folgenden Abschnitten des Buches beschrieben:

Abschnitt 9.1.3, »Benutzerkommandos für FTP- und SFTP-Sitzungen«
 Abschnitt 9.1.4, »Datentransfer mit ›netread‹ und ›netwrite‹«
 Abschnitt 9.1.5, »Verschlüsselte Datentransfers und Kommandoausgaben mit ›cryptcat‹«
 Abschnitt 9.2, »SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung«
 Abschnitt 9.3, »Aufbau eines SSH-Tunnels«

7.5.2 SSL und TLS

Mit SSL (Bezeichnung vor der Version 3.0) bzw. TLS (neue Bezeichnung ab Version 3.0) steht Ihnen ein Verschlüsselungsprotokoll für die Datenübertragung zur Verfügung. Es wird Ihnen in der Praxis hauptsächlich bei HTTP (→ HTTPS), SMTP, NNTP, IMAP und POP3 begegnen. Dieses Protokoll verfügt über einen zweischichtigen Aufbau. Direkt auf TCP setzt das *SSL Record Protocol* auf. Dieses nimmt die Verschlüsselung der Verbindung vor. Darüber liegen auf gleicher Ebene das *SSL Handshake Protocol*, das *SSL Change Cipher Specification Protocol*, das *SSL Alert Protocol* und das *SSL Application Data Protocol*.

Diese Protokolle haben folgende Aufgaben:

SSL Handshake Protocol: Authentifizierung und Identifikation der beteiligten Netzwerkteilnehmer

SSL Change Cipher Specification Protocol: Annahme der beim Handshake ausgehandelten

Parameter für die aktuelle Sitzung. Größe: 1 Byte, Inhalt: 1

SSL Alert Protocol: Entdeckt einer der beteiligten Rechner einen Übertragungsfehler, sendet er eine Fehlermeldung. Sie enthält 2 Byte. Mit dem ersten Byte kennzeichnet das Protokoll die »Wertigkeit« des Fehlers (*warn* (1) oder *fatal* (2)). Das zweite Byte enthält den Fehlercode (Tabelle 7.11). Diese Tabelle hilft Ihnen bei der Fehlerklärung, wenn besonders bei selbst geschriebenen Programmen keine Verbindung zustande kommen will.

SSL Application Data Protocol: Über dieses Protokoll kommuniziert TLS mit der darüberliegenden Anwendung (z. B. HTTP-Server).

RFCs: 2595, 2712, 2817, **2818**, **3207**, 3749, 4162, 4217, 4261, 4279, 4492, 4510, 4511, 4513, 4572, 4616, 4642, 4680, 4681, 4785, 5054, 5077, **5216**, 5238, **5246**, 5281, 5288, 5289, 5311, 5425, 5469, 5487, 5489, 5705, 5746, 5763, 5764, 5785, 5878, 5929, 5932, 6012, 6042, **6066**, 6083, 6084, 6091, 6125, 6176, 6209, 6251, 6347, 6353, 6460, 7027, 7230, 7231, 7465, 7507, 7568, 7589, 7627, 7685, 7817

Fehler-Code	Nachricht	Bedeutung	Wertigkeit
0	close_notify	Schließen der aktuellen Verbindung	1
10	unexpected_message	unpassende Nachricht erhalten	2
20	bad_record_mac	Record-Protocol: Eigener MAC-Wert stimmt nicht mit empfangenem überein.	2
30	decompression_failure	Fehler beim Dekomprimieren der Daten	2
40	handshake_failure	kein Ergebnis beim Aushandeln der Sicherheitsparameter erzielt	2
41	no_certificate	Client besitzt kein passendes Zertifikat (Antwort nach certificate_request).	1
42	bad_certificate	Signatur des Zertifikats fehlerhaft	1
43	unsupported_certificate	Zertifikattyp nicht unterstützt	1
44	certificate_revoked	Zertifikat wurde vom Aussteller (CA) widerrufen.	1
45	certificate_expired	Zertifikat abgelaufen	1

Tabelle 7.11 Fehlercodes und zugeordnete Wertigkeiten des SSL Alert Protocols

7.6 Praxisübungen

Hier können Sie wieder Ihr Wissen anwenden. Die Auflösungen finden Sie in Anhang B, »Auflösungen zu den Prüfungsfragen«.

7.6.1 Konfiguration des Samba-Servers

1. Welchen Namen hat die zentrale Konfigurationsdatei des Samba-Servers?
2. Mit welchem Programm können Sie diese Datei auf ihre syntaktische Richtigkeit hin testen?

7.6.2 NFS-Server

Wie sichern Sie Ihren Server gegen unerwünschte Zugriffe von außen ab? Die Adresse Ihres Servers lautet 192.168.3.80.

7.6.3 HTTP, Sicherheit

1. Sicherheit im Webbrowser: Mit welcher Einstellung verhindern Sie, dass Ihre bisher besuchten Webseiten vom aktuell besuchten Server ausgelesen werden?
2. Sicherheit bei der Kommunikation von Browser und Server: Was setzen Sie am Server ein, damit die Verbindungen nicht mitgelesen werden können?
3. Sicherheit im Webbrowser: Nennen Sie wenigstens drei Einstellungen zur Erhöhung von Sicherheit und Datenschutz.

7.6.4 E-Mail

1. Was bezeichnet der Begriff *MTA*?
2. Mit welchem Eintrag in einer E-Mail werden verschiedene Inhalte unterteilt?
3. Mit welcher Abfrage können Sie (meist) die Kommandos eines SMTP-Servers ermitteln?

Kapitel 8

Standards für den Datenaustausch

Beim Suchen von Fehlern und Sicherheitslücken in Computersystemen und Netzwerken werden Sie allerlei Dateiformaten begegnen. Egal, ob böswillige Kollegen oder Mitarbeiter wertvolle CAD-Daten per FTP direkt der Konkurrenz zuspielen oder ein zentraler Dienst bei jedem Zusammentreffen mit bestimmten Inhalten seine Mitarbeit aufkündigt, Sie können nicht alle Dateiformate und ihre Herkunft (im Sinne des Erzeugerprogramms) kennen. Dafür finden Sie in diesem Kapitel für das schnelle Nachschlagen eine Tabelle (Tabelle 8.1). In ihr finden Sie eine große Anzahl immer wieder auftauchender Dateiendungen und die Informationen dazu.

Falls Sie ein Linux-, FreeBSD- oder Unix-System pflegen, hilft Ihnen auch das `file`-Kommando, das Ihnen den Dateityp ermittelt. Unter diesen Systemen erkennen Sie ausführbare Dateien nicht an einer Endung, sondern nur an den Attributen (wenigstens `rx`).

Endung	Typ	Beschreibung
<i>123</i>	Tabellenkalkulation	Lotus 1-2-3
<i>adt</i>	Datenbank	Sybase Advantage Database Server
<i>afm</i>	Font	Metrics von Adobe Fonts
<i>apt</i>	Datenbank	Lotus Notes
<i>arj</i>	komprimiertes Archiv	MS-DOS: <i>arj</i> und weitere Archiv- und Packprogramme
<i>asp</i>	Dokument	dynamisch erzeugte Webseite, Microsoft Active Server Page
<i>bak</i>	verschiedene	Sicherungskopie einer Datei, vom Programm beim Öffnen zum Bearbeiten angelegt
<i>bat</i>	Skript	MS-DOS Stapelverarbeitungsdatei

Tabelle 8.1 Übersicht über häufig vorkommende Dateinamenendungen

Endung	Typ	Beschreibung
<i>bmp</i>	Grafik	Grafikdateien; MS-Paint und andere
<i>brd</i>	CAD	CAD-Daten, EAGLE Leiterplatten-Editor
<i>bz2</i>	Kompression	komprimierte Datei, <i>bzip2</i>
<i>c</i>	Quellcode	Programmiersprache C
<i>c++</i>	Quellcode	Programmiersprache C++
<i>cab</i>	Softwarepaket	komprimierte Installationsarchive (Microsoft)
<i>cmd</i>	Skript	MS Windows Stapelverarbeitungsdatei
<i>com</i>	Programm	MS-DOS, Programme, die einzelne Befehle darstellen
<i>conf</i>	Programm	Datei mit Einstellungen für Programme (Linux, FreeBSD, Unix)
<i>cpp</i>	Quellcode	Programmiersprache C++
<i>csv</i>	Dokument	Daten im Textformat; Trennung der Felder meist durch die Zeichen »,« und »;«
<i>db</i>	Datenbank	SQLite
<i>dbf</i>	Datenbank	Datenbank dbase II-V, Clipper, FoxPro
<i>deb</i>	Softwarepaket	Programmpaket für Debian oder darauf basierende Linux-Distributionen
<i>dll</i>	Bibliothek	Programmbibliothek unter MS Windows
<i>doc, docx</i>	Dokument	Microsoft Word
<i>dot, dotm</i>	Dokument	Vorlage für Microsoft Word
<i>dtp</i>	Dokument	GST Press Works
<i>dvi</i>	Dokument	Device Independent; wird durch LaTeX erzeugt
<i>dwb</i>	CAD	CAD-Daten, VariCAD
<i>dwg</i>	CAD	CAD-Daten, AutoCAD
<i>dxf</i>	CAD	CAD-Daten, AutoCAD
<i>eps</i>	Grafik	PostScript-Bild; Encapsulated PostScript

Tabelle 8.1 Übersicht über häufig vorkommende Dateinamenendungen (Forts.)

Endung	Typ	Beschreibung
<i>exe</i>	Programm	Programm unter MS-DOS oder MS Windows
<i>fdb</i>	Datenbank	Firebird, Navision
<i>fig</i>	Grafik	Bildformat von <i>xfig</i>
<i>flac</i>	Sound	Codec-Datei des Ogg-Projekts
<i>fm</i>	Dokument	Adobe Frame Maker
<i>gz</i>	Kompression	komprimierte Datei, <i>gzip</i>
<i>html</i>	Dokument	Hypertext Markup Language, meist Webseiten
<i>img</i>	Abbilddatei	Abbilddatei von Disketten im MS-DOS-Format (FAT)
<i>indd</i>	Dokument	Adobe InDesign
<i>ini</i>	Programm	Einstellungen für Programme, überwiegend im Bereich Microsoft Windows
<i>ipg</i>	Softwarepaket	enthält Programmpakete mit Spielen für den iPod der Firma Apple Inc.
<i>iso</i>	Abbilddatei	Abbilddatei einer CD, DVD oder Blu-Ray-Disc
<i>jar</i>	Programm	Klassendateien für Java-Anwendungen
<i>java</i>	Quellcode	Programmiersprache Java
<i>jpg</i>	Grafik	JPEG-Bildformat
<i>js</i>	Skript	JavaScript-Datei
<i>lzh</i>	komprimiertes Archiv	komprimiertes Archiv, LHA
<i>mdb</i>	Datenbank	Microsoft Access
<i>mdf</i>	Datenbank	Microsoft SQL Server
<i>mp3</i>	Sound	komprimiertes Audioformat MPEG Layer 3
<i>mp4</i>	Video	Videoformat der <i>Moving Picture Experts Group</i> , für iPod von Apple Inc.
<i>mpeg</i>	Video	Videoformat der <i>Moving Picture Experts Group</i>
<i>nsf</i>	Datenbank	Lotus-Notes-Datenbank

Tabelle 8.1 Übersicht über häufig vorkommende Dateinamenendungen (Forts.)

Endung	Typ	Beschreibung
<i>odb</i>	Datenbank	Open-Document-Datenbank, LibreOffice, OpenOffice
<i>odp</i>	Dokument	Präsentation, Open-Document-Format, LibreOffice, OpenOffice
<i>ods</i>	Tabellenkalkulation	Open-Document-Format, LibreOffice, OpenOffice
<i>odt</i>	Dokument	Open-Document-Format, Textverarbeitung, LibreOffice, OpenOffice
<i>ora</i>	Datenbank	Oracle-Datenbank-Daten
<i>pbm</i>	Grafik	Portable Bitmap
<i>pdb</i>	Datenbank	Palm-OS-Datenbank
<i>pdf</i>	Dokument	Portable-Document-Format, Adobe
<i>pfa</i>	Font	PostScript, Drucker-Fonts
<i>pfb</i>	Font	Drucker-Fonts, Adobe
<i>pfm</i>	Font	Metrics für Adobe-Drucker-Fonts
<i>php</i>	Skript	PHP-Skripte, auf Webservern
<i>pl</i>	Skript	Perl-Skript
<i>png</i>	Grafik	PNG-Format
<i>pnm</i>	Grafik	Portable Anymap Bitmap Image
<i>ppt</i>	Dokument	PowerPoint-Präsentation (Microsoft)
<i>ps</i>	Dokument	PostScript, bei Linux, FreeBSD und Unix verbreitet
<i>py</i>	Skript	Python-Skript
<i>raw</i>	Multimedia	Rohdaten eines Aufnahmegeräts (Scanner, Kamera [Bild/Video])
<i>rpm</i>	Programmpaket	<i>Red Hat Paket Manager</i> , verwenden viele Linux-Distributionen (Red Hat, Fedora, OpenSuse ...).
<i>rtf</i>	Dokument	<i>Rich Text Format</i> , Austauschformat
<i>sh</i>	Skript	Shell-Skript-Code (<i>sh</i> , <i>bash</i> , <i>zsh</i> ...)
<i>sql</i>	Datenbank	Datenbankabfragen, Kommandostapel

Tabelle 8.1 Übersicht über häufig vorkommende Dateinamenendungen (Forts.)

Endung	Typ	Beschreibung
<i>svg</i>	Grafik	<i>Scalable Vector Graphic</i> , z. B. von Inkscape
<i>tar</i>	Archiv	Archivdatei, <i>tar</i>
<i>tar.bz2</i>	komprimiertes Archiv	komprimiertes Archiv, mit <i>tar</i> erstellt und mit <i>bzip2</i> komprimiert
<i>tar.gz</i>	komprimiertes Archiv	komprimiertes Archiv, mit <i>tar</i> erstellt und mit <i>gzip</i> komprimiert
<i>tbz</i>	komprimiertes Archiv	komprimiertes Archiv, in einem Lauf mit <i>tar</i> erstellt und mit <i>bzip2</i> komprimiert (<i>tar cfj</i>)
<i>tcl</i>	Skript	TCL/TK-Skriptsprache
<i>tcw</i>	CAD	CAD-Daten, TurboCAD
<i>tex</i>	Dokument	TeX- oder LaTeX-Dokument
<i>tfm</i>	Font	Metrics für TeX-Fonts
<i>tgz</i>	komprimiertes Archiv	komprimiertes Archiv, in einem Lauf mit <i>tar</i> erstellt und mit <i>gzip</i> komprimiert (<i>tar cfz</i>)
<i>tif</i>	Grafik	<i>Tagged Image File Format</i>
<i>ttf</i>	Font	TrueType-Fonts
<i>txt</i>	Dokument	reiner Text (ASCII, DIN-ISO, UTF8)
<i>vb</i>	Quellcode	Programmiersprache Microsoft Visual Basic.NET
<i>vbs</i>	Skript	Microsoft Visual Basic
<i>vdi</i>	Abbilddatei	Oracle Virtual Box, Abbild virtueller Platten
<i>wav</i>	Sound	Wave-Datei, Microsoft
<i>wma</i>	Sound	Microsoft Windows Media Audio
<i>xcf</i>	Grafik	Grafikformat von Gimp
<i>xls, xlsx</i>	Tabellenkalkulation	Microsoft Excel
<i>xml</i>	Dokument	Extensible Markup Language
<i>Z</i>	komprimiertes Archiv	komprimiertes Archiv, Unix-Compress
<i>zip</i>	komprimiertes Archiv	komprimiertes Archiv, PKZIP, ZIP

Tabelle 8.1 Übersicht über häufig vorkommende Dateinamenendungen (Forts.)

Kapitel 9 - Netzwerkanwendungen

In diesem Kapitel möchte ich Ihnen einige Möglichkeiten zeigen, wie man Daten über das Netzwerk überträgt und Fernsitzungen abhält. Manches davon habe ich in den zurückliegenden Kapiteln schon vorweggenommen. Sie finden deshalb anstelle von Wiederholungen Verweise darauf.

9.1 Datenübertragung

Fast alle Verfahren der Datenübertragung eignen sich für das lokale Netzwerk ebenso wie für das Internet. Die Netzzugänge verfügen in vielen Fällen über die notwendige Bandbreite. Unverschlüsselte Verfahren wie Samba, teilweise NFS und FTP, können Sie mittels SSH-Tunnel benutzen. Beachten Sie aber, dass NFS für eine WAN-Übertragung trotzdem schlecht geeignet ist. Latenzzeiten, die von Routern und Firewalls verursacht werden, setzen hier die effektive Übertragungsgeschwindigkeit enorm herunter.

9.1.1 File Transfer Protocol (FTP), Server

Mittels FTP können Sie unverschlüsselte Datenübertragungen vornehmen. Die meisten FTP-Server können Sie so einrichten, dass auch anonymen Zugriff möglich ist (Anonymous FTP). Damit ermöglichen Sie Download-Bereiche mit Kundeninformationen, Programmen und Multimedia-Inhalten.

Bei fast allen FTP-Servern wird eine Konfigurationsdatei *ftusers* angelegt. Der Name dieser Datei ist irreführend. In ihr werden all jene User eingetragen, die eben *nicht* auf den FTP-Server zugreifen dürfen. Hierzu zählen in jedem Fall unter Linux, FreeBSD und Unix *root* und unter Windows-Derivaten der *Administrator*.

FTP-Server

- ▶ **Ports:** 20/TCP für die Daten, 21/TCP zur Verbindungssteuerung. Durch die Verwendung unterschiedlicher Ports für die Daten und die Steuerung können Sie Steuerkommandos bei laufender Übertragung übermitteln.
- ▶ **FTP aktiver Modus:** Hier baut der Server eine Verbindung zum Client auf.
- ▶ **FTP passiver Modus:** Hier baut der Client zum Server zwei Verbindungen auf. Dies ist notwendig, wenn der Client hinter einer Firewall liegt. Firewalls blocken den Verbindungsaufbau von außen ab.
- ▶ **Programme:** WuFTP, ProFTP, Pure FTP u. v. a. m.
- ▶ **RFCs:** 959, 1123, 2181, 2228, 2474, 2535, 2640, 2773, 3659, 4033, 4034, 4035, 4343, 5321, 5452, 5797, 7151, 7504, 7766

Der SSH-Server bietet eine eigene FTP-Funktion an (SFTP). Sie kommen hier mit einem einzigen Port aus. Die Steuerung und die Übertragung sind verschlüsselt.

9.1.2 File Transfer Protocol (FTP), Clients

Als Client-Programm können Sie fast jeden Webbrowser verwenden (Abbildung 9.1). Sie sehen hier Opera im Einsatz.



Abbildung 9.1 Opera als FTP-Client

Für gehobeneren Ansprüche können Sie auf spezielle FTP-Clients zurückgreifen (FileZilla, gFTP). Auch viele Dateimanager besitzen die notwendigen Fertigkeiten. In Abbildung 9.2 sehen Sie gFTP während einer FTP-Sitzung.

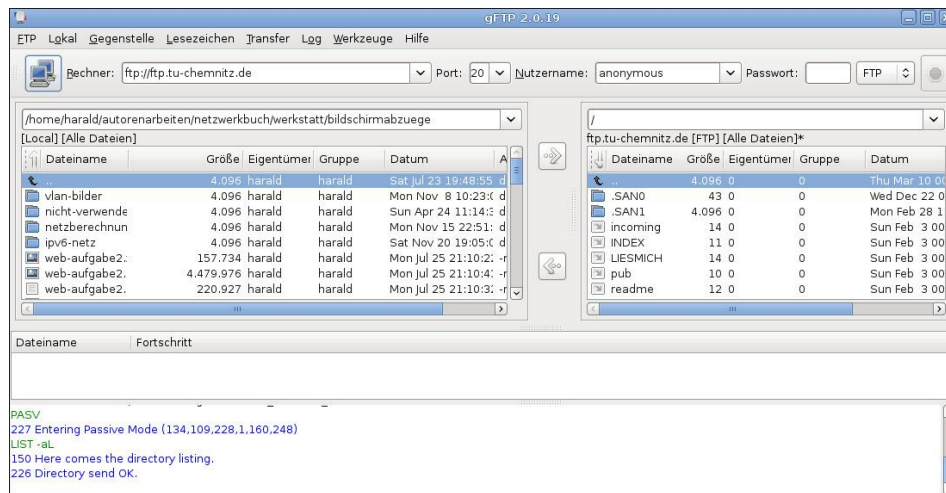


Abbildung 9.2 FTP-Sitzung mit gFTP

Natürlich finden Sie viele Clients für die MS-DOS-Befehlszeile (*PSFTP.exe* aus dem PuTTY-Paket) oder für die Shell. In Abbildung 9.3 wurde die Sitzung mit einem FTPClient für die Shell aufgebaut. Die Shell-Clients eignen sich für Bereiche ohne grafische Benutzeroberfläche, einige mobile Geräte und für den Einbau in Skripte. So können Sie für Ihre Rechner eine automatische Datensicherung über das Netz einrichten.

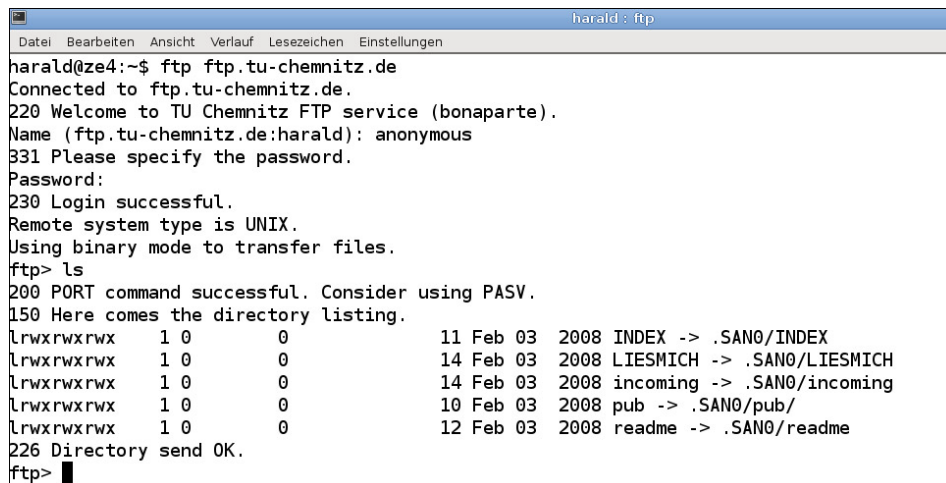


Abbildung 9.3 FTP-Client für die Shell

9.1.3 Benutzerkommandos für FTP- und SFTP-Sitzungen

Mittels der FTP-Kommandos (Tabelle 9.1) können Sie sich Verzeichnisinhalte anzeigen lassen, sich in Verzeichnisbäumen bewegen sowie Dateien hoch- und herunterladen. Gleichzeitig können Sie auch auf das lokale Dateisystem zugreifen, z. B. um das Arbeitsverzeichnis zu wechseln.

Nicht alle Kommandos stehen bei allen Servern (und Clients) zur Verfügung. Die Optionen des `ls`-Kommandos können Sie miteinander kombinieren (z. B. `ls -lt` für die erweiterte Anzeige und Sortierung nach Zeitstempel).

Aktion	Kommando
Herunterladen einer Datei	get <DATEI>
Nur FTP: Herunterladen mehrerer Dateien	mget <DATEIEN>
Hochladen einer Datei	put <DATEI>
Nur FTP: Hochladen mehrerer Dateien	mput <DATEIEN>
Anzeige des aktuellen Verzeichnisses auf dem Server	pwd
Anzeige des aktuellen lokalen Verzeichnisses	lpwd
Auflisten des Verzeichnisinhalts auf dem Server	ls [-<OPTION>]
Auflisten des lokalen Verzeichnisinhalts	lls [-<OPTION>]
Option zur Ausgabe von Benutzer, Größe, Zeitstempel, Attributen	-l
Option zur Ausgabe von »verborgenen Dateien«	-a
Option zur Ausgabesortierung nach Zeitstempel	-t
Anzeigen der Belegung des Plattenspeichers auf dem Server	df -h
Wechseln des Verzeichnisses auf dem Server	cd <VERZEICHNIS>
Wechsel des lokalen Verzeichnisses	lcd <VERZEICHNIS>

Tabelle 9.1 FTP-Kommandos

Aktion	Kommando
Anlegen eines neuen Verzeichnisses auf dem Server	mkdir <VERZEICHNIS-NEU>
Anlegen eines neuen lokalen Verzeichnisses	lmkdir <VERZEICHNIS-NEU>
Umbenennen eines Verzeichnisses oder einer Datei auf dem Server	rename <ALT> <NEU>
Löschen einer Datei auf dem Server	rm <DATEI>
Löschen eines Verzeichnisses auf dem Server	rmdir <VERZEICHNIS>
Verbindung beenden	bye exit quit
Kommandoübersicht anzeigen	help
Lokales Shell-Kommando ausführen	!<SHELLBEFEHL>
Versionsinfo anzeigen	version

Tabelle 9.1 FTP-Kommandos (Forts.)

Für den Verbindungsaufbau können, abhängig von den Erfordernissen, verschiedene Formen notwendig sein (Tabelle 9.2).

Aktion	Syntax
FTP: Standard-Ports werden benutzt.	<code>ftp ftp.<SERVER></code>
FTP: abweichender Steuerungs-Port	<code>ftp ftp.<SERVER> <PORT></code>
SFTP: Standard-Port wird benutzt.	<code>sftp <BENUTZER>@<SERVER></code>
SFTP: Abweichender Port wird benutzt.	<code>sftp -oPort=<PORT> <BENUTZER>@<SERVER></code>

Tabelle 9.2 Kommandos für den Verbindungsaufbau

Wie diese FTP-Kommandos praktisch angewendet werden, sehen Sie in Abbildung 9.4. Bei der Verbindungsaufnahme muss eine vom Standard abweichende Port-Nummer benutzt werden. Sie sehen das Herunterladen und Hochladen von Dateien, einen Verzeichniswechsel auf dem Server und auf dem lokalen Dateisystem sowie eine Abfrage über die Plattenbelegung.

```

harald@ze4:~/bilder/bearbeiten$ sftp -oPort=7167 harald@netzbuch
Password:
Connected to netzbuch.
sftp> ls
diavolezza.jpg      hoehle-val-d-uina.jpg      index.html      infotexte
malerisches-scuol.jpg      mbox      miralago.jpg      piz-cluenas-alm.jpg
sftp> get *.jpg
Fetching /usr/home/harald/diavolezza.jpg to diavolezza.jpg      100% 545KB 544.8KB/s 00:00
/usr/home/harald/diavolezza.jpg
Fetching /usr/home/harald/hoehle-val-d-uina.jpg to hoehle-val-d-uina.jpg      100% 442KB 441.6KB/s 00:00
/usr/home/harald/hoehle-val-d-uina.jpg
Fetching /usr/home/harald/malerisches-scuol.jpg to malerisches-scuol.jpg      100% 433KB 433.5KB/s 00:00
/usr/home/harald/malerisches-scuol.jpg
Fetching /usr/home/harald/miralago.jpg to miralago.jpg      100% 812KB 812.1KB/s 00:00
/usr/home/harald/miralago.jpg
Fetching /usr/home/harald/piz-cluenas-alm.jpg to piz-cluenas-alm.jpg      100% 529KB 528.5KB/s 00:00
/usr/home/harald/piz-cluenas-alm.jpg
sftp> lcd ../infotexte
info-hp9.txt
sftp> put info-hp9.txt
Uploading info-hp9.txt to /usr/home/harald/infotexte/info-hp9.txt      100% 49 0.1KB/s 00:00
info-hp9.txt
sftp> ls
info-hp9.txt  info1.txt
sftp> df -h
      Size      Used      Avail      (root)      %Capacity
 269GB      2.2GB      267GB      267GB           0%
sftp> quit
harald@ze4:~/bilder/bearbeiten$

```

Abbildung 9.4 SFTP-Sitzung

9.1.4 Datentransfer mit »netread« und »netwrite«

Besonders bei Installations- und Wartungsarbeiten fehlt oft ein funktionierender sftpoder ftp-Server. Wenn Sie in diesem Fall Daten übertragen müssen, greifen Sie, wenn räumlich möglich, zu USB-Stick oder SD-Karte. Besteht jedoch zwischen den beteiligten Rechnern eine Netzwerkverbindung (gleich, welcher Art), können Sie auch mit den Programmen `netread` und `netwrite` aus dem `netrw`-Paket die gewünschten Daten übertragen.

Dieses Verfahren benötigt keine Authentifizierung über das Netzwerk. Vielmehr sind auf jedem Rechner die Benutzer angemeldet, die einen Transfer starten bzw. empfangen. Sie benötigen als Sender also weder eine Benutzererkennung noch ein Passwort am Zielrechner.

Der Empfangs-Port wird zeitnah durch `netread` geöffnet. Dies erledigen Sie auf »Zuruf« und bevor auf der Senderseite `netwrite` gestartet wird. Durch den kurzfristigen Start von `netread` ist der Port nicht lange offen und ungenutzt, was mögliche Sicherheitsprobleme minimiert. Wenn Sie außerdem `netread` außerhalb der üblichen Programmpfade verstecken, ist auch eine missbräuchliche Nutzung unwahrscheinlich. Sie können die Programme auch auf externe Datenträger legen. Beachten Sie bitte folgende Punkte bei einer Nutzung außerhalb eines geschützten lokalen Netzwerks:

Verschlüsseln Sie die Nutzlast.

Nutzen Sie einen SSH-Tunnel.

Wenn IPv4 genutzt wird, muss in den Zugangsroutern ein entsprechendes Portforwarding (siehe Abschnitt 6.6, »Port and Address Translation (PAT), Network Address

Translation (NAT)« eingerichtet sein.
Zusätzliches Portknocking (siehe Abschnitt 10.6.8) erhöht die Sicherheit.

Sie übertragen Daten in der Form

```
netwrite <IP-ADRESSE|RECHNERNAME PORT> < DATEI
```

und empfangen diese mittels

```
netread <PORT> > ZIELDATEI
```

Übertragen einer Datei

Zuerst wird im »hellen« Terminal `netread` mit Angabe der Port-Nummer und Zieldatei gestartet. Anschließend beginnt `netwrite` vom anderen Rechner aus (»dunkles« Terminal) zu senden. Hier sind die Ziel-IP-Adresse bzw. ein auflösbarer Rechnername und die Port-Nummer einzugeben. Die Nutzlast wird mittels Umleitung der Standardeingabe übergeben (Abbildung 9.5).

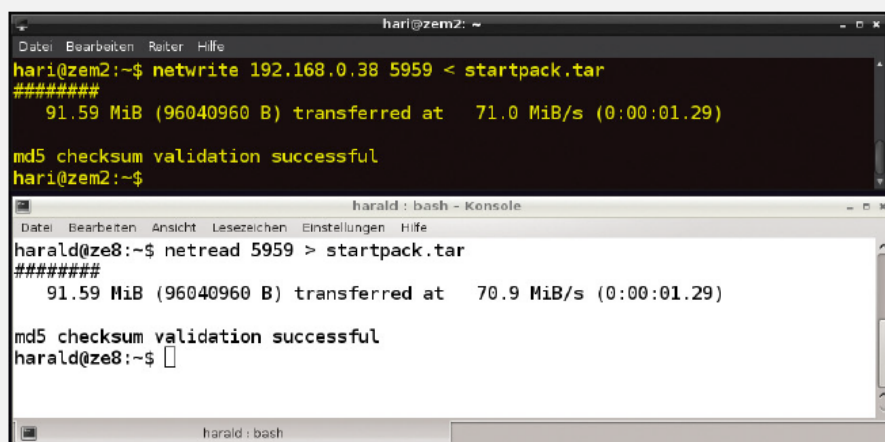


Abbildung 9.5 Datenübertragung mit »netwrite«/»netread«

Notfall-Chat

Ideal, wenn kein Mobiltelefon (oder Betriebsfunk) funktioniert oder verfügbar ist. Je Rechner müssen dabei zwei Terminals geöffnet werden. Je Rechner laufen `netwrite` und `netread` in einem eigenen Terminal. Auch hier gilt, dass Sie zuerst mit `netread` beginnen.

Die Standardeingaben (Tastatureingaben) werden direkt gesendet. Die Ein- und Ausgabeterminals der Rechner unterscheiden sich im Beispiel auch wieder durch die Hintergrundfarben (Abbildung 9.6).

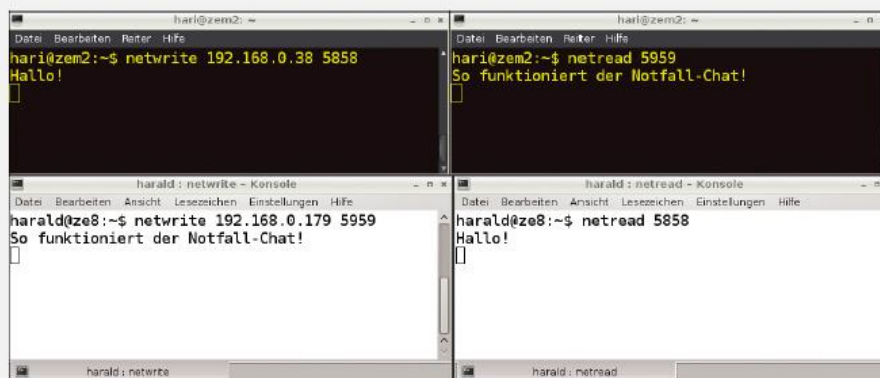


Abbildung 9.6 Notfall-Chat

Außerdem ist es mit diesen Programmen auch möglich, die Bildschirmausgaben von

Programmen auf andere Rechner umzuleiten. Dies wird beim nachfolgend beschriebenen Programm `cryptcat` dargestellt.

9.1.5 Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat«

Mit `cryptcat` können Sie *auch* Datentransfers vornehmen. Weitere Funktionen dieses Programms sind in Abschnitt 10.7.9, »cryptcat: im Dienste der Sicherheit«, beschrieben. Auf der »Senderseite« ist das Kommando wie folgt aufgebaut:

```
... LIEFERNDES_KOMMANDO | cryptcat -k "KENNWORT" -w 1 <ZIELRECHNER PORT>
```

Beim Empfänger kommt die Umlenkung der Standardausgabe zum Einsatz, falls die übermittelten Daten nicht am Bildschirm ausgegeben werden sollen:

```
cryptcat -k "KENNWORT" -l -p <PORT> > ZIELDATEI
```

Im Beispiel wird die Datei `startpack.tar` auf einen anderen Rechner übertragen. Der Empfänger (»dunkles« Terminal) startet `cryptcat` zuerst. Anschließend wird vom anderen, »hellen« Terminal und Rechner aus gesendet (Abbildung 9.7).

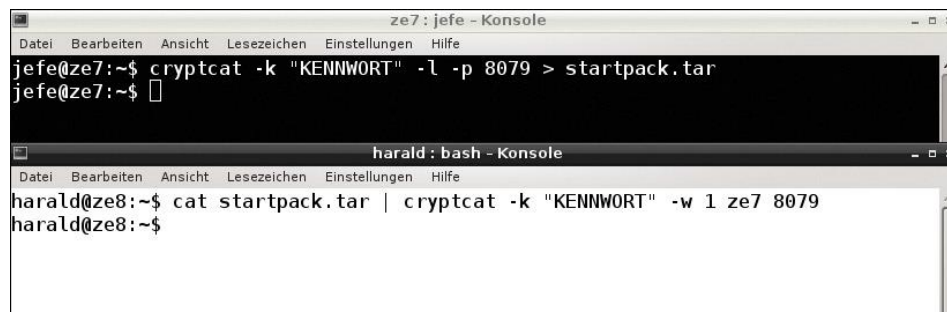


Abbildung 9.7 Dateitransfer mit »cryptcat«

Die gleiche Wirkungsweise gilt auch für andere Kommandos. Hier sehen Sie die Abfrage des Zustands eines Dienstes (Abbildung 9.8).

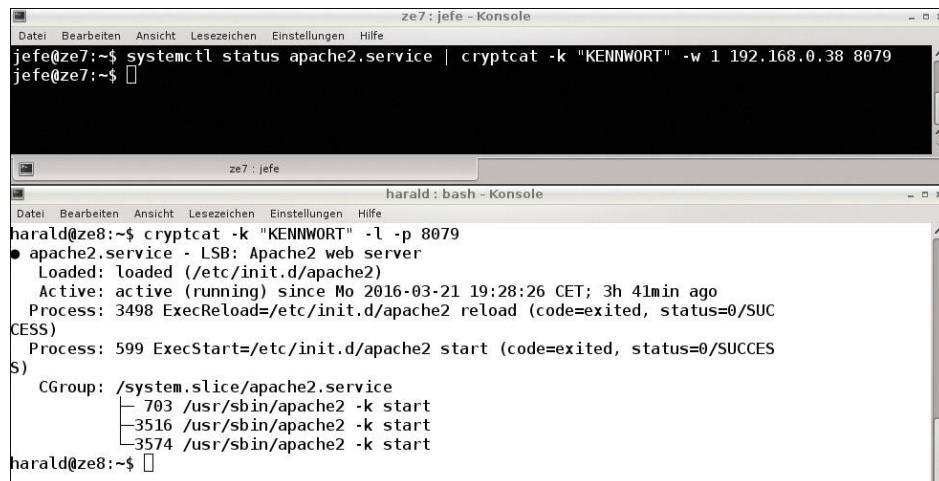


Abbildung 9.8 Übertragung einer Bildschirmausgabe

Beachten Sie bitte, dass das Standardkennwort `metallica` lautet und in Fachkreisen hinreichend bekannt sein dürfte.

9.1.6 Secure Copy (scp), Ersatz für Remote Copy (rcp)

Sie können direkt Dateien kopieren, ohne dafür eine Sitzung zu eröffnen. Programme für Windows finden Sie im PuTTY-Paket (*PSCP.exe*). Bei Linux oder FreeBSD haben Sie das

Programm *scp* auf dem System, wenn Sie wenigstens den SSH-Client installieren. Mit *scp* können Sie eine Datei vom Client zum Server und auch umgekehrt kopieren. Dabei können Sie für das Ziel (Server oder lokales Verzeichnis) einen anderen Namen vergeben. In Abbildung 9.9 sehen Sie folgende Vorgänge dargestellt:

- Kopieren einer Datei vom lokalen Verzeichnis zum Server, Standard-Port
- Kopieren einer Datei vom lokalen Verzeichnis zum Server mit abweichender Port-Nummer
- Kopieren einer Datei vom Server zum lokalen Verzeichnis, Angabe eines anderen Namens für die Dateikopie, Standard-Port
- Kopieren einer Datei vom Server zum lokalen Verzeichnis, Angabe eines anderen Namens für die Dateikopie und abweichende Port-Nummer

```

harald@ze4:~/bilder/infotexte$ scp info-hp9.txt harald@zentrale:info-hp9.txt
Password:
info-hp9.txt                                100% 49    0.1KB/s   00:00
harald@ze4:~/bilder/infotexte$
harald@ze4:~/bilder/infotexte$ scp -P7167 info-hp9.txt harald@netzbuch:info-hp9.txt
Password:
info-hp9.txt                                100% 49    0.1KB/s   00:00
harald@ze4:~/bilder/infotexte$
harald@ze4:~/bilder/infotexte$ scp harald@zentrale:info-hp9.txt infoallgemein.txt
Password:
info-hp9.txt                                100% 49    0.1KB/s   00:00
harald@ze4:~/bilder/infotexte$
harald@ze4:~/bilder/infotexte$ scp -P7167 info-hp9.txt harald@netzbuch:info-hp9.txt
Password:
info-hp9.txt                                100% 49    0.1KB/s   00:00
harald@ze4:~/bilder/infotexte$

```

Abbildung 9.9 »scp«

9.1.7 SSHFS: entfernte Verzeichnisse lokal nutzen

Unter Linux und FreeBSD können Sie Ihr Heimatverzeichnis, das sich auf einem anderen Rechner befindet, wie ein NFS-Laufwerk in den Verzeichnisbaum einhängen und damit wie ein lokales Laufwerk nutzen. Auch Windows-Anwender stehen nicht im Abseits: Unter <http://dokan-dev.net/en/download> wird eine Lösung angeboten. Windows-Anwender haben quasi ein »Netzlaufwerk« per *ssh*. Die für die Verbindung notwendigen Einträge sind in allen Anwendungen gleich. Sehen Sie hier die Einbindung eines Verzeichnisses unter der *GNOME*-Oberfläche:

1. Klicken Sie im Dateimanager auf Datei • Mit Server verbinden.
2. Tragen Sie in die sich nun öffnende Maske (Abbildung 9.10) alle notwendigen Daten ein. Der untere Eintrag Lesezeichenname hilft Ihnen, die Verbindung im Dateimanager leicht zu finden.

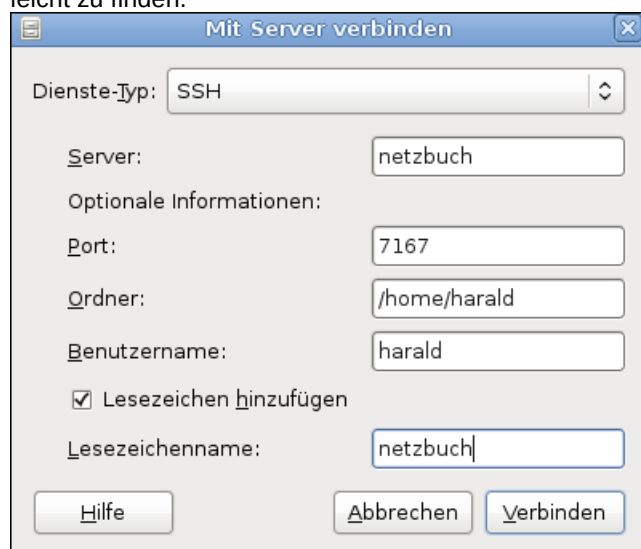


Abbildung 9.10 Anmeldedaten für den SSHFS-Zugriff

3. Waren Ihre Eintragungen richtig, werden Sie zur Eingabe Ihres Kennworts aufgefordert (es sei denn, Sie benutzen die Authentifizierung mit Schlüssel).

4. Der Dateimanager legt das Lesezeichen für das entfernte Verzeichnis an und öffnet die Ansicht darauf (Abbildung 9.11).

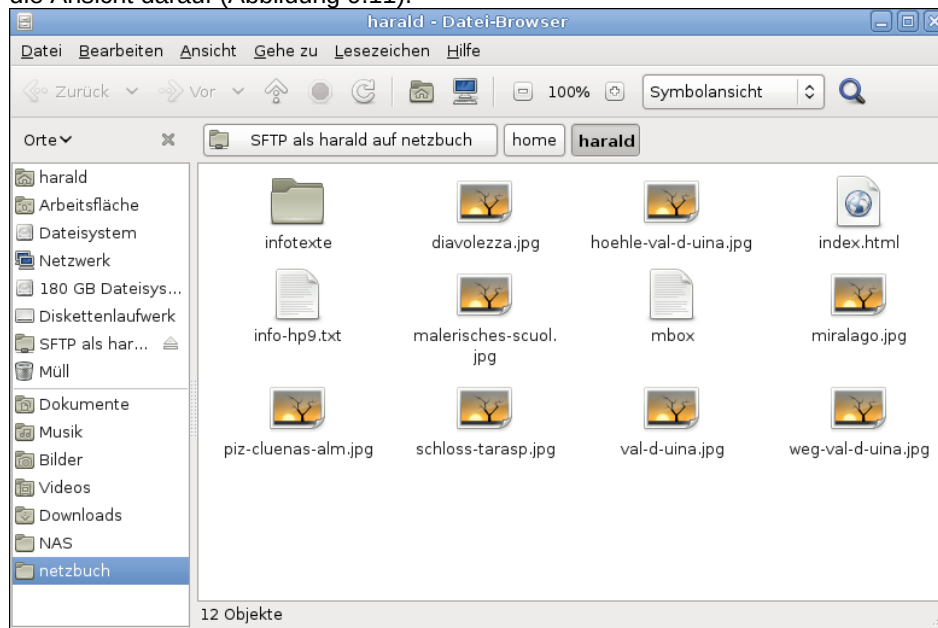


Abbildung 9.11 Ansicht des entfernten Verzeichnisses im Dateimanager

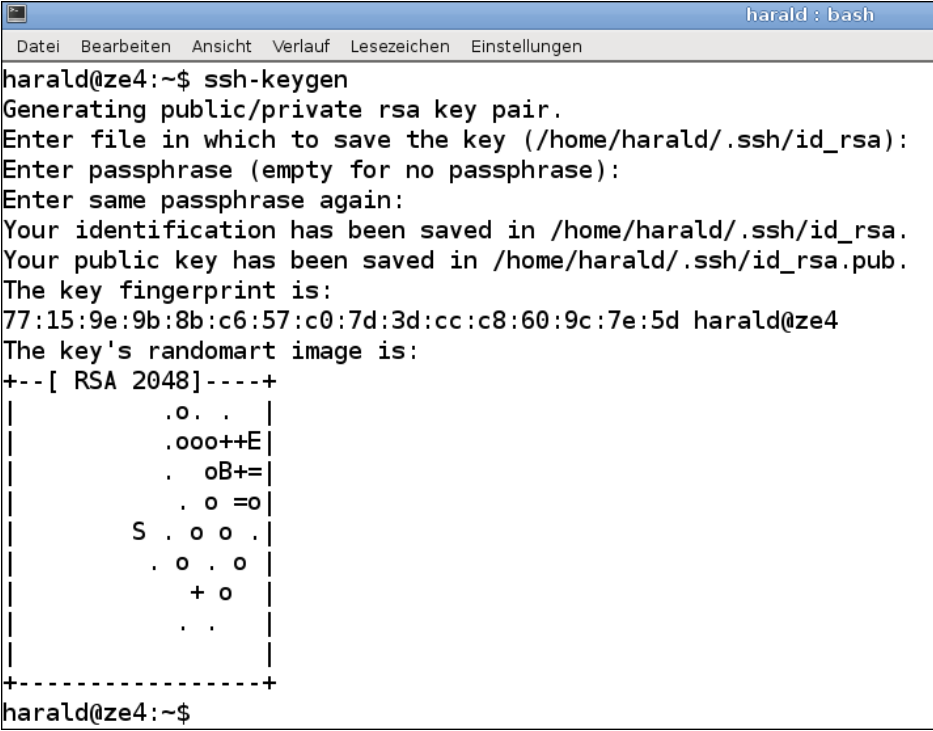
5. Falls Sie Zweifel haben, doch nicht per SFTP verbunden zu sein, prüfen Sie dies durch Klick oder Doppelklick auf eine Datei. Sofern sie sich öffnet, was bei SFTP nicht funktioniert, handelt es sich um eine lokale Datei.

9.2 SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung

Aus Sicherheitsgründen sollten Sie stets eine Anmeldung mit Kennwort benutzen, wenn Sie über das Netz auf einen anderen Rechner zugreifen. Wie aber sollen Skripte ohne Benutzereingriff an Ihrer Stelle eine Verbindung aufbauen? Sie hinterlegen Ihren öffentlichen Schlüssel auf dem Zielsystem. Ihren privaten Schlüssel müssen Sie unter allen Umständen geheim halten! Sie können für SSH aber auch einen Schlüssel zusätzlich mit einem Kennwort versehen. Damit erhöhen Sie die Sicherheit für Ihre Fernzugriffe. Sie sehen im Folgenden die Schritte auf einem Debian-Linux-System. Für den Einsatz unter Windows folgen Sie den Anweisungen in der Dokumentation Ihres SSH-Serverprodukts.

1. Führen Sie `ssh-keygen` aus (Abbildung 9.12).

Für die Anwendung des Schlüssels ohne zusätzliche Kennworteingabe lassen Sie den Eintrag, wie im Bild gezeigt, leer. Die beiden Schlüssel liegen in Ihrem Heimatverzeichnis unter `.ssh`. Der private Schlüssel ist in der Datei `id_rsa` untergebracht, Ihr öffentlicher Schlüssel unter `id_rsa.pub`.



```

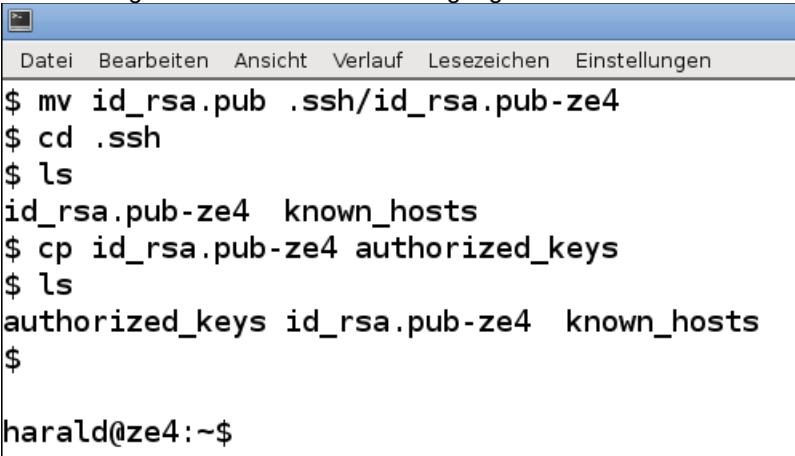
harald@ze4:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/harald/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/harald/.ssh/id_rsa.
Your public key has been saved in /home/harald/.ssh/id_rsa.pub.
The key fingerprint is:
77:15:9e:9b:8b:c6:57:c0:7d:3d:cc:c8:60:9c:7e:5d harald@ze4
The key's randomart image is:
+--[ RSA 2048 ]-----+
|      .o. .      |
|      .ooo++E|
|      . oB+=|
|      . o =o|
|      S . o o .|
|      . o . o|
|      + o|
|      . .|
+-----+
harald@ze4:~$

```

Abbildung 9.12 Ausführen von »ssh-keygen«

2. Übertragen Sie Ihren öffentlichen Schlüssel in Ihr Heimatverzeichnis auf dem Zielsystem.
3. Melden Sie sich am Zielsystem per SSH an.
4. Ändern Sie den Dateinamen von *id_rsa.pub* in *id_rsa.pub-<RECHNERNAME-Herkunft>* ab. Sollten Sie von mehreren Rechnern aus zugreifen, können Sie den Schlüssel zuordnen.
5. Verschieben Sie die Schlüsseldatei nach *.ssh*.
6. Prüfen Sie, ob hier bereits eine Datei *authorized_keys* existiert. Falls nein, kopieren Sie die Schlüsseldatei einfach. Geben Sie als Dateinamen für die Kopie *authorized_keys* an. Falls ja, fügen Sie den Inhalt Ihrer Schlüsseldatei mit dem *cat*-Befehl an:
`cat id_rda.pub-<RECHNERNAME> >> authorized.keys`

In Abbildung 9.13 sehen Sie diesen Vorgang auf einem FreeBSD-Server.



```

$ mv id_rsa.pub .ssh/id_rsa.pub-ze4
$ cd .ssh
$ ls
id_rsa.pub-ze4  known_hosts
$ cp id_rsa.pub-ze4 authorized_keys
$ ls
authorized_keys id_rsa.pub-ze4  known_hosts
$
harald@ze4:~$

```

Abbildung 9.13 Einbinden des Schlüssels auf dem Zielsystem

7. Testen Sie die Verbindung, z. B. mit SSH (Abbildung 9.14).

```

Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
harald@ze4:~$ ssh -p7167 harald@netzbuch
Last login: Thu Jul 28 13:24:50 2011 from 192.168.0.34
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
    The Regents of the University of California. All rights reserved.

Willkommen auf

# # ##### ##### ##### ##### # # ##### # #
## # # # # # # # # # # #
# # # ##### # # ##### # # # #####
# # # # # # # # # # # #
# ## # # # # # # # # # #
# # ##### # ##### ##### ##### # #

192.168.0.67
-----
Hinweise von der Systemverwaltung: Geänderte Datensicherungs-
zeiten! Werktags jetzt ab 21:00 Komplettsicherung!
$

```

Abbildung 9.14 Testen der SSH-Verbindung mit Authentifizierung über Schlüssel

9.3 Aufbau eines SSH-Tunnels

Mit einem SSH-Tunnel erhöhen Sie die Sicherheit bei Verbindungen über unsichere Netze (Internet). Anwendungen, die ihre Daten nicht für eine Übertragung verschlüsseln, können nicht mehr so leicht durch Unbefugte abgehört werden. Ein SSH-Tunnel behebt aber nicht grundsätzliche Sicherheitsprobleme dieser Programme. Möchten Sie von einem Windows-Rechner aus zugreifen, benutzen Sie PuTTY. Damit können Sie ebenso einen Tunnel einrichten. Im umgekehrten Fall müssen Sie einen SSH-Server für Windows einrichten und gegebenenfalls auch einen Benutzer für den SSH-Zugriff anlegen. Dann können Sie ebenso einen Tunnel benutzen und z. B. eine verschlüsselte

Fernsitzung mittels VNC oder RDP nutzen.

Unter Linux oder FreeBSD bauen Sie per Hand einen SSH-Tunnel in der Form

```
ssh -L<PORT-LOCAL>:<RECHNER>:<PORT> <RECHNER>
```

auf. Mit der Option `-L` leiten Sie den entfernten Port auf Ihren `localhost` um, und mit `-R` geschieht dies umgekehrt.

Beispiel:

Die Eingabe

```
ssh -L8080:netzbuch:80 netzbuch -p7167
```

bewirkt, dass Sie am lokalen Rechner `ze4` die über `zentrale` auf `localhost` getunnelte Webseite von `netzbuch` betrachten können (Abbildung 9.15). Achten Sie auf die Darstellung der URL im Browser.



Abbildung 9.15 Per SSH-Tunnel übertragene Webseite

9.4 Fernsitzungen

Heim-, Tele- und Satellitenarbeitsplätze, Wartungs- und Kundendienstzugriffe sowie zentrale Serverkonzepte erfordern die Möglichkeit, interaktiv Programme auf dem entfernten Rechner auszuführen. Sie dürfen dabei nicht durch mangelnde Geschwindigkeit oder auch Sicherheitsprobleme beeinträchtigt werden.

9.4.1 Telnet

Nur den `telnet`-Client kann ich noch als Testwerkzeug empfehlen (wie in Abschnitt 7.4.2, »Konfigurationshinweise«, gezeigt). Setzen Sie keinen `telnet`-Server auf! Jeder Tastenanschlag und jeder Buchstabe der Bildausgabe kann mitgelesen werden. Telnet ist unverschlüsselt und damit ein Sicherheitsrisiko.

9.4.2 Secure Shell (SSH), nur Textdarstellung

Wenn Ihnen ein Terminal zur Ausführung von Shell-Kommandos oder DOS-Befehlen ausreicht, arbeiten Sie mit SSH. Ihre Eingaben und die Bildausgabe sind verschlüsselt. Sie können sich mit einem Anmeldekennwort oder durch Schlüssel (siehe Abschnitt 9.2, »SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung«) authentifizieren. Terminalsitzungen mit SSH kommen auch mit langsamen Leitungen (Modem, ISDN, GPRS) zurecht.

Der Verbindungsaufbau (siehe auch Abbildung 9.16) erfolgt mit

```
ssh <BENUTZER>@<RECHNERNAME>
```

oder mit

```
ssh <BENUTZER>@<IP-ADRESSE>
```

Vom Standard abweichende Port-Nummern übergeben Sie mit einer Option:

```
ssh -p<PORT> <BENUTZER>@<RECHNERNAME>
```

oder so:

```
ssh -p<PORT> <BENUTZER>@<IP-ADRESSE>
```

Eine `ssh`-Sitzung beenden Sie durch Eingabe von `exit`.

```

zentrale : harald
Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
harald@ze4:~$ ssh harald@zentrale
Password:
Last login: Fri Jul 29 09:21:27 2011 from ze4.zislers.de
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
The Regents of the University of California. All rights reserved.

Willkommen auf

#####  #####  #  #  #####  #####  ##  #  #####
#  #  ##  #  #  #  #  #  #  #  #  #
#  #####  #  #  #  #  #  #  #  #  #  #####
#  #  #  #  #  #  #  #####  #####  #  #
#  #  #  ##  #  #  #  #  #  #  #  #
#####  #####  #  #  #  #  #  #  #  #  #####  #####

192.168.0.25
-----
If you `set filec' (file completion) in tcsh and write a part of the
filename, pressing TAB will show you the available choices when there
is more than one, or complete the filename if there's only one match.
$ █

```

Abbildung 9.16 Fernsitzung mit SSH

9.4.3 Display-Umleitung für X11-Sitzungen

Sie können einzelne Anwendungen oder einen ganzen Desktop unter Linux oder FreeBSD auf einen anderen PC umleiten. Die Übertragung geschieht in beide Richtungen unverschlüsselt, was ein hohes Sicherheitsrisiko darstellt. Ich rate deshalb von der Verwendung ab. Die Funktionsweise allerdings sollten Sie trotzdem kennen. Sie ist für viele andere Konzepte in diesem Bereich eine wichtige Grundlage:

Der X-Server läuft auf dem PC, vor dem Sie sitzen, Ihre Eingaben mit Tastatur und Maus vornehmen und die Bildausgabe verfolgen (Abbildung 9.17). Der X-Client ist der Rechner, auf dem Sie Ihre Programme ausführen. Auch wenn es sich dabei um einen gut ausgestatteten Server-Rechner handelt, spielt er in diesem Fall die Rolle des Clients.

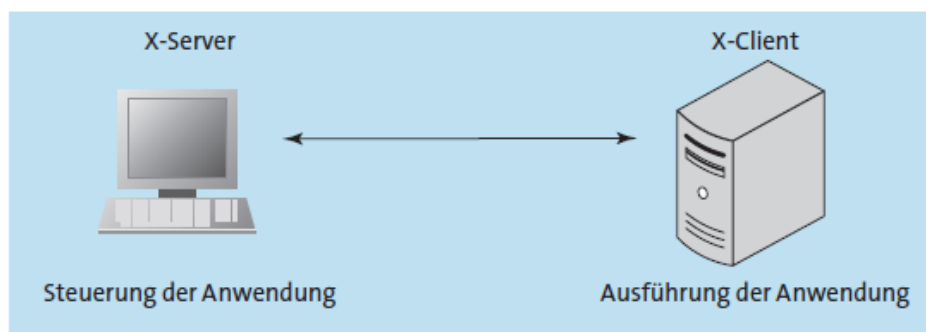


Abbildung 9.17 X11-Client-Server-Modell

9.4.4 SSH zur Display-Umleitung für X11

Die Display-Umleitung der SSH können Sie für grafische Fernsitzungen auf Linux- und FreeBSD-Rechnern nutzen. Dabei müssen Sie nur einen erweiterten Aufruf tätigen. Auf Ihrem PC muss ein X-Server laufen. Für Microsoft Windows können Sie dieses Verfahren nicht einsetzen. Die Aufrufsyntax lautet:

```
ssh -X <BENUTZER>@<RECHNERNAME>
```

Vom Standard abweichende Port-Nummern übergeben Sie mit einer Option:

```
ssh -X -p<PORT> <BENUTZER>@<RECHNERNAME>
```

Anschließend starten Sie manuell das GUI-Programm (Abbildung 9.18). Schließen Sie die Eingabe mit dem Zeichen »&« ab. Damit bleibt das Terminal frei für weitere Eingaben. Eine

korrekte Abmeldung ist erst möglich, wenn Sie alle GUI-Anwendungen beendet haben.

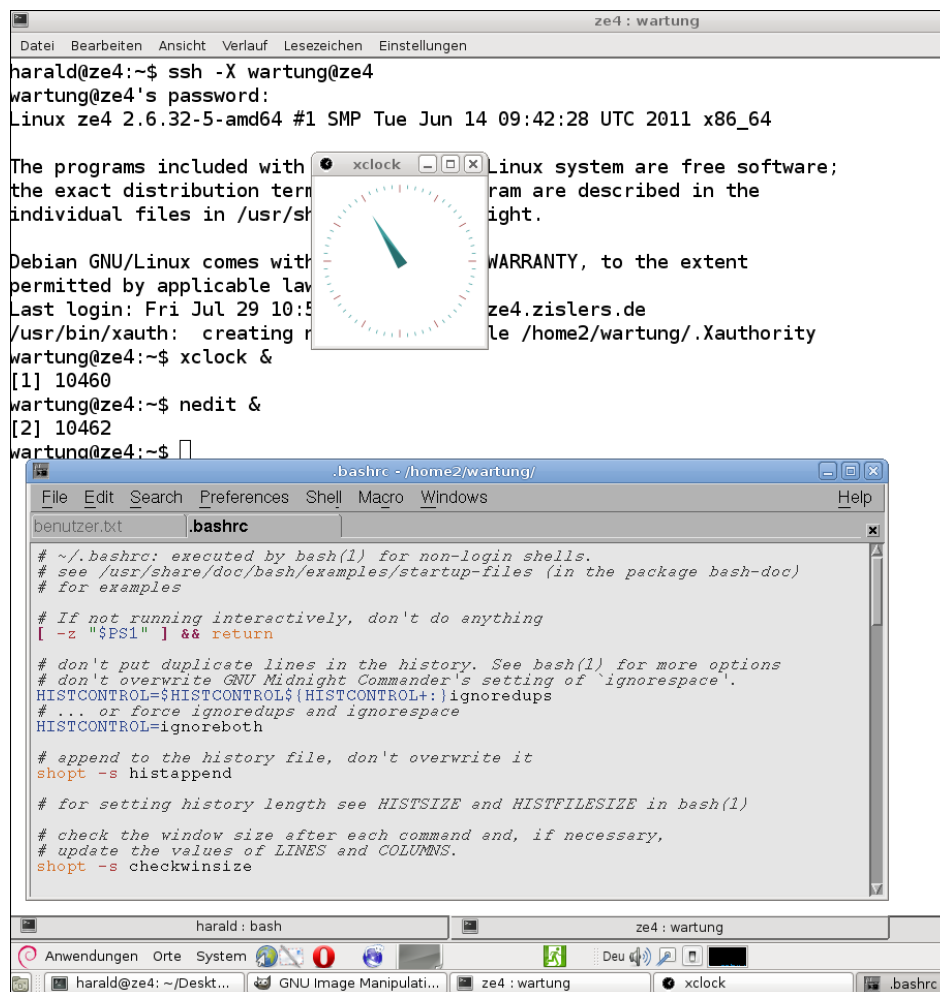


Abbildung 9.18 SSH-Sitzung mit Display-Umleitung

Alternativ können Sie, wenn Sie nur ein Programm ausführen möchten, dieses gleich mit der Anmeldung starten. Dies geschieht wie folgt:

```
ssh -X <BENUTZER>@<RECHNERNAME> <PROGRAMMNAME>
```

Beim Beenden des Programms werden Sie zugleich abgemeldet. Diese Handlungsweise eignet sich auch, wenn Sie unter verschiedenen Benutzerkennungen gleichzeitig auf einem Linux- oder FreeBSD-Rechner arbeiten möchten.

9.4.5 Virtual Network Computing (VNC)

VNC ist ein sehr verbreitetes Werkzeug. Es hat einen großen Leistungsumfang, aber auch Risiken beim Einsatz.

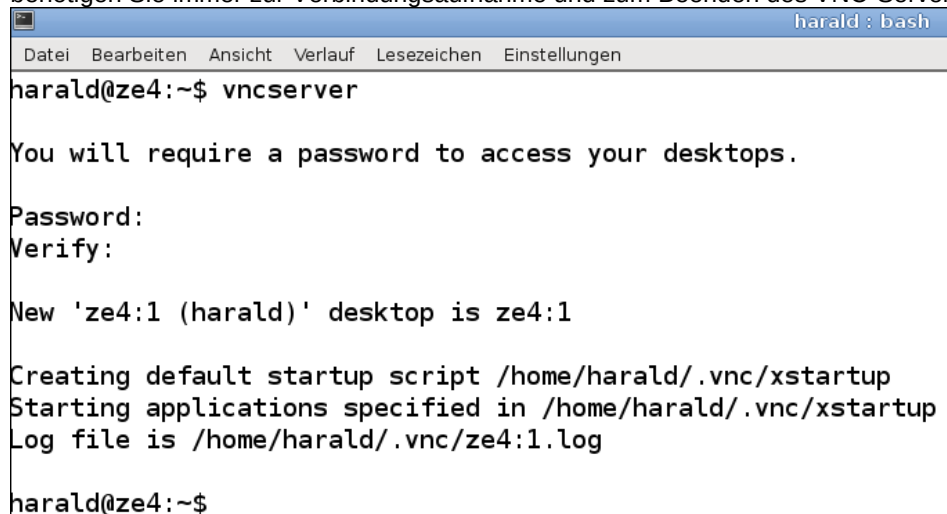
VNC in Kürze

- ▶ **Viele Implementierungen:** für Linux, FreeBSD, OS X und Microsoft Windows, z. B. RealVNC oder tightvnc
- ▶ **Ports:** 5800/TCP, 5900/TCP (Windows), 58XX/TCP, 59XX/TCP Linux/FreeBSD; XX steht für die Display-Nummer.
- ▶ **Verschlüsselung:** Das VNC-Protokoll sieht keine Verschlüsselung vor. Leiten Sie die Verbindung deshalb durch einen SSH-Tunnel. Manche Implementierungen verfügen allerdings über eine Verschlüsselungsfunktion.
- ▶ **Microsoft Windows:** Fernsteuerung eines Desktops
- ▶ **Linux/FreeBSD:** Durchführung einer Fernsitzung, gleichzeitig für mehrere Benutzer
- ▶ **Programme:** Server und Clients (Viewer)

Der Programmstart unter Windows erfolgt per Mausklick. Damit können Sie Ihren Desktop fernsteuern lassen, z. B. durch einen Administrator. Zum Aufbau eines sicheren SSH-Tunnels muss auf dem PC ein SSH-Server installiert werden. Auf dem fernsteuernden Rechner benötigen Sie PuTTY. Bauen Sie damit einen SSH-Tunnel auf, und leiten Sie die beiden VNC-Ports durch diesen.

Installieren Sie unter Linux oder FreeBSD das Paket `ssvnc`. Dieser VNC-Viewer baut selbstständig einen SSH-Tunnel auf. Unter Linux oder FreeBSD müssen Sie zunächst einige Konfigurationsdateien bearbeiten:

1. Melden Sie sich per SSH am entfernten Rechner an.
2. Führen Sie `vncserver` aus, und vergeben Sie ein Kennwort für die Fernsitzung (Abbildung 9.19). Bei diesem ersten Start wird das Konfigurationsverzeichnis angelegt. Beim Serverstart wird auch jedes Mal eine Desktop-Nummer ausgegeben. Diese benötigen Sie immer zur Verbindungsaufnahme und zum Beenden des VNC-Servers.



```

harald@ze4:~$ vncserver

You will require a password to access your desktops.

Password:
Verify:

New 'ze4:1 (harald)' desktop is ze4:1

Creating default startup script /home/harald/.vnc/xstartup
Starting applications specified in /home/harald/.vnc/xstartup
Log file is /home/harald/.vnc/ze4:1.log

harald@ze4:~$

```

3. Wenn Sie einen Windowmanager als Oberfläche möchten, wechseln Sie in das Verzeichnis `.vnc`, und öffnen Sie mit einem Editor die Datei `xstartup`. Hier setzen Sie das Kommentarzeichen vor den Eintrag `#x-window-manager &` und fügen eine neue Zeile mit dem gewünschten Windowmanager, hier `icewm`, ein: `icewm &`
4. Beenden Sie jetzt den noch laufenden VNC-Server durch die Eingabe von `vncserver -kill :<Desktop-Nummer>`. Diese Nummer sehen Sie beim Start des Servers.

Die Konfiguration ist damit abgeschlossen.

Starten Sie jetzt eine VNC-Sitzung, um die Einstellungen zu testen:

1. Melden Sie sich mittels `ssh` am entfernten Rechner an.
2. Starten Sie den `vncserver`. Beachten Sie die Desktop-Nummer, die er ausgibt. Sie benötigen diese für den Verbindungsaufbau und das Beenden des Servers.
3. Starten Sie auf dem Client-Rechner das Viewer-Programm (Abbildung 9.20).

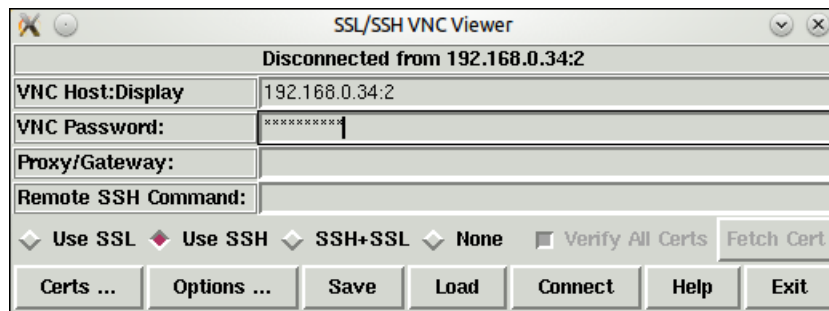


Abbildung 9.20 »ssvnc«

4. Nach dem Verbinden sehen Sie einen Desktop (Abbildung 9.21). Sollten Sie keine Taskleiste o. Ä. sehen, scrollen Sie im VNC-Fenster nach unten.

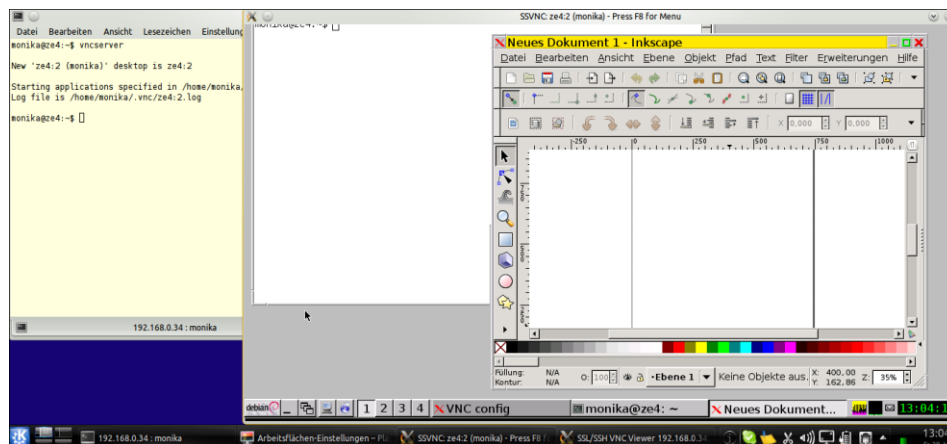


Abbildung 9.21 VNC-Desktop

5. Sie können die VNC-Sitzung jederzeit durch Beenden des Client-Programms unterbrechen. Zu einem späteren Zeitpunkt können Sie sich mit der gleichen Display-Nummer wieder anmelden. In der VNC-Sitzung gestartete Programme arbeiten auch weiter, wenn Sie abgemeldet sind.

6. Möchten Sie die VNC-Sitzung (Abbildung 9.22) beenden, geben Sie am `ssh`-Terminal das Kommando

```
vncserver -kill :<Desktop-Nummer>
```

ein.



Abbildung 9.22 Beenden von »vncserver«

9.4.6 X2Go (Server und Client)

Eine recht einfach zu handhabende Lösung für das Arbeiten mit grafischen Benutzeroberflächen auf räumlich entfernt liegenden Linux-Rechnern erhalten Sie bei Verwendung des X2Go-Servers und -Clients. Das Terminalserver-Projekt finden Sie im Internet unter www.x2go.org. Das Serverpaket läuft ausschließlich auf Linux-Rechnern (und bei Installation aus den Quelltexten auch unter FreeBSD). Die Client-Pakete gibt es für Linux, FreeBSD, Microsoft Windows und OS X.

Sie können bereits mit ISDN-Geschwindigkeit halbwegs vernünftig arbeiten. Mit einer guten DSL-Anbindung zwischen Heimarbeitsplatz und Server läuft es dagegen schon flüssig: Die Reaktions- und Latenzzeiten bemerken Sie nur noch am Rande. Auch UMTS-,

Kabel- und LTE-Verbindungen reichen natürlich aus.

Im lokalen Netzwerk ohne »Drossel« steht Ihnen die volle Übertragungsgeschwindigkeit zur Verfügung. Bremsend wirken sich natürlich zu viele gleichzeitig arbeitende Benutzer aus. Deren Zahl hängt von der Art der Anwendungen (Büro: viele Benutzer, CAD & Co: weniger Benutzer) und der Leistungsfähigkeit der Hardware ab. Mit vier Kernen und 16 GB, besser 32 GB Arbeitsspeicher können schon mal 20 Benutzer arbeiten, ohne dass Sie Einschränkungen wahrnehmen. Hier spüren Sie dann die Ressourcenteilung auch im Budget: Viele Benutzer teilen sich ein besser ausgebautes System, am Arbeitsplatz steht möglicherweise ein Banana Pi mit seinem kleinen Steckernetzteil anstelle eines vollwertigen PCs. Sie sparen Anschaffungs- und Betriebskosten und auch Arbeitszeit bei der Administration ein.

Die Programme des X2Go-Projekts fassen die Funktionalitäten der SSH-Display-Umleitung, Kompression und XDMCP mehr oder weniger zusammen. Deshalb wird z. B. `openssh` als Installationsvoraussetzung genannt.

Die Installation verläuft je nach verwendeter Linux-Distribution etwas unterschiedlich. Unter Debian und Verwandten ergänzen Sie vor der eigentlichen Installation zunächst die Datei `/etc/apt/sources.list`. Dazu nehmen Sie die Identität von `root` an.

Führen Sie zunächst das Kommando

```
apt-key adv --recv-keys --keyserver keys.gnupg.net E1F958385BFE2B6E
```

aus. Damit stehen die notwendigen Schlüssel für die Arbeit mit dem Repo-Archiv zur Verfügung.

Anschließend ergänzen Sie die Datei `/etc/apt/sources.list` um diese Einträge:

```
# X2Go Repository (release builds)
deb http://packages.x2go.org/debian wheezy main
# X2Go Repository (sources of release builds)
deb-src http://packages.x2go.org/debian wheezy main
# X2Go Repository (nightly builds)
#deb http://packages.x2go.org/debian wheezy heuler
# X2Go Repository (sources of nightly builds)
#deb-src http://packages.x2go.org/debian wheezy heuler
```

Sie können zwischen den `release builds` und den meist tagesaktuellen `nightly builds` wählen. Mit dem Einsatz der ersten Auswahl setzen Sie mehr auf Beständigkeit und Betriebssicherheit, während die zweite Wahl sich für Experimente mit den neuesten Entwicklerversionen eignet. Falls später Sicherheitsaktualisierungen anstehen, werden diese automatisch berücksichtigt.

Nun müssen Sie dem Debian-Paketsystem die Änderung mittels `apt-get update` bekannt geben. Fügen Sie den Schlüsselbund hinzu: `apt-get install x2go-keyring && apt-get update`, und prüfen Sie anschließend, welche Pakete zur Verfügung stehen (Abbildung 9.23). Um diese Anzeige zu erhalten, geben Sie `apt-cache search x2go` ein.

```

/home/harald : bash
root@ZE6:~# apt-cache search x2go
cups-x2go - Virtual X2Go printer for CUPS
pinentry-x2go - Qt4-based PIN or passphrase entry dialog for x2goclient
plasma-widget-x2go - Plasma widget for control X2Go sessions
pyhoca-cli - Command line X2Go client written in Python
pyhoca-gui - Graphical X2Go client written in (wx)Python
python-x2go - Python module providing X2Go client API
python-x2go-doc - Python module providing X2Go client API (documentation)
python-x2gobroker - X2Go http(s) based session broker (Python modules)
x2go-keyring - GnuPG keys of all X2Go developers and the X2Go archive
x2goagent - X2Go agent
x2gobroker - X2Go http(s) based session broker (executable)
x2gobroker-agent - X2Go http(s) based session broker (common files)
x2gobroker-authservice - X2Go http(s) based session broker (PAM authentication service)
x2gobroker-daemon - X2Go http(s) based session broker (daemon)
x2gobroker-wsgi - X2Go http(s) based session broker (CGI)
x2gocdmanager - clientside daemon enabling automatic CD-Rom mounting
x2goclient - X2Go Client application (Qt4)
x2goclient-dbg - X2Go Client application (Qt4), debug symbols (client)
x2godesktopsharing - Share X11 desktops with other users via X2Go
x2golxdebindings - LXDE bindings for X2Go
x2gomatebindings - Description: x2gomatebindings (MATE mimetypes for X2Go)
x2goplugin - X2Go Client (Qt4) as browser plugin
x2goplugin-dbg - X2Go Client application (Qt4), debug symbols (plugin)
x2goplugin-provider - Provide X2Go Plugin via Apache webserver
x2goserver - X2Go server daemon scripts
x2goserver-compat - X2Go server daemon scripts (backwards compatibility to old client versions)
x2goserver-extensions - X2Go server daemon scripts (extensions)
x2goserver-fmbindings - Generic (freedesktop-based) file manager bindings for X2Go
x2goserver-printing - X2Go server daemon scripts (printing)
x2goserver-pyhoca - X2Go server daemon scripts (add-ons for pyhoca client)
x2goserver-xsession - X2Go server daemon scripts (Xsession runner)
x2gosmartcardrules - UDEV rules for smartcard readers
x2gothinclient - login daemon starting x2goclient in displaymanager mode
x2gothinclient-chroot - Install X2Go Thin Client chroot (meta-package)
x2gothinclientmanagement - Management tools for X2Go Thin Client chroot server
x2gousbmount - clientside usb mass-storage device mounting
root@ZE6:~#

```

Abbildung 9.23 Zugriff auf X2Go-Pakete mittels »apt«

Mittels `apt-get install x2goserver` spielen Sie das Programm ein.

Überprüfen Sie unmittelbar danach die Funktion des Servers durch den Prozessstatus:

```
ps ax | grep x2go
```

Ein laufender Server, auf den aber noch niemand zugreift, ergibt die Ausgabe aus Abbildung 9.24.

```

/home/harald : bash
root@ZE6:~# ps ax | grep x2go
590 pts/5    S+        0:00 grep x2go
31596 pts/4   S         0:00 /usr/bin/perl /usr/sbin/x2gocleansessions
root@ZE6:~#

```

Abbildung 9.24 Prozessstatus des X2Go-Servers

Sie können das Client-Programm unter Linux, FreeBSD, OS X und Microsoft Windows betreiben. Wollen Sie einen »richtigen« Client aufbauen, der kostengünstig in Anschaffung und Betrieb ist, können Sie einen Raspberry Pi oder besser einen Banana Pi verwenden. Neben dem Kleinrechner mit Steckernetzteil, Gehäuse, SD-Karte, Maus und Tastatur müssen Sie in Ihrer Kalkulation noch einen eventuell notwendigen HDMI/VGA-Adapter für den Bildschirmanschluss vorsehen. Befestigen Sie den Kleinrechner am besten am Monitor. Der Kabelsalat hält sich in Grenzen, und der so geschaffene Arbeitsplatz zieht in einem Rutsch um. In Abbildung 9.25 sehen Sie eine solche Gerätekombination.



Abbildung 9.25 Monitor mit Raspberry Pi als Thin Client

Das X2Go-Projekt bietet auch die Möglichkeit, einen klassischen Thin Client einzurichten, der mittels BOOTP sein Betriebssystem lädt. Wegen den dabei auftretenden Unsicherheiten, vor allem bei Verbindungen außerhalb geschützter Netze, zeige ich stattdessen die Einrichtung auf der SD-Karte. Die Besitzer eines Raspberry Pi holen sich die Abbilddatei für die Speicherkarte unter www.raspberrypi.org/downloads (wählen Sie das Debian-basierte **raspbian** aus!), während die Besitzer eines Banana Pi unter www.bananian.org/download fündig werden.

Tabelle 9.3 zeigt Ihnen den vollständigen Weg vom »Impfen« der Karte bis zum ersten Login am Server.

Vorgang	Kommando, Hinweis
Beschreiben der SD-Karte mit der Abbilddatei, gegebenenfalls vorher Entkomprimieren der Download-Datei	1. Linux: <code>dd if=bananian-1508.img of=/dev/GERÄTEDATEI bs=1M && sync</code> Führen Sie <code>lsblk</code> aus, und lesen Sie die letzten Zeilen der Ausgabe. Dort sollte ein GeräteName auftauchen, der mit <code>sd</code> beginnt. Im Beispiel von Abbildung 9.26 und Abbildung 9.27 lautet dieser Name <code>sde</code>. Dies tragen Sie in obigem Befehl anstelle von <code>GERÄTEDATEI</code> ein. Sollte Ihre Download-Datei komprimiert sein, müssen Sie diese vor dem Schreiben noch dekomprimieren. 2. Windows: eventuell Download-Datei entkomprimieren und mit <i>win32diskimager</i> auf die SD-Karte schreiben (Abbildung 9.27)
Banana Pi erstmalig starten	SD-Karte in den Banana Pi einschieben, den Kleinrechner anschließen (richtigen USB-Anschluss für die Stromversorgung benutzen!), Stromversorgung einschalten/einstecken
Anmelden als <code>root</code>	Passwort: PI
HINWEIS!	ACHTUNG! US-Tastatur-Belegung: <code>[Y]=[Z]</code>, <code>[Z]=[Y]</code>! Navigation: Pfeiltasten, Bestätigen mit <code>[↵]</code> bzw. Leertaste für Markieren betätigen
Aufruf des Skripts für die Erstkonfiguration	<code>bananian-config</code>
Tastatureinstellung	<code>us → other → german → keyboard: german (dead acute)</code>

Tabelle 9.3 Installation eines Banana Pi als Thin Client ohne BOOTP/TFTP

Vorgang	Kommando, Hinweis
root-Passwort ändern	☐ Y → neues Kennwort vergeben
Zeitzone einstellen	☐ Y → Europe → Berlin
Spracheinstellungen bestimmen	de_DE.UTF-8
Standard-Systemsprache	default locale: de_DE.UTF-8
Rechnername	hostname: tc02 (für das Beispiel)
Hardware angeben	current hardware configuration – Modell auswählen
Die Größe des Root-Dateisystems an die SD-Karte anpassen	expand root fs? Y
Banana Pi neu laden	reboot
Benutzer tc anlegen	adduser tc
Benutzer tcadmin anlegen	adduser tcadmin
Software updaten	apt-get update && apt-get upgrade
Software-Installation: grafische Benutzeroberfläche, xorg	apt-get install xorg
Fenstermanager installieren	apt-get install lxde
Grafische Benutzeroberfläche testweise starten	startx – zum Beenden auf das Start-Symbol des LXDE links unten klicken und dort ABMELDEN wählen
Weitere Software installieren: sudo für die Möglichkeit, dass ein anderer Benutzer root vorbehaltene Kommandos ausführt	apt-get install sudo
Einstellungen für sudo vornehmen	visudo, Einträge unter # Allow members ... tcadmin ALL=(ALL:ALL) ALL tc ALL=(ALL) NOPASSWD: /sbin/init 0 visudo beenden: ☐ Esc, ☐ Esc :wq!

Tabelle 9.3 Installation eines Banana Pi als Thin Client ohne BOOTP/TFTP (Forts.)

Vorgang	Kommando, Hinweis
Anmelden als <code>tcadmin</code> und testen, ob Systemzugriff möglich ist	Drücken Sie die Tasten <code>[Alt]+[F2]</code> , um auf eine neue Konsole zu gelangen. Hier können Sie sich dann anmelden.
Testweise Updaten des Systems als Benutzer <code>tcadmin</code>	<code>sudo apt-get update</code> <code>sudo apt-get upgrade</code>
Hat das Updaten funktioniert, zurückwechseln zur anderen Konsole und das Benutzerkonto von <code>root</code> sperren	Drücken Sie die Tasten <code>[Alt]+[F1]</code> , um zur Sitzung von <code>root</code> zurückzugelangen. Hier geben Sie ein: <code>passwd -l root</code> und <code>exit</code> (<code>root</code> abmelden)
Zur anderen Konsole (<code>tcadmin</code>) zurückwechseln und weitere Einstellungen vornehmen	Drücken Sie die Tasten <code>[Alt]+[F2]</code> , um zur Sitzung von <code>tcadmin</code> zu gelangen.
<code>x2goclient</code> installieren	<code>sudo apt-get install x2goclient mingetty</code>
Anmelden auf freier Konsole als Benutzer <code>tc</code>	Drücken Sie die Tasten <code>[Alt]+[F3]</code> , und melden Sie sich als <code>tc</code> an.
Die Datei <code>.profile</code> ergänzen	<code>nano .profile</code> , fügen Sie am Ende der Datei nachstehende Zeilen ein: <code>if [-z "\$DISPLAY"] && [\$(tty) = /dev/tty7];</code> <code>then startx</code> <code>sudo shutdown -h now</code> <code>fi</code>
Anlegen von <code>.xinitrc</code>	<code>nano .xinitrc</code> , fügen Sie dies als Inhalt ein: <code>exec x2goclient</code>
Abmelden von <code>tc</code>	<code>exit</code>
Weiterarbeiten als <code>tcadmin</code>	Drücken Sie die Tasten <code>[Alt]+[F2]</code> , um zur Sitzung von <code>tcadmin</code> zu gelangen.
<code>sysVinit</code> durch <code>systemd</code> ersetzen	<code>rm /etc/apt/preferences.d/systemd</code> <code>apt-get update && apt-get install systemd dbus</code> <code>systemd-sysv</code> <code>reboot</code> <code>apt-get remove sysvinit</code>

Tabelle 9.3 Installation eines Banana Pi als Thin Client ohne BOOTP/TFTP (Forts.)

Vorgang	Kommando, Hinweis
Autologin für Benutzer tc: neue Service-Datei xauto.service mit nano oder vi anlegen	Datei <code>/etc/systemd/system/xauto.service</code> : [Unit] After = systemd-user-sessions.service [Service] ExecStart = <code>/sbin/mingetty --autologin tc --noclear tty7 38400</code> [Install] WantedBy = multi-user.target
xauto.service mit systemctl aktivieren	<code>systemctl enable xauto.service</code> <code>systemctl start xauto.service</code>
Kleinrechner neu starten	<code>sudo shutdown -r now</code>
Sitzung im x2goclient konfi- gurieren (1)	Vergeben Sie einen Sitzungsnamen, und tragen Sie einen auflösbaren Rechnernamen oder die IP-Adresse ein. Ergänzen Sie auch den Benutzernamen für das Ziel- system. Bei der Sitzungsart wählen Sie einen möglichst schlanken Desktop, wie hier LXDE (Abbildung 9.28).
Sitzung im x2goclient konfi- gurieren (2)	Wählen Sie entsprechend der Netzwerkanbindung die Geschwindigkeit (Abbildung 9.29).
Sitzung im x2goclient konfi- gurieren (3)	Für den Thin-Client-Einsatz wählen Sie hier, anders als dargestellt, für das Display VOLLBILD aus. Sie können Ihre Tastatureinstellungen aus dem lokalen Profil gel- ten lassen, geben Sie dann Modell (= Zahl der Tasten) und das Layout (= de) an. Die Audiounterstützung kön- nen Sie auch deaktivieren.
Anmeldebildschirm	Klicken Sie rechts die gewünschte Sitzung an. Tragen Sie Ihr Kennwort ein, und bestätigen Sie es mit OK. Die Sitzung wird aufgebaut.
Sitzung beenden	Klicken Sie im Sitzungsbildschirm auf ABMELDEN.
Banana Pi abschalten	Beenden Sie den x2goclient. Der Kleinrechner fährt das lokale System herunter und schaltet sich ab.

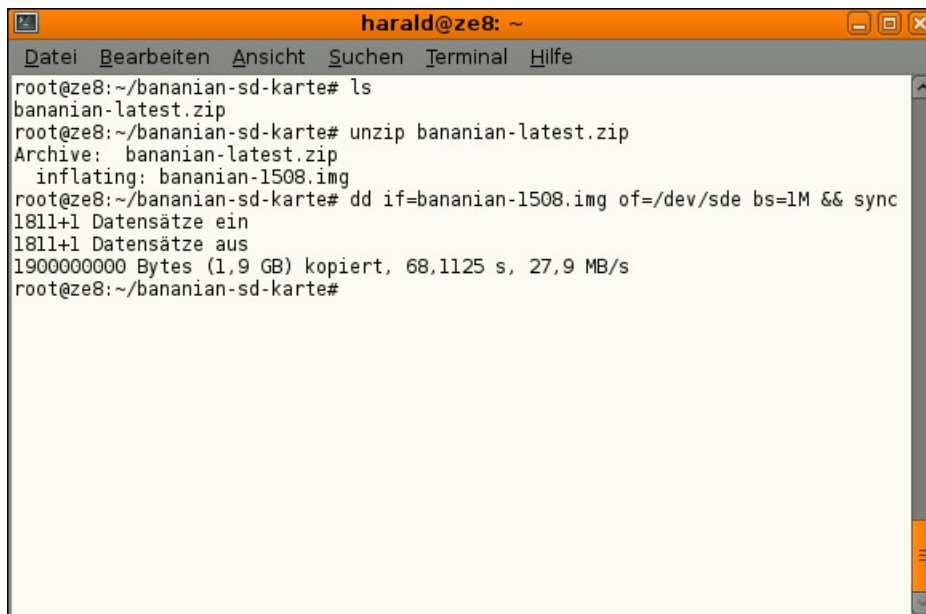
Tabelle 9.3 Installation eines Banana Pi als Thin Client ohne BOOTP/TFTP (Forts.)

```

root@ze8:~# lsblk
NAME        MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
fd0          2:0    1     4K  0 disk
sda          8:0    0 111,8G  0 disk
├─sda1       8:1    0  93,1G  0 part /
├─sda2       8:2    0  18,7G  0 part [SWAP]
└─sdb        8:16   0   1,8T  0 disk
   ├─sdb1     8:17   0  93,1G  0 part /tmp
   ├─sdb2     8:18   0 186,3G  0 part /var
   ├─sdb3     8:19   0 186,3G  0 part /srv
   └─sdb4     8:20   0   1,4T  0 part /home
sdc          8:32   0 931,5G  0 disk
├─sdc1       8:33   0 838,2G  0 part
└─sdc2       8:34   0  93,3G  0 part
sde          8:64   1    15G  0 disk
├─sde1       8:65   1    20M  0 part /media/harald/BCCA-7937
└─sde2       8:66   1    1,8G  0 part /media/harald/root
sr0         11:0    1 1024M  0 rom
root@ze8:~#

```

Abbildung 9.26 Ausgabe von »lsblk«, Ermitteln des Speichergeräts



```

harald@ze8: ~
Datei Bearbeiten Ansicht Suchen Terminal Hilfe
root@ze8:~/bananian-sd-karte# ls
bananian-latest.zip
root@ze8:~/bananian-sd-karte# unzip bananian-latest.zip
Archive: bananian-latest.zip
  inflating: bananian-1508.img
root@ze8:~/bananian-sd-karte# dd if=bananian-1508.img of=/dev/sde bs=1M && sync
1811+1 Datensätze ein
1811+1 Datensätze aus
1900000000 Bytes (1,9 GB) kopiert, 68,1125 s, 27,9 MB/s
root@ze8:~/bananian-sd-karte#

```

Abbildung 9.27 Entkomprimierung der Abbilddatei und Beschreiben der SD-Karte unter Linux

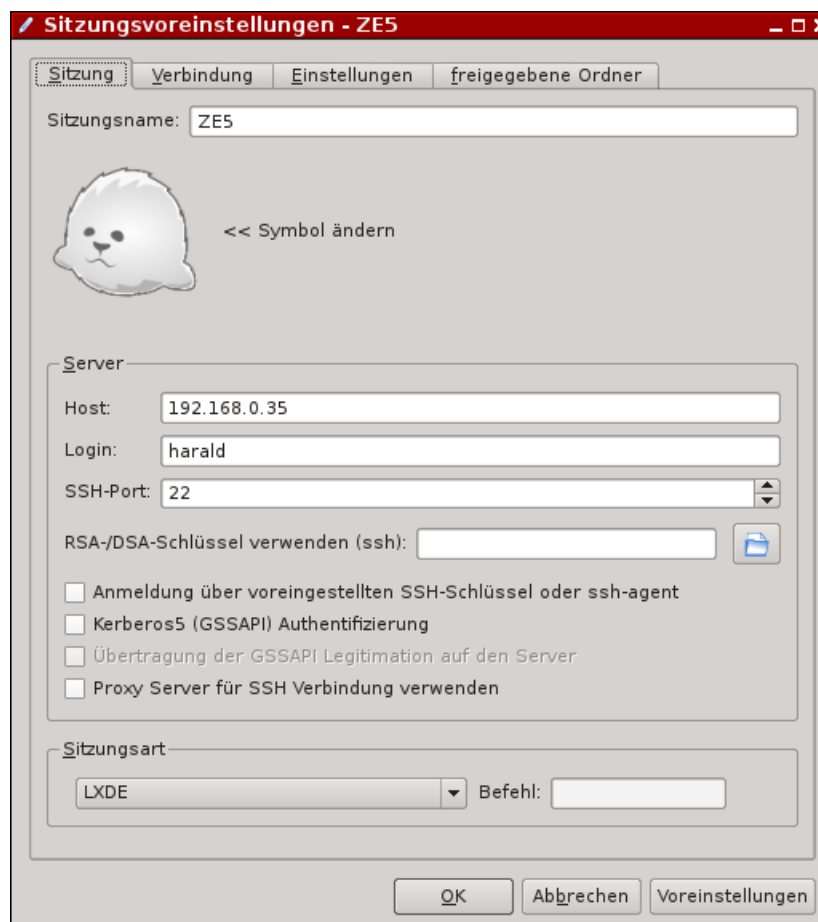


Abbildung 9.28 Sitzungseinstellungen im »x2goclient«
(Server, Benutzername, Sitzungsart und -name)

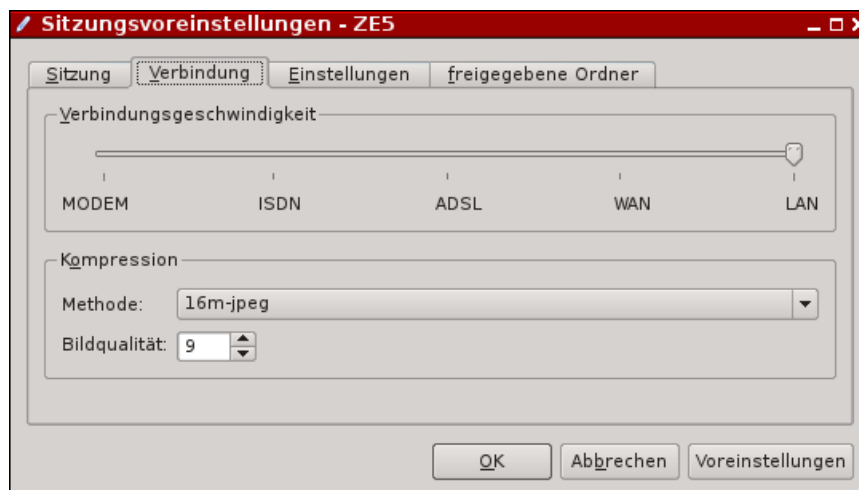


Abbildung 9.29 Einstellung der Übertragungsgeschwindigkeit beim »x2goclient«

Wenn Sie mehrere Banana Pis als Thin Client (TC) einrichten möchten, entnehmen Sie die SD-Karte eines nach Tabelle 9.3 konfigurierten Geräts. Unter Linux oder FreeBSD legen Sie mit einem Shell-Befehl die Abbilddatei an:

```
dd if=/dev/sdX of=bananatc.img bs=1M (X steht für das dritte Zeichen des
Gerätenamens).
```

Unter Microsoft Windows verwenden Sie ein entsprechendes Image-Programm.

Diese Abbilddatei schreiben Sie auf die weiter notwendigen SD-Karten, wie in Tabelle 9.3 beschrieben, nur dass die Eingabedatei (*if*) nunmehr *bananatc.img* heißt.

Stecken Sie die Karte in den »neuen« Banana Pi ein, und laden Sie den Kleinrechner. Drücken Sie die Tasten (Alt)+(F2), und melden Sie sich als *tcadmin* an. Mit `sudo nano /etc/hostname` öffnen Sie die Datei */etc/hostname* zum Bearbeiten. Ändern Sie hier den Eintrag zutreffend ab. Starten Sie mittels `sudo shutdown -r now` den Kleinrechner neu.

Sollen Ihre Banana-Pi-TCs über feste IP-Adressen verfügen, öffnen Sie `sudo nano /etc/network/interfaces`. Dort setzen Sie vor der Zeile `iface eth0 inet dhcp` das Kommentarzeichen

#. Dieses Zeichen entfernen Sie anschließend von den vier unteren Zeilen.

Ändern Sie die Beispieldaten entsprechend Ihren Vorgaben ab. Starten Sie den Kleinrechner neu, und prüfen Sie dessen Funktion.

Zusätzliche Sicherheit für X2Go-Heim- und Filialarbeitsplätze erhalten Sie, wenn Sie z. B. ein VPN einrichten.

Möchten Sie als Serververwalter wissen, welche Benutzer per X2Go angemeldet sind, rufen Sie `x2golistsessions_root` auf. Ohne Einschränkung der Ausgabe durch weitere Shell-Mittel erhalten Sie eine Vielzahl von Informationen: die Prozess-ID des X2Go-Agenten, die Session-ID (diese benötigen Sie für weitere Kommandos), den X2Go-Port, den X2Go-Server, den Status, den Anmeldezeitpunkt, ein Session-Cookie, die IP-Adresse von *X2Goclient*, den RX-Port, den Sende-Port, die letzte Aktivität, die Benutzer, die verbrauchte Zeit in Sekunden sowie die Port-Nummer für SSHFS.

Aus dieser Vielzahl filtern Sie eine übersichtliche Anzahl wichtiger Angaben heraus. Damit Sie dies nicht immer von Hand eingeben müssen, verwenden Sie dieses Shell-Skript:

```
#!/bin/sh
# werda.sh
# angemeldete X2Go-Benutzer anzeigen
while true;
do
clear
echo -n "Aktive x2go-Benutzer "; date
```

```

echo "-----"
x2golistsessions_root | cut -d \| -f2,8,12
echo "-----"
echo "Abbruch mit [STRG]+[C]"
sleep 15
done

```

Dies zeigt jede Viertelminute die Session-ID, die IP-Adresse des Arbeitsplatzes und den Benutzernamen an. Zum Beenden von Sitzungen rufen Sie `x2goterminate-session` zusammen mit dieser Session-ID auf. Auch hier vereinfacht Ihnen ein kleines Shell-Skript die Arbeit. Sie geben darin den leichter zu handhabenden Benutzernamen ein.

```

#!/bin/sh
# x2gokilluser.sh
# Beenden von X2Go-Sitzungen
#
echo -n "Benutzername eingeben: ";read bn
if [ -z $bn ];
then
exit
fi
echo "Gefundene Sitzung:"
sitzenzen=$(x2golistsessions_root | cut -d \| -f2,12 | grep $bn)
echo $sitzenzen
sitzenzen=$(echo $sitzenzen | cut -d \| -f1)
echo -n "Sitzung beenden? (j) ";read w
if [ "$w" = "j" ];
then
x2goterminate-session $sitzenzen
fi

```

Abbildung 9.30 zeigt Ihnen den Ablauf.

Vergessen Sie nicht, regelmäßig Updates auf Ihre Thin Clients einzuspielen (siehe auch Tabelle 9.3, Benutzer: `tcadmin`, `apt-get update` und `apt-get upgrade`)!

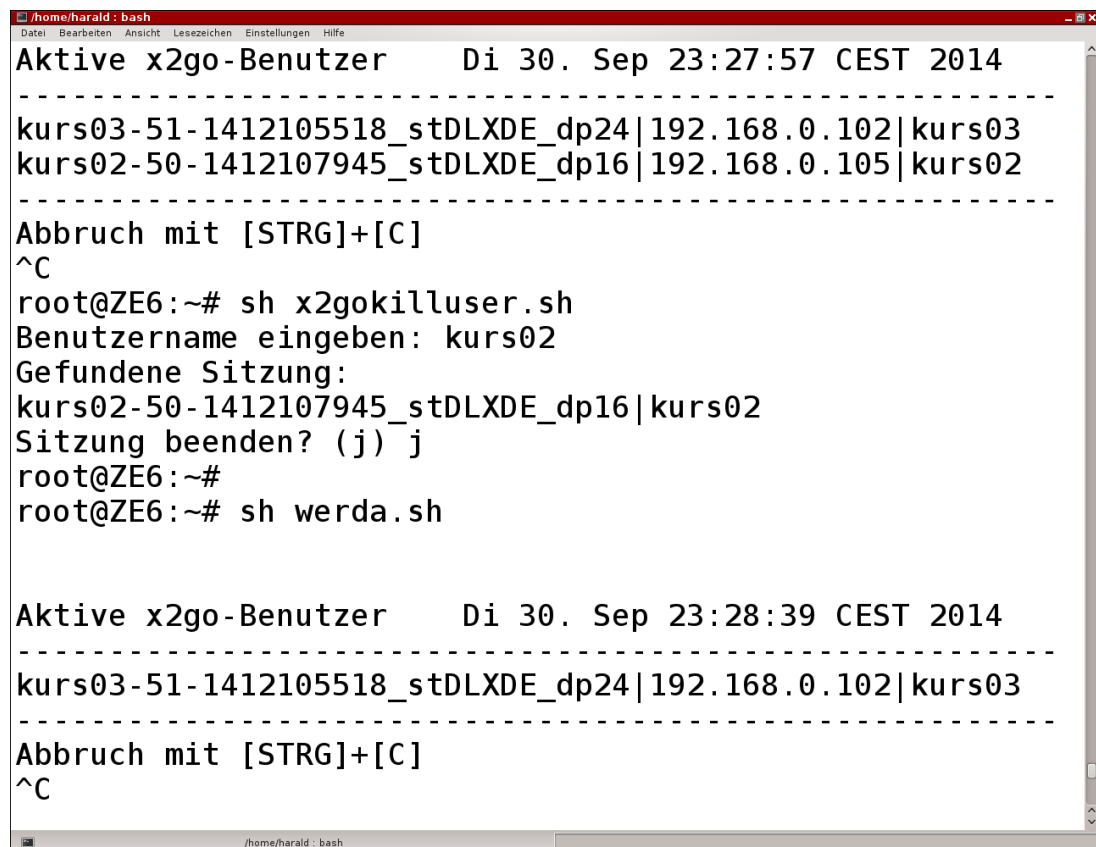


Abbildung 9.30 Sitzungsverwaltung mittels Shell-Skripten

9.5 Telefonie-Anwendungen über Netzwerke (VoIP)

Mit dem *Voice over Internet Protocol* (VoIP) werden Sprachdienste bezeichnet, die abseits der herkömmlichen Fernsprechtechnik geführt werden. An die Stelle der leitungsbezogenen Vermittlungstechnik treten Router.

Normalerweise wird für den Transport von Sprache (und auch Videotelefonie) UDP benutzt. Wenn einzelne Pakete verloren gehen, bemerkt der Telefonteilnehmer nur kleine Aussetzer. Solange sich die Zahl dieser Ausfälle in Grenzen hält, wird die Qualität der Übertragung nicht sonderlich beeinträchtigt.

9.5.1 Grundlagen

Die Fernsprechpartner betreiben sowohl als Anrufer den *User Agent Client* (UAC) als auch den *User Agent Server* (UAS). Dabei handelt es sich aber nur um eine Anwendung bzw. ein Endgerät. Dieses übersendet dem Registrar-Server die SIP- und IP-Adresse, der diese Informationen in einer Datenbank ablegt. Nur in einem Intranet oder bei kleinen Providern gibt der Server direkt Auskunft an Endgeräte. An dessen Stelle arbeitet üblicherweise der SIP-Proxy. Er nimmt Abfragen entgegen und holt sich die Informationen aus der Datenbank.

Manche Provider verwenden eigene Bezeichnungen für diese Dienste oder verlagern Kundenkontaktaufgaben auf weitere Server, z. B. einen Redirect Server. Bei der Konfiguration von Endgeräten führt dies regelmäßig zu Fehleingaben und damit zu Frust bei den Benutzern.

VoIP verwendet keine Telefonnummer im üblichen Sinne. Nur wenn Sie einen Übergang in das »normale« Fest- oder Mobilfunknetz benötigen, wird eine solche vergeben. Sie adressieren in der Form *sip:BENUTZER@DOMAIN/IP-ADRESSE* bzw. beim Vorliegen einer Telefonnummer durch *sip:+LÄNDERKENNZIFFER-VORWAHL-NUMMER@DOMAIN* das Ziel bzw. die eigene Erreichbarkeit.

Die Steuerung der Anrufe (Anbahnung, Halten, Beenden einer Verbindung) wird mittels des SIP-Protokolls (*Session Initiation Protocol*) abgewickelt; hierfür wird in der Regel der Port 5060 verwendet (Abbildung 9.31).

Zur Vertiefung können Sie die RFCs 2543, 3261 (Updates: RFCs 3265, 3853, 4320, 4916, 5393, 5621, 5626, 5630, 5922, 5954, 6026, 6141, 6665, 6878, 7462, 7463), 3265, 3515, 3665, 3581, 3853, 4320 und 4916 heranziehen.

Ähnlich dem HTTP-Protokoll verwendet das SIP-Protokoll *Response Codes*. Eine Auswahl dazu finden Sie in Tabelle 9.4.

Code	Bedeutung
100	Herstellung der Verbindung
180	Anläuten, Gegenseite erreichbar
181	Rufumleitung
182	Anruf in Warteschlange, z. B. bei der Vermittlung
183	Übergabe weiterer Informationen für den Verbindungsaufbau
199	Aufbau durch den Benutzer abgebrochen
200	Anfrage erfolgreich (OK)
300	Auswahl mehrerer Ziele
301	Rufumleitung, alte Adresse erloschen
302	Rufumleitung auf Zeit
305	auf benannten Proxy zum Erhalt weiterer Informationen zugreifen
400	Anfrage hat Syntaxfehler.

Tabelle 9.4 Die »Response Codes« des SIP-Protokolls

Code	Bedeutung
401	Benutzeranmeldung erforderlich
403	Zugriff verboten
404	Benutzer (Rufnummer) unbekannt
407	Proxy verlangt Benutzerauthentifizierung.
408	Zeitüberschreitung der Anfrage
410	Benutzer (Rufnummer) erloschen
433	anonymer Zugriff verboten
480	Ziel momentan nicht erreichbar (abgeschaltet)
486	belegt
487	aufgelegt
500	interner Serverfehler
503	Dienst wegen Wartung oder Überlastung nicht verfügbar
600	Überlastung, alle Ziele bzw. »Leitungen« belegt, Anruf kann auch nicht auf Ausweichziele (wie AB) geleitet werden.

Tabelle 9.4 Die »Response Codes« des SIP-Protokolls (Forts.)

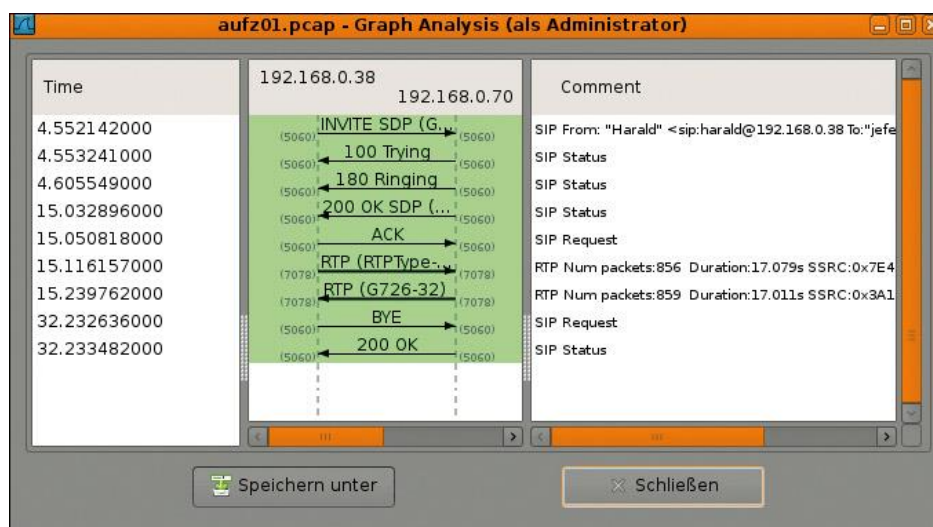


Abbildung 9.31 Die Steuerkommandos des SIP-Protokolls

Die Informationsübertragung als solches (Sprache, Video ...) steuern Sie mittels zweier anderer Protokolle:

RTP (Realtime Transport Protocol, Datenstrom) und mit
RTCP (Realtime Control Protocol, Flusskontrolle, Steuerung).

Diese *können* die Ports 5004 und 5005 belegen, in der Regel werden aber andere, wie z. B. 7078, genutzt (siehe dazu die RFCs 1890, 2508, 3545, 3550, 3551, 3611, 5506, 5761, 6051, 6222, 7007, 7022, 7160 und 7164).

Die Sprache wird mittels eines Codecs digitalisiert. Diese Information wird durch das RTP-Protokoll übergeben. Gängige Codecs sind G.722, G.711, G.723.1, G.726-32 und G.729. Sie unterscheiden sich hinsichtlich ihrer Bandbreite und damit auch in Bezug auf die Sprachqualität.

Liegen Ihre Geräte hinter einer Firewall, haben Sie zwei Möglichkeiten, diese »ins Netz« zu bringen. Entweder Sie erlauben die Port-Weiterleitung (Abbildung 9.32), oder Sie nutzen den meist vom Provider vorgegebenen STUN-Server.

telefon	IPv4-UDP	IP 192.168.0.38, port 5060 in lan	☒				
From any host in wan							
Via any router IP at port 5060							
tele2	IPv4-UDP	IP 192.168.0.38, port 7078 in lan	☒				
From any host in wan							
Via any router IP at port 7078							
tele3	IPv4-UDP	IP 192.168.0.38, port 9078 in lan	☒				
From any host in wan							
Via any router IP at port 9078							

Abbildung 9.32 Port-Weiterleitungen für VoIP

Der *STUN*-Server (STUN: Simple Traversal of User Datagram Protocol [UDP] Through Network Address Translators [NATs]) ermöglicht den Endgeräten »hinter« einer Firewall (mit NAT/PAT) den Verbindungsaufbau mit dem VoIP-Provider. Dabei ermittelt die Anwendung/das Endgerät die öffentliche Internetadresse und den entsprechenden lokalen Port und übergibt diese Informationen dem Server. STUN-Server verwenden zwei IP-Adressen und *können* den Port 3478 verwenden.

Das Endgerät 192.168.5.20 sendet eine STUN-Anforderung über den DSL-Router 192.168.5.1 (= auch Gateway) an den STUN-Server 93.184.216.34, der auf der SIP-Port-Nummer 5060 Anfragen erwartet. Der DSL-Router (Gateway) ändert dabei den Port auf seiner »öffentlichen« Seite von 5060 nach z. B. 15060. Der STUN-Server 93.184.216.34 sendet seinerseits eine Anfrage an die öffentliche Adresse des Gateways mit der geänderten Port-Nummer zurück. Der eigentliche SIP-Verbindungsaufbau kann beginnen.

Die RFCs 5389 5766, 5769, 5780, 6062 und 6156 führen Sie in die Details ein.

9.5.2 Endeinrichtungen und ihre Konfiguration

Sie können auf verschiedene Endeinrichtungen zugreifen:

Softwarelösungen für PCs und Smartphones,
VoIP-Adapter für analoge und ISDN-Telefone,
DSL-Heimrouter und Telefonanlagen, die den Anschluss von analogen bzw. ISDN-Endgeräten ermöglichen,
Telefonanlagen, die mit VoIP-Telefonen zusammenarbeiten,
VoIP-Telefone.

Fast alle diese Geräte werden üblicherweise mittels einer Webschnittstelle über das lokale Netzwerk konfiguriert. Die dabei anzugebenden Zugangsdaten können sich in ihrer Art fallweise von Provider zu Provider unterscheiden. Tabelle 9.5 zeigt Ihnen eine Übersicht über diese möglicherweise erforderlichen Informationen. Nicht bei jedem Provider werden alle aufgezeigten Angaben benötigt.

Angabe	Eintrag	Hinweis
SIP-ID / Benutzer	Telefonnummer	Hauptfehler: Schreibweise der Telefonnummer
Benutzername	normalerweise nicht die Telefonnummer, sondern eine extra Zugangskennung	meist Kundennummer, E-Mail-Adresse o. Ä.
Passwort	Zugangskennwort	
Registrar	Adressangabe für die Session-Initiation-Protocol-Registrierung	
Realm	Server mit den Benutzerdaten	Benutzerdatenbank
SIP-Proxy	URL des SIP-Dienstes	meist wie Registrar
STUN-Server	URL des STUN-Servers	dient dem Zugriff aus einem durch NAT verborgenen Netz

Tabelle 9.5 Angaben zur VoIP-Konfiguration

Eine Konfigurationsmaske eines VoIP-Programms finden Sie in Abbildung 9.33. Die geforderten Angaben können dabei Laien leicht überfordern. Provider benennen oftmals die Zugangsdaten mit anderen Bezeichnungen.

Abbildung 9.33 Konfigurationsmaske eines VoIP-Programms

Wenn die Verbindung zum VoIP-Provider nicht funktioniert, prüfen Sie zunächst, ob Ihr Endgerät auch durch die Firewall die Außenwelt erreicht (Stichwort: STUN-Server).

Ist dies der Fall, prüfen Sie, ob die zutreffenden Einträge bei Server, »Telefonnummer«, Benutzerkennung und Kennwort stimmen. Spätestens an dieser Stelle klären sich schon viele Probleme.

9.5.3 Besonderheiten der Netzwerkinfrastruktur für VoIP

Ein VoIP-Telefon (»Hardware«) benötigt eine eigene Stromversorgung. Um die Akzeptanz des Telefonierens über das Netzwerk zu erhöhen, möchte man den zusätzlichen Verkabelungsaufwand (Steckernetzteil) vermeiden (»Luxusmanagertelefone der alten Technik« brauchten aber auch schon eine eigene Stromversorgung ...). Aus diesem Grund werden Switches oder PoE-Injektoren (*Power over Ethernet*) verwendet, die die Versorgungsspannung in das LAN speisen. Nach dem Standard IEEE 802.3at-2009 wird eine Nennspannung von 48 Volt abgegeben. Ältere Standards lassen eine Stromabgabe von 350 mA zu, neuere maximal 600 mA. Betriebliche Vorteile bringt diese Technik eigentlich nur, wenn Sie beispielsweise einen WLAN-Accesspoint oder ein VoIP-Telefon an einer Stelle montieren möchten, in deren Nähe sich keine Stromversorgungsleitungen befinden und nur das LAN-Kabel geführt wird. Normalerweise lässt sich das andernfalls notwendige Steckernetzteil ebenso »ungesehen« in den Kabelleisten moderner Büroschreibtische unterbringen. Die genaue Spezifikation können Sie unter <http://standards.ieee.org/getieee802/download/802.3at-2009.pdf> herunterladen und nachlesen. Auch auf der Seite www.poweroverethernet.com finden Sie in englischer Sprache Informationen zu diesem Thema.

Mit *Quality of Service* (QoS) versucht man, durch Bandbreitenmanagement schlechter Sprach- und Bildübertragung Herr zu werden. Sie benötigen in jedem Fall Hardware, die dies unterstützt, um Datenverkehr entsprechend priorisieren zu können. E-Mails, WWW-Zugriffe und »normale« Datenübertragungen laufen dann langsamer zugunsten der Telefonie. Es ist aber kein Heilmittel gegen zu wenig installierte Bandbreite! Dies betrifft alle »Netzwerker«, vom LAN-Admin bis natürlich hin zum Internet-Provider und Backbone-Betreiber.

In den RFCs 3644, 2386, 3670, 4323, 4923, 5160, 5432, 5624, 5777, 5866, 5966, 5977, 7222 und 7561 finden Sie die derzeit angewandten Standards.

9.5.4 Sonderfall Fax: T38

Das menschliche Gehör verfügt über eine eigene Art von Fehlerkorrektur. Kürzere Abrisse durch verlorene Datenpakete, aber auch Störgeräusche können zu einem gewissen Maße ausgeglichen werden. Das ist bei einem Faxgerät anders. Hier darf bei der Übertragung kein einziges Paket verloren gehen. Daher sind häufige Abbrüche über VoIP-Verbindungen keine Seltenheit. Wenn der Codec G.711 verwendet wird, *kann* es aber wenigstens für eine Seite ohne Probleme funktionieren. Von einem analogen Faxgerät ausgehend, benötigen Absender und Empfänger gleichermaßen einen VoIP-Adapter (oder ein DSL-Routergerät mit entsprechender Ausstattung), der die ITU-Norm T38 unterstützt. Diese Adapter nutzen dann das *Internet Fax Protocol* (IFP). Natürlich muss auch der VoIP-Provider die Übertragung unterstützen. Problematisch sind meist Verbindungen, in denen ein Partner noch »echte« Telefontechnik und der andere schon *All-IP* benutzt.

Zusätzlich können Sie Ihr Faxgerät noch in den robusten »Überseemodus« schalten, was Abbrüche ebenso minimieren kann.

9.5.5 Sicherheit

Verwenden Sie für VoIP ein am besten physikalisch getrenntes Netz. Lesen Sie hierzu auch die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik, die Sie unter www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/baust/b04/b04007.html finden. Die manchmal sogar mit internem Switch ausgestatteten Telefone können zu Sicherheitsproblemen mutieren, besonders dann, wenn einige Zeit nach deren Abverkauf im Handel keine Software-Updates mehr angeboten werden. In einem eigenen Netz, das nur der Sprachübertragung dient, wird dann

wenigstens nicht die restliche IT-Infrastruktur angegriffen.

Bei der Kommunikation zwischen zwei Standorten (Zweigstellen, Teilbetriebe) nutzen Sie VPN oder einen SSH-Tunnel. Dies ist in Abschnitt 9.3, »Aufbau eines SSH-Tunnels« und Abschnitt 10.6.2 beschrieben.

Auch wenn es bequem erscheint, lagern Sie Ihre interne Kommunikation nicht an einen externen Dienstleister aus. Die eigene Telefonanlage benötigt nur einen extra Rechner, Container (LXC) oder eine virtuelle Maschine. Mit *Asterisk* (www.asterisk.org) können Sie sich so etwas aufbauen (lassen). Alternativ sehen Sie sich einmal *Gemeinschaft an*: www.alternative-solution.de/gs5. In jedem Fall lernen Sie beim Aufsetzen einer VoIP-Telefonanlage eine Menge Grundlagen, die vom Umfang her ein eigenes Buch ergeben würden.

Grundsätzlich ist die VoIP-Kommunikation nicht abhörsicher und kann von jeder halbwegs technisch versierten neugierigen Person auch aufgezeichnet werden. Abhilfe besteht in der Verwendung der Protokolle SSIP und SRTP, die Steuerung und Nutzlast verschlüsseln. Fragen Sie bei Ihrem Provider nach! Natürlich müssen auch die Endgeräte/ die Software dies unterstützen. SIP und RTP über TLS ermöglichen nur den sicheren Transfer zwischen zwei Punkten, nicht aber über die gesamte Strecke.

Die hierfür maßgeblichen RFCs sind unter anderem RFC 5630 und 5506.

9.5.6 Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP

Um sich über das Netzwerk nur unterhalten zu können, benötigen Sie nicht unbedingt einen extra Telefonie-Provider. Mit wenigen Schritten schaffen Sie Ihre Verbindung im LAN:

Beide Partner ermitteln ihre IP-Adresse.

Beide Partner schalten ihr IP-Telefon ein bzw. starten ihr Telefonie-Programm.

Einer der Partner gibt die URL in der Form **sip:BENUTZER@IP-ADRESSE** ein und lässt anwählen.

Die Gegenstelle nimmt an. Das Gespräch kann geführt werden.

In Abbildung 9.34 sehen Sie die beiden »Softphones« mit bestehender Verbindung.

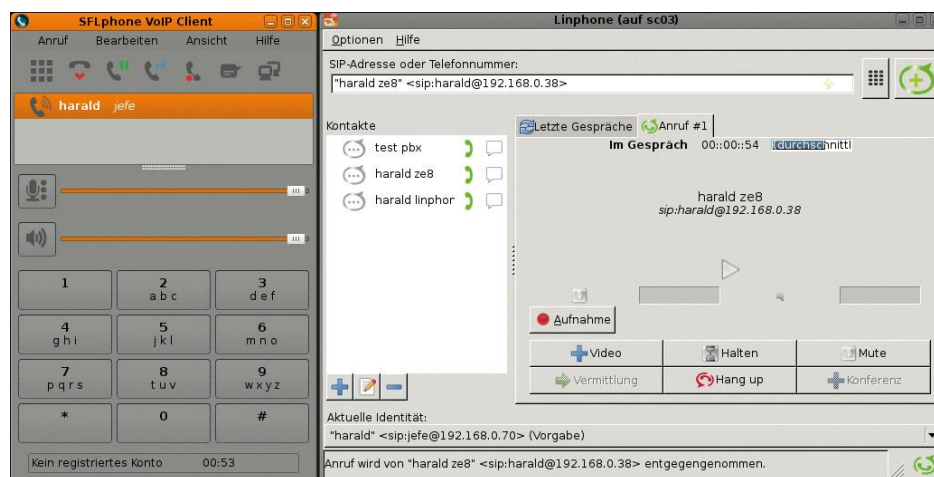


Abbildung 9.34 Sprachverbindung über das LAN

9.5.7 Remote Desktop Protocol (RDP)

Mit dem RDP können Sie PCs unter Microsoft Windows fernsteuern. Client-Programme finden Sie auch für Linux und sogar PDAs. Für Linux können Sie `xrdp` als Server installieren. Auf einem Windows-PC benötigen Sie keine weitere Software.

Klicken Sie in Windows 7 in folgender Reihenfolge an:

Start • Computer (rechte Maustaste) • Eigenschaften (unter Windows 8/8.1/10 klicken Sie mit der rechten Maustaste auf das Windows-Symbol • System).

Links im Fenster klicken Sie Remoteeinstellungen an. Gegebenenfalls müssen Sie jetzt das Administrator Kennwort eingeben. Im Dialogfeld Systemeigenschaften wählen Sie eine der Optionen aus und fahren mit Benutzer auswählen fort. Hier fügen Sie einen Remotedesktop-Benutzer hinzu.

So bauen Sie die RDP-Verbindung auf: Das Programm liegt unter Programme • Alle Programme • Zubehör. Hier geben Sie nach dem Start die Anmeldeinformationen ein. Die Verbindung kann hergestellt werden.

Kapitel 10

Netzwerkpraxis

In diesem Kapitel finden Sie zusammengefasste Informationen zur Planung, zum Bau und zum Betrieb von Netzwerken. Sie finden hier Anregungen für die Umsetzung eigener Projekte.

10.1 Planung von Netzwerken

Die Planung eines Netzwerks können Sie in verschiedene Phasen unterteilen. Damit erreichen Sie mehr Klarheit und schaffen mehr Entscheidungsspielraum. Bevor Sie den ersten Meter Netzkabel verlegen (lassen), haben Sie bereits den Bedarf und den Ist-Zustand ermittelt, die räumlichen und baulichen Verhältnisse erkundet, sich Gedanken über die Ausfallsicherheit gemacht und Investitionssicherheit und Unterbringung durchdacht.

10.1.1 Bedarf ermitteln

Für Nachrüstungen und Neubauten müssen Sie die Zahl der Netzwerkanschlüsse überschlägig ermitteln.

Wie viele Netzwerkanschlüsse Sie in einem Betrieb benötigen, hängt überwiegend vom tatsächlichen Gebrauch der EDV ab. Bei Verkabelungsprojekten versuchen die Bauherren oft die Kosten dadurch zu drücken, dass sie auf Nachrüstmöglichkeiten und den Einsatz von mobilen Mini-Switches setzen. Einfache und kostengünstig vorzunehmende Nachrüstungen sehen Sie sowieso vor. Beim Einsatz von Mini-Switches sollten Sie aber Folgendes bedenken:

Bei zugriffsintensiven Netzwerkteilnehmern wird die Kapazität der Zuleitung zum Haupt-Switch mit jedem aktiven Anschluss des Mini-Switchs geteilt. Damit werden die Zugriffe für die angeschlossenen Geräte verlangsamt (Abbildung 10.1).

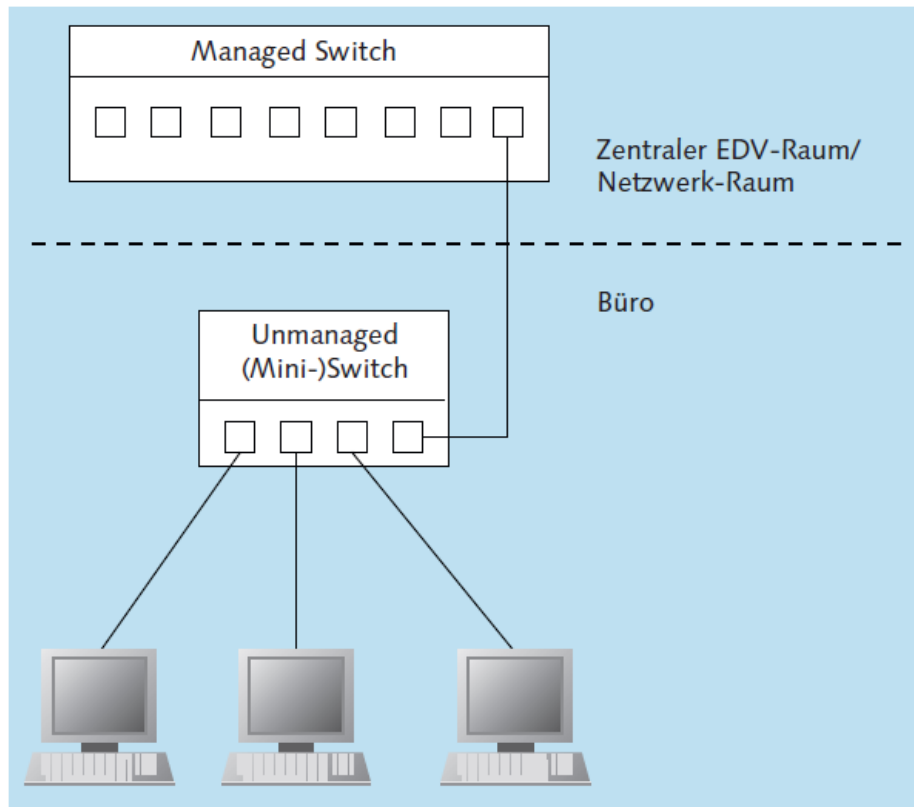


Abbildung 10.1 Weiterverteilung mit Mini-Switch

Sicherheitsmaßnahmen am Haupt-Switch wirken meist nur beim Mini-Switch, nicht bei daran angeschlossenen PCs und Druckern.

Sehen Sie deshalb nur 1:1-Anschlussmöglichkeiten zum zentralen Switch vor!

Wie viele Anschlüsse Sie je Arbeitsplatz vorsehen müssen, hängt natürlich von der Art des Geräteeinsatzes ab:

Wie viele PCs oder Thin Clients benutzt eine Person an einem Arbeitsplatz?
 Verwenden Sie Netzwerkdrucker/Printserver?
 Müssen mitgebrachte Außendienst-Laptops am gleichen Arbeitsplatz angeschlossen werden, oder sehen Sie für diese Personen eigene Büros vor?
 Haben Sie vor, Voice over IP als Haustelefon einzusetzen?

Werden Überwachungskameras, Fernwirkleinrichtungen, Steuerungen, Besucherterminals, Werbemonitore usw. eingesetzt?
 Maschinen: Wie viele Anschlüsse hat eine Maschine, und wie viele kommen zum Einsatz?
 Administrative Arbeitsplätze: Betreiben Sie mehrere Netze (»Echtnetz« und »Schattennetz«)?
 Arbeiten Sie mit Reserveräumen?
 Liegt das Gebäude in einem Überschwemmungsgebiet? (Eventuell müssen Sie die Lage des EDV-Raumes anpassen.)
 Sind Erweiterungen in der nahen planbaren Zukunft für Sie schon vorhersehbar?
 Nach Ihren Erhebungen richten sich:
 die Zahl der Anschlüsse, also der Netzwerkdosen und Zuleitungen in den Räumen
 die Zahl der Anschlüsse am zentralen Switch
 die Leistungsmerkmale des zentralen Switches
 die Zahl der Anschlüsse am zentralen Patchfeld
 die Aufnahmefähigkeit der Kabeltrassen
 der Bau neuer Kabeltrassen
 die Größe und die zusätzliche Ausstattung zentraler Netzwerk- und Rechnerräume
 zusätzliche Maßnahmen, wie die Berücksichtigung einer höheren Brandlast und die

eventuelle Erweiterung der Sicherheitstechnik
rechtliche Rahmenbedingungen (Unfallverhütungsvorschriften, Baurecht usw.)

10.1.2 Ermitteln des Ist-Zustands

Bei Erweiterungen und Erneuerungen der Netzwerkinfrastruktur müssen Sie abwägen, was Sie von der vorhandenen Technik noch über längere Zeit verwenden können. Für Ihre Entscheidung müssen Sie Folgendes feststellen:

Reichen die Anschlüsse im Arbeitsplatzbereich aus?
Ist die Übertragungsgeschwindigkeit für Ihre Anwendungen noch über einen längeren Zeitraum ausreichend?
Sind die verbauten Kabel noch für höhere Geschwindigkeiten nutzbar?
Sind die verbauten Kabel mit dem Telefonnetz kombiniert (strukturierte Verkabelung, gemeinsame Nutzung der Kabel für Telefon und 100Base-T-Netze)? In welchem Zustand befinden sich die zentralen Einrichtungen?
Haben zentrale Komponenten wie Switches und Patchfelder noch freie Kapazitäten?
Verfügt der zentrale Switch über zeitgemäße Ausstattungsmerkmale (Sicherheit, VLAN usw.)?
Sind zentrale Komponenten nach derzeitigen und vorhersehbaren künftigen Kriterien ausreichend untergebracht, gesichert und gegebenenfalls klimatisiert?
Mit welchem Aufwand lassen sich Erweiterungen installieren?
Sind eventuell vorhandene Kabeltrassen aufnahmefähig?
Stehen weitere Sanierungsmaßnahmen für das Gebäude an?

Die Antworten auf diese Fragen fließen in Ihre Planungen mit ein. Bei einem Neubau haben Sie natürlich keine »Altlasten« zu berücksichtigen.

10.1.3 Berücksichtigung räumlicher und baulicher Verhältnisse

Bei einem Neubau können Sie meist die Bedürfnisse der Netzwerktechnik in vollem Umfang berücksichtigen. Anders sieht es bei Bestandsbauten aus. Hier müssen Sie bei der Einbringung der neuen Netzwerktechnik auf weitere Gegebenheiten Rücksicht nehmen:

Denkmalschutz: Wie können Sie trotzdem Kabelkanäle oder Unterputzleitungen in das Gebäude einbringen?
Bausubstanz: Haben Sie Feuchtigkeit im Gebäude?
Grundriss: Wie lässt sich das Leitungsnetz am effektivsten anordnen?
Sicherheit: Wie kann der EDV-Raum einfach und effektiv geschützt werden?
Telefonnetz: Ist hier eine ausreichende Infrastruktur vorhanden? Können hier Kabelarbeiten zusammengefasst werden?
Klimatisierung: Wie können Sie die eventuell notwendige Klimatechnik im Rechnerraum unterbringen?
Stromversorgung: Reicht die Gebäudestromversorgung aus? Wo können Sie eine USV-Anlage unterbringen?
Brandschutz: Hat das Einbringen der Verkabelung und die damit verbundene Erhöhung der Brandlast Folgen?
Brandmeldeanlage: Ist eine solche Anlage vorhanden oder notwendig?
Zutrittskontrolle/Alarmanlage: Ist eine Anlage vorhanden, oder muss eine errichtet werden?

10.1.4 Investitionssicherheit

Auch bei der Planung des Netzwerks stehen Sie zwischen kaufmännischen Zwängen und technischer Vernunft. Falsches Sparen führt aber auch hier dazu, dass Sie später mit eventuell teuren Nachrüstmaßnahmen »belohnt« werden. Schenken Sie deshalb einigen Punkten Beachtung:

Sind für Sie Erweiterungen des Netzes absehbar?
Können Sie bereits jetzt günstig die Voraussetzungen für solche Erweiterungen schaffen (mehr Trassenplatz, mehr Einbauplatz für Switches und Patchfelder, Auslegung von USV und Klimatechnik)?
Verwenden Sie die Verkabelungstechnik mit der höchstmöglichen Übertragungsgeschwindigkeit.
Raumanbindung: Setzen Sie zusätzliche Leerrohre ein, oder sehen Sie größere Kabelkanäle

vor.

Sehen Sie eine leichte Austauschbarkeit der Verkabelung vor. Zu solchen Maßnahmen gehören neben Leerrohren und Kabelkanälen mit mehr Platz *Zugdosen* und weiter gefasste Radien in der Kabelführung.

Switch(es): Können Sie diese Geräte einfach per gesichertem Webzugang konfigurieren, oder müssen Sie auf systemabhängige proprietäre Software zurückgreifen?

Switches: Können und dürfen Sie diese selbst konfigurieren?

Zentrale Komponenten (Switch, USV, Klima): Wie lange und unter welchen Kosten und Bedingungen gewähren Hersteller oder Lieferanten zentraler Komponenten eine unbedingte Schadenersatzleistung (Garantie)? Welche Zeiten werden für die Wiederherstellung der Funktionsbereitschaft angeboten? Unterscheiden Sie zwischen Reaktionszeit und Reparaturzeit. Können Sie günstig eine Garantieverlängerung abschließen?

Zentrale Komponenten: Wer kommt zur Behebung einer Störung? Hat der Kundendienst eine lange Anfahrt?

Zentrale Komponenten: Achten Sie auf vollständige IPv6-Kompatibilität.

10.1.5 Ausfallsicherheiten vorsehen

In Grenzen können Sie Ihre Netzwerkinfrastruktur vor Ausfällen schützen. Hauptsächliche Gründe für einen Ausfall können sein:

Stromausfall: Hiergegen setzen Sie ein USV-Konzept ein (unterbrechungsfreie Stromversorgung).

Funktionsausfall Switch: Halten Sie entweder ein Reservegerät oder Reservebaugruppen

vor, oder bilden Sie den zentralen Switch aus mehreren managbaren kleineren Einzelgeräten. Von den kostengünstigen Einzelgeräten beschaffen Sie eines oder mehrere als Ausfallreserve.

Kabelschaden: Schaffen Sie die Möglichkeit des leichten Kabelwechsels, sehen Sie auch Reserveleitungen in wichtigen Bereichen des Betriebs vor.

Klimatisierung: Verteilen Sie, wenn möglich, die Arbeit auf mehrere Anlagen.

Abhängigkeit von Kundendiensten: Achten Sie bei Ihrer Auswahl darauf, dass Sie und gegebenenfalls Ihre Kollegen bei Ausfällen so viel wie möglich selbst beheben können.

VoIP: Wenn das LAN ausfällt, ist telefonisch niemand erreichbar. Es sollte zumindest eine kleine Telefonanlage für Geschäftsleitung, EDV und Hausmeister sowie wichtige Abteilungen mit Kundenkontakt oder gefahrenorientierten Arbeiten installiert sein.

Meist ist in größeren Betrieben eine Brandmeldeanlage installiert, die einen eigenen Anschluss an das Telefonnetz besitzt. Diesen können Sie auf mehrere ISDN-Kanäle »aufweiten« lassen und dafür nutzen. Verzichten Sie aber sowohl auf DECT-Telefone (sie funktionieren nicht bei Stromausfall) als auch auf Funktelefone für das öffentliche Netz. Bei Letzteren erwarten Sie vielerlei Probleme, vom leeren, ungepflegten Akku bis hin zur Tatsache, dass niemand die Nummern der anderen Geräte kennt.

10.1.6 Zentrales oder verteiltes Switching

Je nachdem, wie Ihr Gebäude beschaffen ist, können Sie die zentralen Komponenten entweder in einem zentralen Raum oder nach Gebäuden bzw. Stockwerken unterteilt unterbringen. Die zentrale Unterbringung (Abbildung 10.2) bietet Ihnen Vor- und Nachteile:

Einen zentralen, gegebenenfalls überwachten Raum: In diesem sind auch andere Komponenten wie Router, Server und das zentrale Patchfeld untergebracht.

Anschlussmöglichkeit an die USV

Ein großer Switch oder mehrere kaskadierte Geräte tragen zur Erwärmung des EDVRaums bei.

Die verteilte Unterbringung der Switches auf dem Betriebsgrundstück oder im Haus ist sicher bei besonders umfangreichen Installationen auch eine Überlegung wert:

Ein kompletter Netzausfall ist (fast) unmöglich.

Es kommt zu keiner zusätzlichen Erwärmung durch die Switches.

Ersparnis bei der Verkabelung, da zu den einzelnen Räumen hin kürzere Verbindungen genutzt werden (stockwerksweise, flurweise usw.).

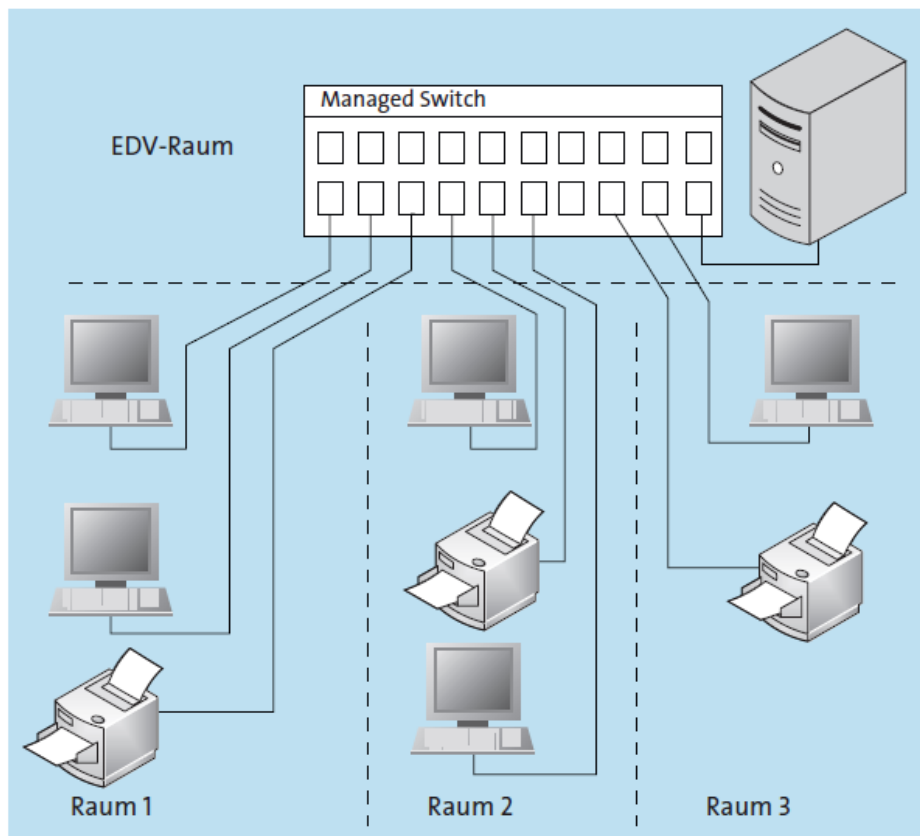


Abbildung 10.2 Zentraler Switch

Aber: Sie benötigen managere Switches, die das *Port Trunking* (Link Aggregation) unterstützen. Einige Anschlüsse der Switches werden hierfür benötigt und stehen nicht für den Anschluss von Netzwerkteilnehmern zur Verfügung (siehe auch Abschnitt 4.6.3, »Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)«, und Abbildung 10.3).

In bestimmten Fällen können Sie die Trunking-Verbindungen auch in Glasfasertechnik ausführen. Dies ist sogar notwendig, wenn die zulässigen Leitungslängen überschritten werden. Insgesamt ist die gemischte Ausführung (Kupfer/LWL) kostengünstiger als eine reine Glasfaserverkabelung.

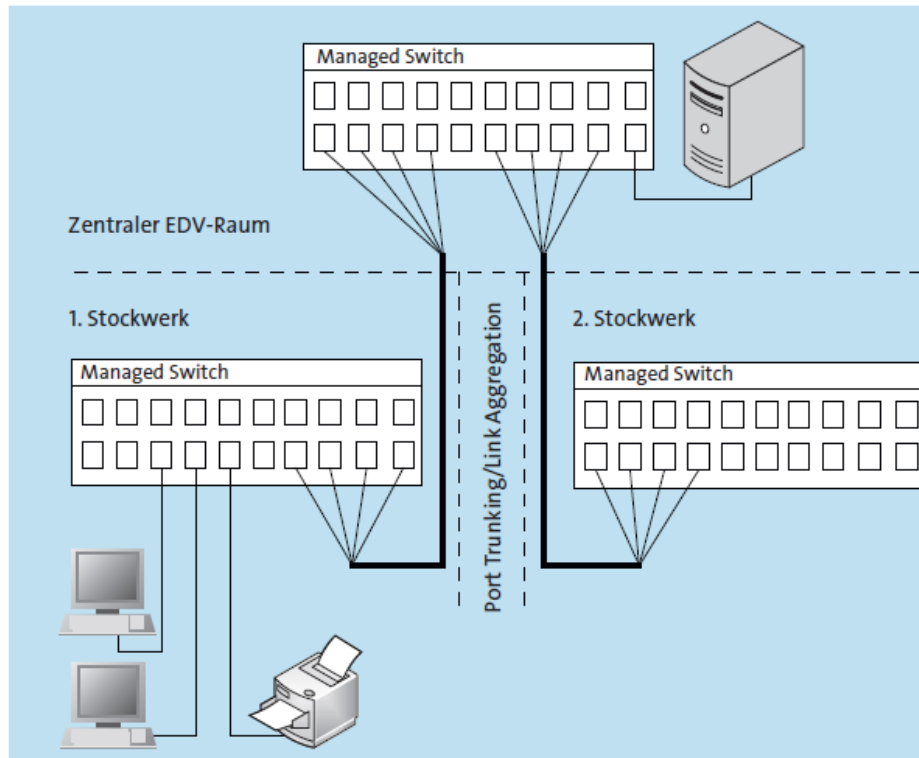


Abbildung 10.3 Verteiltes Switching

10.2 Netzwerke mit Kupferkabeln

Besonders räumlich kleinere Netze können Sie noch auf Jahre hin günstig in Kupfertechnik betreiben:

- Für Verkabelungsarbeiten benötigen Sie nur einfache Werkzeuge.
- Sie haben geringere Kosten für Router und Switches.
- Die Standardnetzwerkanschlüsse der Endgeräte (PCs, Thin Clients und Printserver) reichen aus.
- Mögliches Problem: Potenzialunterschied zwischen zwei Gebäuden, die Sie per Kupferkabel verbinden möchten. Diese eine Verbindung führen Sie besser in Glasfasertechnik aus.
- Beachten Sie: Die Schirmungen fest verbauter Netzwirkabel müssen durch einen Fachmann mit dem Potenzialausgleich des Gebäudes verbunden werden.

Technische Erläuterungen zu Kupferkabeln finden Sie in Abschnitt 2.1.2, »Netze mit Twisted-Pair-Kabeln«.

10.2.1 Kabel (Cat. 5 und Cat. 7)

Für die Ergänzung von älteren Bestandsnetzen können Sie in Einzelfällen noch das Kabel nach Cat. 5 verbauen. Bei Neuinstallationen oder umfangreichen Ergänzungen verwenden Sie lieber Cat. 7. Es ermöglicht nicht nur schnellere Datenverbindungen, es ist auch hinsichtlich seiner Schirmung deutlich besser.

Wenn Sie Kabel nach Cat. 7 verbauen, werden Sie immer noch auf die herkömmliche RJ45-Steckverbindertechnik zurückgreifen, auch wenn diese nicht der Cat.-7-Norm entspricht. Bis 1 Gbit/s können Sie damit übertragen. Ob sich noch neuere Normen mit höherer Geschwindigkeit für die Datenübertragung auf Kupfernetzen durchsetzen, ist nicht klar. Bevor Sie hierauf warten, verwenden Sie besser die Glasfasertechnik.

10.2.2 Anforderungen an Kabeltrassen und Installationskanäle

Ihre Kupferverkabelung benötigt eigene Kabeltrassen und Installationskanäle. Sie dürfen die Netzwirkabel nicht zusammen mit Stromkabeln in einem gemeinsamen Kanal führen (Abbildung 10.4). Wenn Sie am gleichen Ort einen Netzwerk- und Stromanschluss

benötigen, müssen Sie daher getrennte Kabelkanäle oder solche mit zwei getrennten Kammern (Abbildung 10.5) verwenden. Gleiches gilt für Leerrohre.

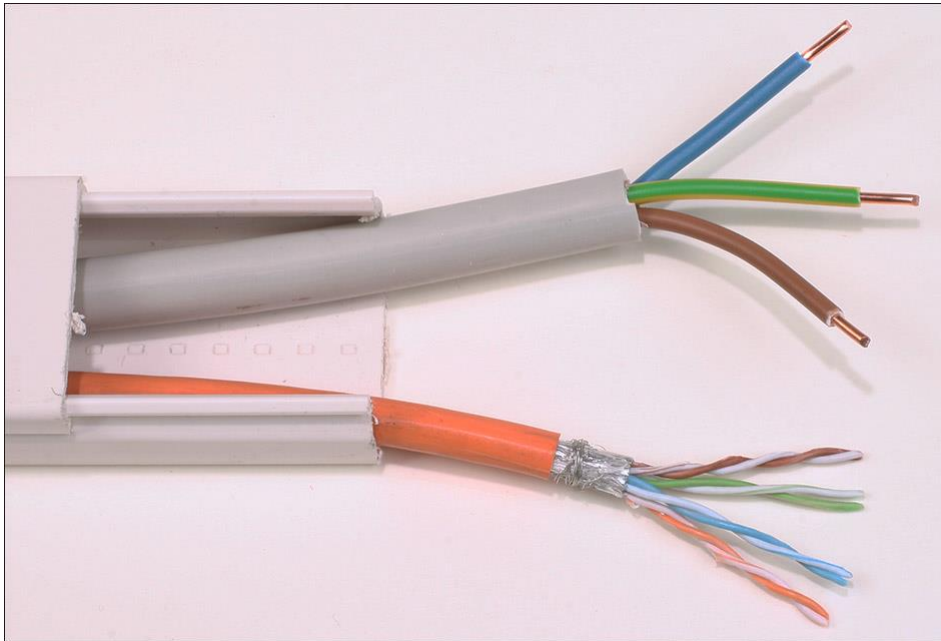


Abbildung 10.4 Verboten: gemeinsame Führung von Strom- und Netzkabeln

Kabelrinnen, die Sie entlang von Geschossdecken, aber auch Hallendächern (z. B. in Verbrauchermärkten, Werkhallen) anbringen lassen, müssen das Gewicht der Kabel sicher tragen. Denken Sie auch an mögliche Nachrüstungen, die vielleicht hierin verlegt werden.

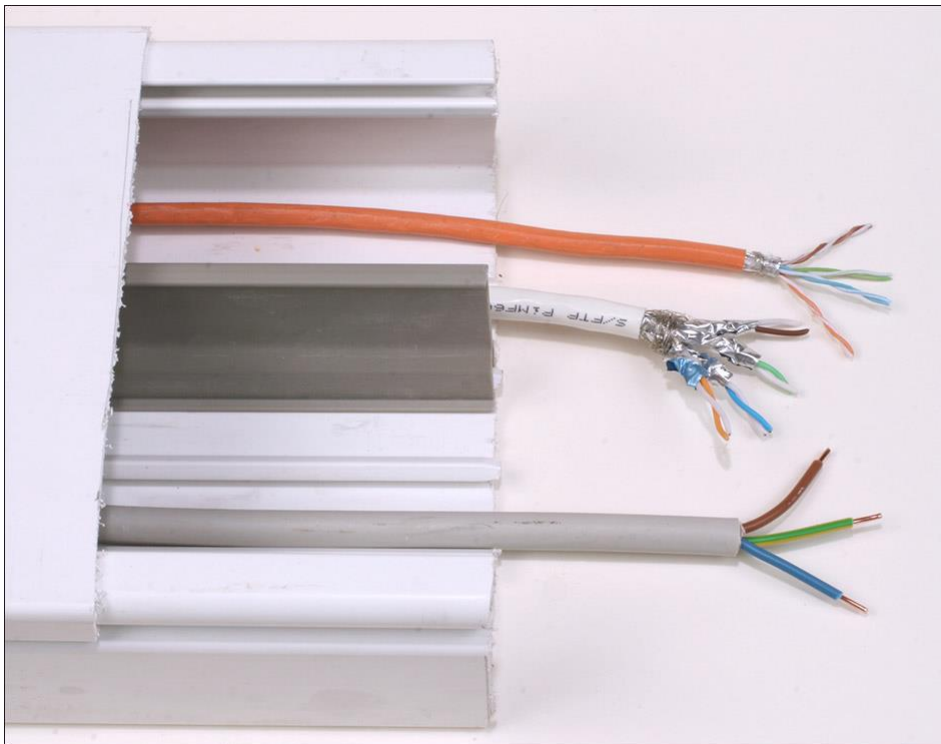


Abbildung 10.5 Richtig: Strom- und Netzkabel befinden sich in getrennten Kammern des Kabelkanals.

Die Kabelrinnen sollen auch nicht so überquellern, dass Kabel beschädigt werden können. Bringen Sie nur so viele Kabel in Kabelkanäle ein, dass Sie den Deckel noch ohne Druck und Gewalt wieder anbringen können. Bei Leerrohren ziehen Sie nur so viele

Kabel ein, dass Sie jederzeit defekte Kabel herausziehen können.

Achten Sie darauf, dass über Ecken und Kanten geführte Kabel nicht geknickt werden. Wenn es für Sie möglich ist, schaffen Sie größere Biegeradien.

Lassen Sie sich auch von einem Brandschutzexperten hinsichtlich weiterer Maßnahmen in Sachen Brandlast beraten. Zwischen Brandabschnitten verlaufende Kabeltrassen benötigen unter Umständen ein Brandschott.

Ihre Netzkabel sollten Sie vor Nässe, Fraßschäden (Lagerhausbetriebe!) und anderen Beschädigungen geschützt führen.

10.2.3 Dosen und Patchfelder

Bringen Sie Netzwerkdosen und Kabelkanäle so an, dass diese nicht beschädigt werden:

In Werks- und Lagerhallen, aber auch in Verbrauchermärkten und an ähnlichen Orten besteht die Gefahr, dass Sie mit Flurförderzeugen Kabelkanäle und Dosen regelrecht »abrasieren«. Hier bringen Sie einmal in Palettenhöhe (ca. 10 cm über dem Boden) und nochmals je 50 cm und 100 cm über dem Boden Schutzkeile an der Wand an. Damit weisen Sie an der Mauer entlangschrammende Fahrzeuge und ihre Lasten ab (Abbildung 10.6).

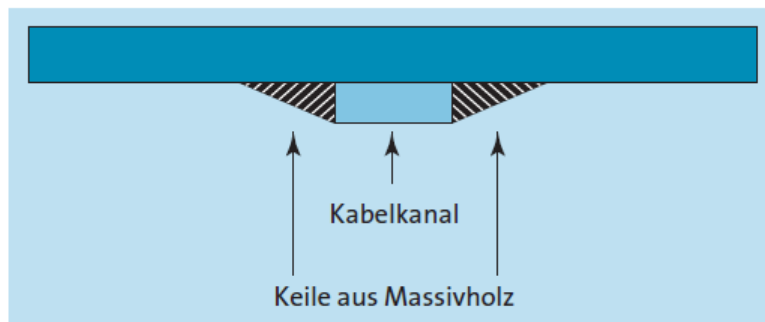


Abbildung 10.6 Schutzkeile für Aufputzkabelkanäle und Netzwerk-Anschlussdosen

Im Umfeld von Kleinkindern (Arztpraxen, Kindertagesstätten, Kindergärten oder auch zu Hause im Kinderzimmer) können Sie die Dose mit einem RJ45-Blindstopfen vor kleinen »Elektrikerfingern« schützen.

In Werks- und Lagerhallen mit hohem Staubanfall bewahren Sie Ihre Netzwerkdosen mit diesen Blindstopfen vor übermäßiger Verschmutzung der Kontakte.

Patchfelder verwenden Sie in der Hauptverteilung beim Switch (Abbildung 10.7) oder als Stockwerksverteiler. Sie sollten diese vor unbefugtem Zugriff schützen. Achten Sie darauf, dass sie vom Elektrofachmann an den Potenzialausgleich des Gebäudes angeschlossen werden.

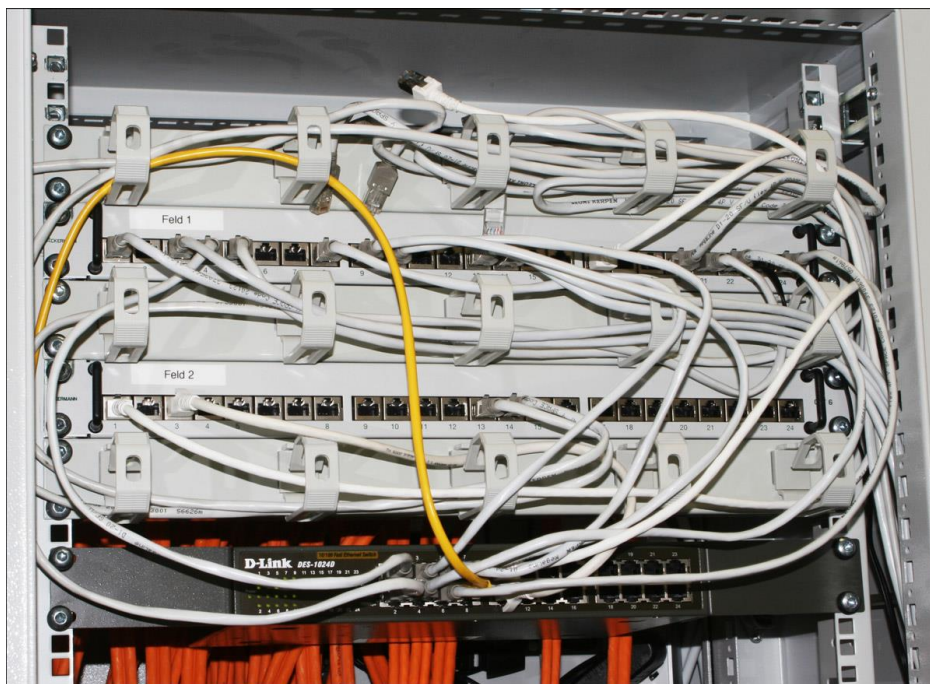


Abbildung 10.7 Netzwerkschrank mit Patchfeldern und Switch

Wie Sie die Patchfelder unterbringen, hängt vor allem von deren Größe und Menge ab. Hohe Anschlusszahlen montieren Sie in eigenen Netzwerkschränken, wie die aktiven Komponenten auch. Hier ist es wichtig, dass Sie keine zu langen Patchkabel zum Verbinden benötigen. Beschriften Sie jedes Patchkabel an beiden Enden jeweils in Steckernähe mit einer laufenden Nummer. Bei vielen Verbindungen können Sie sich bei Konfigurationsarbeiten die Kabelnummer und die Steckplätze an Switch und Patchfeld notieren. Im Störfall werden Sie das schnelle Auffinden der beteiligten Komponenten sehr schätzen. Kleine Patchfelder können Sie in entsprechenden Schränken hochkant montieren, womit Sie Bautiefe einsparen. Patchfelder sollten Sie ebenso vor Feuchtigkeit schützen. Nicht benutzte Anschlüsse verschließen Sie mit den vorhin erwähnten RJ45-Blindstopfen und schützen damit die Kontakte vor Verschmutzung.

10.3 Netzwerke mit Glasfaserkabeln

Für räumlich größere Netze, aber auch bei Neubauten empfehlen sich Glasfaserkabel. Vor dem Bau oder der Erweiterung Ihres Netzes müssen Sie aber für Ihre Planung auf einige Besonderheiten Rücksicht nehmen:

Sie können Glasfaserkabel zusammen mit Stromleitungen in einem Kanal, einer Kabelrinne oder einem Leerrohr gemeinsam verlegen (Abbildung 10.8). Sie brauchen keine Rücksicht auf einen möglichen elektrischen Potenzialunterschied zwischen zwei Gebäuden zu nehmen. Glasfaserkabel benötigen keinen Anschluss an den Potenzialausgleich eines Gebäudes. Für die Installationsarbeiten von Glasfasern benötigen Sie Spezialwerkzeuge. Für Messungen und die Fehlersuche an Glasfaserstrecken brauchen Sie (teure) Messgeräte. Sie können dadurch Kosten sparen, dass Sie vorkonfektionierte Kabel in räumlich kleineren Netzen verwenden. An diesen befinden sich bereits an beiden Enden die Steckverbinder. Dies können Sie nutzen, wenn Sie für die Leitungsführung vor allem Kabelrinnen und zu öffnende Kanäle verwenden. Sie müssen die Kabel dann nur über kurze Strecken durch Mauer- und Deckendurchbrüche ziehen. Wenn Sie Leerrohre verwenden, sollten diese innen eine glatte Oberfläche aufweisen. Bedenken Sie auch, dass Sie die Kabel mit einem Stecker oder Steckerpaar durch das Rohr ziehen und schieben müssen. Es darf hier also nicht zu eng werden, sonst wird das Kabel beim Einbringen beschädigt.

Sie können einen gemischten Betrieb mit herkömmlicher Kupferverkabelung einrichten. Dies können Sie vor allem bei Bestandsnetzen so handhaben. Aber auch für

schnelle Backbones zwischen Etagen-Switches oder Gebäuden können Sie die Glasfasern einsetzen. Die Versorgung der Arbeitsplätze geschieht dann wiederum über die Kupferverkabelung (Abbildung 10.3). Weitere Informationen finden Sie in Abschnitt 2.2, »Lichtwellenleiter, Kabel und Verbinder«.

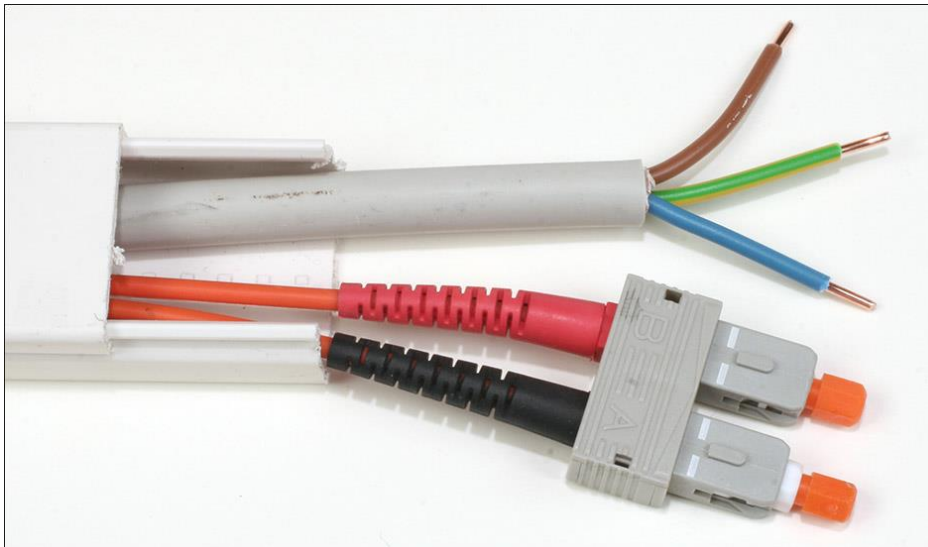


Abbildung 10.8 Gemeinsame Führung von Glasfaser- und Stromkabeln

10.3.1 Kabeltrassen für LWL-Kabel

Sie können Glasfaserkabel wie Kupferkabel auch durch Leerrohre, Kabelkanäle und Kabelrinnen führen:

Beachten Sie bei der Verlegung unbedingt die vom Hersteller angegebenen minimalen Biegeradien. Anders als ein Kupferkabel können Sie ein LWL-Kabel nicht »um die Ecke« verlegen. Sie müssen Platz für »runde« Führungen vorsehen. Auch Glasfaserkabel dürfen keiner Staunässe ausgesetzt werden. Für diese Zwecke gibt es aber speziell ummantelte Kabel.

Vermeiden Sie große mechanische Beanspruchungen Ihrer LWL-Kabel. Diese können besonders bei der gemeinsamen Führung mit Stromkabeln auftreten.

Bei längeren Strecken benötigen Sie Platz für die sichere und trockene Aufbewahrung der Spleißboxen. Dafür verwenden Sie abschließbare Unter- oder Aufputzschränke. Im Freien auf dem Werks- oder Campusgelände benutzen Sie entsprechende Verteilerkästen.

Im Gegensatz zu herkömmlichen Spleißmuffen, die Sie in Kabelschächten unterirdisch unterbringen, erreichen Sie hier die Kabel bei jeder Witterung. Stellen Sie den Kasten aber so auf, dass er nicht durch Fahrzeuge, Flurförderzeuge oder Lastkräne beschädigt werden kann. Eventuell bauen Sie einen entsprechend starken mechanischen Schutz auf. Wenn Sie Ihr Gelände nicht gegen den Zutritt Unbefugter schützen können, bringen Sie die Kästen so unauffällig und stark gesichert

wie nur möglich unter.

Auch Glasfaserkabel erhöhen die Brandlast!

10.3.2 Dosen und Patchfelder

Dosen und Patchfelder können Sie genauso anbringen, wie Sie es von der Kupfertechnik her gewohnt sind. Sichern Sie Aufputzkanäle und Dosen, wie für die Kupferkabel in Abschnitt 10.2.3, »Dosen und Patchfelder«, gezeigt wurde. Einige Besonderheiten müssen Sie wegen der andersartigen Betriebsgefahren beachten:

Sichern Sie ungenutzte LWL-Dosen und Steckplätze an Patchfeldern und Medienkonvertern so ab, dass niemand in die Öffnungen blicken kann (Unfallverhütung, Augenschutz). Die Schutzabdeckungen verhindern auch, dass Staub, Ölfilm und Feuchtigkeit die empfindliche Optik verschmutzen.

Bauen Sie das räumliche Umfeld von Patchfeldern und Medienkonverterleisten wegen nicht abzusehender Weiterentwicklungen großzügig auf.

Auch bei den Patchkabeln müssen Sie Biegeradien beachten. Sparen Sie deshalb nicht mit Halterungen, an denen die Kabel zugfrei geführt werden.

10.3.3 Medienkonverter

Für gemischte Netzwerke benötigen Sie Medienkonverter zur Signalumsetzung. Diese erhalten Sie in verschiedenen Bauformen:

- 19-Zoll-Einbau-Leiste oder -Feld (EDV-Raum, Stockwerksverteiler)
- Modul für Switches (Bauformen GBIC, SFP, XFP)
- Einzelgerät zur Montage in einer Wanddose, auf Hutschiene oder Aufputz
- Mini-Switch mit einem LWL-Anschluss
- Tischgerät mit einem Kupferanschluss

Bei Medienkonvertern handelt es sich um aktive Komponenten. Für diese müssen Sie einen Stromanschluss vorsehen. Verwenden Sie 19-Zoll-Felder im EDV-Raum, müssen Sie die eventuell entstehende Abwärme in Ihre Klimatisierungsberechnung mit einbeziehen. Ein Beispiel für ein Tischgerät finden Sie mit dem *Edimax ET-913MSC+*. Er setzt von 1000Base-T nach 1000Base-SX (Multimode) um. Er verfügt über einen RJ45- und einen SC-Duplex-Anschluss. LEDs für die Link-Kontrolle und Aktivität befinden sich an der Frontplatte. Sie können mehrere dieser Konverter im Rack ET-920MCR zusammenfassen und in Ihrem Netzwerkschrank im EDV-Raum unterbringen.

10.3.4 LWL-Multiplexer

Mittels LWL-Multiplexer verbinden Sie auch weiter auseinanderliegende Firmenstandorte. Die Glasfaserverbindung stellt Ihnen Ihr Telekommunikationsdienstleister zur Verfügung. Meist werden zwei oder vier Monomode-Fasern bereitgestellt. Sie können je Faserpaar einen herkömmlichen Medienkonverter für Monomode-Fasern anschließen. Sie schaffen damit eine Kopplung zum entfernten LAN mit 10 oder maximal 100 Mbit/s.

Wenn Sie einen LWL-Multiplexer zur Standortverbindung benutzen, erhöhen Sie die Verbindungsgeschwindigkeit enorm. Sie können dabei Übertragungsraten zwischen 1 Gbit/s und 10 Gbit/s nutzen.

Der Multiplexer teilt den Datenstrom auf mehrere Wellenlängen auf, die er gleichzeitig in eine Faser einspeist. Beim Empfänger werden die verschiedenfarbigen Signale wieder zu einem Datensignal zusammengesetzt. Eine weitere Variante filtert auf der Empfängerseite die einzelnen Farben aus und gibt diese zur weiteren Konvertierung (optisch/optisch oder optisch/elektrisch) weiter. Damit ist es Ihnen möglich, Port-Trunking zwischen zwei Switches über ein WAN zu benutzen. LWL-Multiplexer arbeiten mit verschiedenen Verfahren:

- WWDM, Wide Wavelength Division Multiplex
- CWDM, Coarse Wavelength Division Multiplex; Übertragungsraten bis 10 Gbit/s über 70 km ohne Repeater sind möglich.
- DWDM, Dense Wavelength Division Multiplex; Übertragungsraten von 10 bis 100 Gbit/s über 80–200 km werden erreicht.

LWL-Multiplexer dieser Art finden Sie unter anderem auf der Webseite [www. lambda-line.com/de](http://www.lambda-line.com/de) der Firma DeltaNet AG (Dietikon, Schweiz) dargestellt.

10.4 Geräte für Netzwerkverbindungen und -dienste

Bei der Kupferverkabelung haben Sie nach wie vor die RJ45-Steckverbindung als Standard. Hier können Sie hinsichtlich der Anschlusstechnik keine Fehler machen. Bei Glasfaserkomponenten müssen Sie immer auf die Anschlussnormen achten.

10.4.1 Netzwerkkarten

Neue PCs und Notebooks verfügen über eingebaute Netzwerkanschlüsse. Netzwerkkarten kaufen Sie im Reparaturfall und zur Aufrüstung.

Netzwerkkarten für PCs werden von allen gängigen Betriebssystemen unterstützt. Alle neueren Typen unterstützen Übertragungsraten bis 1 Gbit/s. Sie stellen sich aber auch automatisch auf 100 Mbit/s oder 10 Mbit/s ein. Weit verbreitet sind Netzwerkkarten

mit dem Chipsatz der Firma Realtek (Tabelle 10.1).

Chipsatz	10Base-T	100Base-TX	1000Base-T	Steckplatz
RTL8139	X	X	–	PCI
RTL8169	X	X	X	PCI
RTL8111	X	X	X	PCI-Express

Tabelle 10.1 Chipsätze der Firma Realtek

Für Ihren Server verwenden Sie spezielle Netzwerkkarten. Diese sind für den harten Dauergebrauch ausgelegt. Einige Modelle benötigen einen PCI-EXPRESS-x8-Einbauplatz. Dafür bekommen Sie 10 Gbit/s Übertragungsrate für LWL (*Ethernet Server Adapter X520-SR2* der Firma Intel, 2 × LC-Anschluss, Multimode). LWL-Netzwerkkarten für Büro-PCs sind eher selten im Einsatz (z. B. *Allied Telesis AT 2916SX/SC*, SC-Duplex, 1000Base-SR, Multimode, PCI-Steckplatz).

Der Handel bietet ferner sogenannte *USB-Netzwerkkarten* an. Technisch gesehen sind diese Adaptergeräte. Mit ihnen können Sie Rechner über den USB-Anschluss an Ihr Netzwerk anbinden.

10.4.2 WLAN-Router und -Sticks

In Privathaushalten finden Sie oft WLAN-Router vor, mit denen die Verbindung zum Internet hergestellt wird. Oftmals werden diese Geräte nicht über den Handel, sondern über den Telekommunikationsdienstleister bezogen. Einige dieser Geräte verfügen über einen zusätzlichen USB-Anschluss. Über den stecken Sie ein UMTS- oder LTE-USB-Funkmodem

an. Fällt die DSL-Verbindung aus, arbeiten Sie drahtlos weiter. Auch in Gegenden mit keiner oder sehr schlechter DSL-Anbindung stellen solche Geräte den Internetanschluss her.

Allgemein finden Sie bei diesen Geräten meist eine Firewall, einen DHCP-Server, PAT/NAT und manchmal sogar einen VPN-Client vor.

Der Router WL0082 aus dem Hause LogiLink (Abbildung 10.9) eignet sich wegen seiner Größe für den Außendienst- oder Hotelzimmereinsatz. Ihr Notebook verbinden Sie dabei per LAN-Kabel mit dem Mini-Router. An diesem steckt Ihr Funkmodem. Damit bauen Sie eine eigene Internetverbindung unabhängig von der Netzinfrastruktur des Hotels auf. Sie können damit unkompliziert VPN- oder SSH-Tunnelverbindungen betreiben. Den Mini-Router können Sie auch noch als WLAN-Accesspoint einsetzen.



Abbildung 10.9 WL0082 von LogiLink

Die WLAN-Funktechnik finden Sie praktisch in allen mobilen Rechnern. Wenn diese defekt geworden ist, benötigen Sie einen USB-WLAN-Stick als Ersatz. Mithilfe dieser Sticks können Sie auch PCs mit dem WLAN verbinden.

10.4.3 Router

Mit einem Router verbinden Sie Netze. Die notwendigen Geräte erhalten Sie in unterschiedlicher Leistungsfähigkeit und Softwareausstattung. Modelle mit hohem Datendurchsatz verfügen über mehrere Netzwerkschnittstellen und extra ausgeführte Wartungsanschlüsse. Einige dieser Hochleistungsrouter können Sie über eine eigene Backbone-Verbindung auch zu einem einzigen logischen Gerät vereinen. Achten Sie beim Einsatz dieser Geräte auf den Anschluss über eine unterbrechungsfreie Stromversorgung und auf die anfallende Abwärme, besonders beim Einbau in 19-Zoll-Schränke. Derartige hochprofessionelle Geräte werden unter anderem von Cisco oder HP gefertigt.

Während Hochleistungsrouter sich oft ausschließlich der Aufgabe des Datentransports widmen, übernehmen die Kompaktgeräte in kleineren Firmen, Praxen und Privathaushalten weitere Aufgaben: NAT/PAT, Firewall, VPN-Client, Proxy- oder DHCP-Server. In viele dieser Geräte ist neben den üblichen Netzwerkanschlüssen auch WLAN, gegebenenfalls ein DSL- oder Kabel-Modem, integriert, sodass man mit einem Gerät alle Bedürfnisse abdeckt.

Ein sehr verbreitetes Modell dieser Geräteklasse ist der *Linksys WRT54GL* (Abbildung 10.10 und Abbildung 10.11).

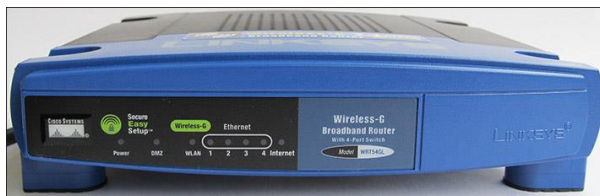


Abbildung 10.10 Linksys WRT54GL, Frontseite



Abbildung 10.11 Linksys WRT54GL, Anschlussseite

Dieser Router verwendet ein Linux-basiertes System (das durch das freie OpenWRT ersetzt werden kann). Falls Sie den Router ohne den Einsatz der mitgelieferten Setup-CD konfigurieren möchten, finden Sie in Tabelle 10.2 die notwendigen Daten für den ersten Zugriff.

IP-Adresse	192.168.1.1
Benutzername	(ohne)
Kennwort	admin

Tabelle 10.2 Zugriffsdaten für den Linksys WRT54GL

Falls Ihr lokales Netz nicht die Adresse 192.168.1.0 aufweist, müssen Sie wenigstens einen PC mit einer Adresse aus diesem Netz versehen, z. B. 192.168.1.20. Diese Adresse wird kaum von Routern mit DHCP-Dienst verwaltet, sodass ihre Verwendung eher nicht zu Problemen führen dürfte. In Microsoft Windows finden Sie diesen Punkt in der Systemsteuerung, unter Linux reicht (als Benutzer `root`, für die erste Netzwerkkarte) der Aufruf:

```
ip addr add 192.168.1.20/24 dev eth0
```

Laden Sie auf diesen PC gleich die aktuelle Firmware von der Herstellerseite <http://https://www.linksys.com/de/support-product?pid=01t80000003K7hCAAS> herunter. Sie wird im Anschluss aufgespielt.

Verbinden Sie sich per Webbrowser nun mit dem Router, indem Sie dessen Adresse 192.168.1.1 eingeben.

Wechseln Sie in das Menü Administration, und darin wählen Sie Firmware Upgrade. Klicken Sie auf Durchsuchen, und wählen Sie die neue Firmwaredatei aus. Abbildung 10.12 zeigt den Upgrade-Vorgang.



Abbildung 10.12 Firmware-Upgrade für den Linksys WRT54GL

Nach dem Upgrade starten Sie den Router nochmals neu und verbinden sich wieder mit dem Gerät.

Nach dem Aufruf landen Sie in der Maske, in der Sie Ihren DSL-Internetzugang und die Zeitzone einrichten können (Abbildung 10.13). Die DHCP-Einstellungen dürften für die meisten Anwendungsfälle unverändert verwendbar sein.

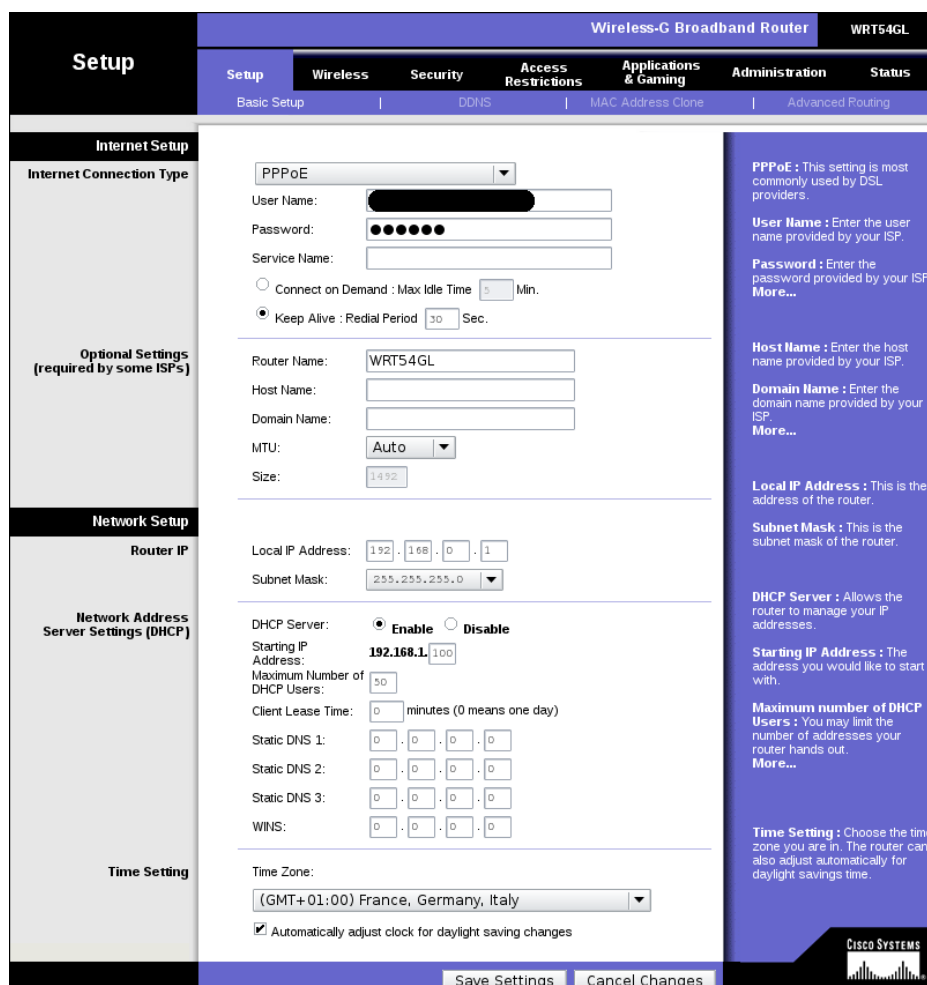


Abbildung 10.13 Einstellungen für Internetzugang und Zeitzone

Im folgenden Schritt sorgen Sie für sicherere Einstellungen bezüglich des Konfigurationszugangs (Administration • Management, siehe Abbildung 10.14). Ändern Sie in jedem Fall das Kennwort ab, und lassen Sie ausschließlich kabelgebundenen Zugang per HTTPS für die Weboberfläche zu. Stellen Sie auch die Möglichkeit des Remote-Managements und von UPnP ab.

Abbildung 10.14 Einrichtung des Konfigurationszugangs

Die weiteren Schritte, wie gegebenenfalls die Einrichtung eines WLANs, Zugriffbeschränkungen und weitere Verfeinerungen, nehmen Sie im Anschluss daran vor. Vergessen Sie nicht, Ihre Einstellungen zu sichern. Dazu gehen Sie zu Administration • Config Management und klicken auf Backup (Abbildung 10.15).

Abbildung 10.15 Sichern der Einstellungen

Sie können diesen Kleinrouter auch zum Verbinden zweier Netze verwenden. Im Beispiel aus Abbildung 10.16 soll das Netz 192.168.1.0 mit 192.168.0.0 kommunizieren. Anstelle der vorhin gezeigten Internetverbindung wählen Sie hier Static IP und geben die Adresse des Routers im Zielnetz ein. Vergessen Sie den DNS-Eintrag nicht. Im Beispiel sehen Sie den Router des übergeordneten Netzes 192.168.0.1.

LINKSYS[®] by Cisco Firmware Version : v4.30.16

Wireless-G Broadband Router WRT54GL

Setup

Setup | Wireless | Security | Access Restrictions | Applications & Gaming | Administration | Status

Basic Setup | DDNS | MAC Address Clone | Advanced Routing

Language: English

Select your language

Internet Setup

Internet Connection Type: Static IP

Internet IP Address: 192 . 168 . 0 . 4

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 0 . 1

Static DNS 1: 192 . 168 . 0 . 1

Static DNS 2: 0 . 0 . 0 . 0

Static DNS 3: 0 . 0 . 0 . 0

Optional Settings (required by some ISPs)

Router Name: WRT54GL

Host Name: schule

Domain Name:

MTU: Auto

Size: 1500

Network Setup

Router IP

Local IP Address: 192 . 168 . 1 . 1

Subnet Mask: 255.255.255.0

Network Address Server Settings (DHCP)

DHCP Server: ☒ Enable ☐ Disable

Starting IP Address: 192.168.1.100

Maximum Number of DHCP Users: 50

IP Address Range: 192.168.1.100 to 149

Client Lease Time: 0 minutes (0 means one day)

WINS: 0 . 0 . 0 . 0

Time Setting

Time Zone: (GMT+01:00) France, Germany, Italy

☒ Automatically adjust clock for daylight saving changes

Save Settings Cancel Changes

Static IP : This setting is most commonly used by Business class ISP.

Internet IP Address : Enter the IP address provided by your ISP.

Subnet Mask : Enter your subnet mask. More...

Host Name : Enter the host name provided by your ISP.

Domain Name : Enter the domain name provided by your ISP. More...

Local IP Address : This is the address of the router.

Subnet Mask : This is the subnet mask of the router.

DHCP Server : Allows the router to manage your IP addresses.

Starting IP Address : The address you would like to start with. More...

Time Setting : Choose the time zone you are in. The router can also adjust automatically for daylight savings time.

Abbildung 10.16 Verbindung zweier Netze

Auf dem WRT54GL und weiteren verschiedenen Routern und Kleinrechnern können Sie OpenWRT (www.openwrt.org) anstelle von proprietärer Firmware nutzen. Das Linuxbasierte System verleiht den meisten Geräten zusätzliche Eigenschaften, wie z. B. die Fähigkeiten eines VPN-Clients, und zumindest oftmals schnellere Sicherheits-Updates. Wenn Sie den Wunsch haben, es einzusetzen, sehen Sie auf der Webseite nach, ob Ihr Routermodell unterstützt wird. Ältere Konstruktionen wie der Linksys WRT54GL können wegen Speichermangel nicht die neuesten Entwicklungen nutzen. Diese laufen aber in jedem Fall auf diversen Kleinrechnern (z. B. dem Raspberry Pi). Speziell für den Linksys WRT54GL werden im Internet Anleitungen zur Speicheraufrüstung gezeigt. Wenn Sie sich zutrauen, SMD-ICs aus- und einzulöten, erhalten Sie eine deutlich leistungsfähigere Hardware. Informieren Sie sich unter <http://wiki.openwrt.org/toh/linksys/wrt54g>.

Besonders beim Linksys WRT54GL ist die Hardwareversion wichtig. Sie finden die notwendige Angabe auf der Unterseite des Geräts beim Barcode-Aufkleber von Seriennummer und MAC-Adresse (hier: v1.1).

Laden Sie sich von <http://downloads.openwrt.org/backfire/10.03.1/brcm-2.4/> die Datei *openwrt-wrt54g-squashfs.bin* herunter. Melden Sie sich am Router an, und führen Sie ein Upgrade mit der neuen »Firmware« wie in Abbildung 10.12 gezeigt durch. Nach erfolgreichem Upload startet der Router neu. Dieser Vorgang kann bis zu zwei Minuten dauern. Das Gerät ist anschließend per telnet unter der Adresse 192.168.1.1 erreichbar. Geben Sie auf einer Linux/Unix-Shell oder im CMD-Fenster von Microsoft Windows

telnet 192.168.1.1 ein. Führen Sie als Erstes `passwd` (Vergabe eines sicheren Kennworts) aus. Beenden Sie die Sitzung mit `reboot`. Nach dem erneuten Start ist das Gerät nicht mehr per telnet erreichbar, sondern über ssh. Microsoft Windows-Benutzer benötigen `putty`, um per SSH eine Verbindung zur weiteren Konfiguration aufzubauen. Anwender von Linux, FreeBSD und Verwandte verbinden sich per Shell wieder mit dem Router: `ssh root@192.168.1.1`. Eine Sitzung wird stets mit `exit` beendet, außer Sie weisen einen Systemneustart an.

Die Entwickler von OpenWRT empfehlen, für eine »Notbetankung« per `tftp` folgende Einstellungen zu setzen und anschließend den Router neu zu starten:

```
nvrnm set boot_wait=on
nvrnm set boot_time=10
nvrnm commit && reboot
```

Melden Sie sich wieder an, und installieren Sie das deutsche Sprachpaket für die Weboberfläche:

```
opkg update && opkg install luci-i18n-german
```

Falls Sie per Shell am Router einen Internetzugang einrichten möchten, funktioniert dies so:

```
uci set network.wan.proto=pppoe
uci set network.wan.username='BENUTZERKENNUNG'
uci set network.wan.password='KENNWORT'
uci commit network
ifup wan
```

Als Paketsystem verwendet OpenWRT `opkg`, eine Abwandlung von Debians `dpkg`. In Tabelle 10.3 finden Sie die wichtigsten Aktionen der Softwareverwaltung aufgelistet.

Aktion	Kommando
Liste verfügbarer Pakete auf neuen Stand bringen	<code>opkg update</code>
Paket installieren	<code>opkg install PAKETNAME</code>
Installiertes Paket durch neuere Version ersetzen	<code>opkg upgrade PAKETNAME</code>
Installiertes Paket löschen	<code>opkg remove PAKETNAME</code>
Liste verfügbarer Pakete	<code>opkg list</code>
Liste von installierten Paketen, für die es neuere Versionen gibt	<code>opkg list-upgradable</code>
Liste installierter Pakete	<code>opkg list-installed</code>

Tabelle 10.3 Wichtige »opkg«-Kommandos

Übersichtlicher geschieht die Konfiguration des OpenWRT-Routers über die Weboberfläche. Rufen Sie in Ihrem Webbrowser einfach die Adresse 192.168.1.1 auf. Sie werden dann von der Statusseite begrüßt. Als dieser Screenshot erstellt wurde, war der Zugriff auf einen Zeitserver noch nicht konfiguriert, weshalb die Ortszeit noch in der Vergangenheit liegt (Abbildung 10.17) und die Oberfläche in englischer Sprache erscheint.

Nach einem Neustart (System • reboot) erhalten Sie die deutschsprachige Oberfläche.

Konfigurieren Sie jetzt das Netzwerk. Dazu klicken Sie auf Netzwerk und erhalten eine Übersicht (Abbildung 10.18) über die aktiven Schnittstellen. Sie erreichen das jeweilige Einstellmenü entweder über die obere Leiste (hier: WAN und LAN) bzw. über die Schaltfläche Bearbeiten in der rechten Hälfte des Bildes. Sie sehen in dieser Übersicht nur die aktiven Schnittstellen (WLAN war bereits vorher abgeschaltet).

OpenWrt | OpenWrt Backfire 10.03.1 | Load: 0.49 0.20 0.07 | Auto Refresh: **on** | Changes:

Status

System

Router Name	OpenWrt
Router Model	Linksys WRT54G/GS/GL
Firmware Version	OpenWrt Backfire 10.03.1 / LuCI 0.10.0 Release (0.10.0)
Kernel Version	2.4.37.9
Local Time	Thu Sep 8 17:04:12 2011
Uptime	1h 5m 24s
Load Average	0.64, 0.25, 0.08

Memory

Total Available	6952 kB / 14316 kB (48%)
Free	736 kB / 14316 kB (5%)
Cached	4644 kB / 14316 kB (32%)
Buffered	1572 kB / 14316 kB (10%)

Network

IPv4 WAN Status: Not connected

Active Connections: 0 / 4096 (0%)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
There are no active leases.			

Wireless

Generic 802.11bg Wireless Controller (wif0)

SSID: [OpenWrt](#)

Mode: Client

Channel: 0 (0.00 GHz)

Bitrate: 54 Mb/s

Wireless is disabled or not associated

Associated Stations

MAC-Address	Network	Signal	Noise
No information available			

Abbildung 10.17 Statusseite bei erstmaligem Aufruf

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 0.17 0.25 0.12 | Auto Refresh: **on** | Änderungen: 0

Netzwerk

Schnittstellen

Schnittstellenübersicht

Netzwerk	Status	Aktionen
LAN br-lan	Laufzeit: 12h 33m 19s MAC-Adresse: C8:B3:73:41:8E:10 RX: 12.23 MB (136616 Pkte.) TX: 167.12 MB (143095 Pkte.) IPv4: 192.168.0.1/24	Verbinden Stoppen Bearbeiten Löschen
WAN pppoe-wan	Laufzeit: 12h 33m 10s RX: 163.91 MB (137544 Pkte.) TX: 10.67 MB (107526 Pkte.) IPv4: 217.237.62.229/32	Verbinden Stoppen Bearbeiten Löschen

[Neue Schnittstelle hinzufügen...](#)

Abbildung 10.18 Übersicht über die Netzwerkschnittstellen

Konfigurieren Sie zunächst die Schnittstelle LAN (Abbildung 10.19). Hier vergeben Sie normalerweise eine feste IP-Adresse (Static address). Geben Sie wenigstens die IP-Adresse und die Netzmaske ein. Im unteren Bereich der Einstellmöglichkeiten finden Sie Eintragungen zum DHCP.

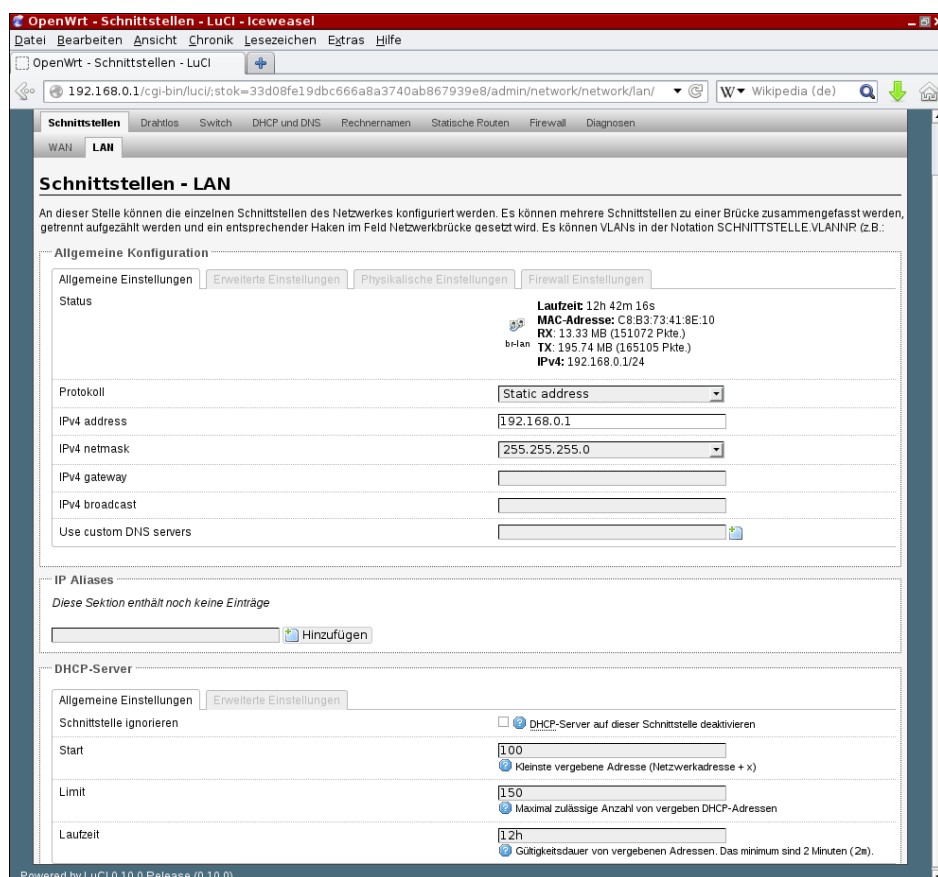


Abbildung 10.19 Konfiguration der LAN-Schnittstelle des Routers

Unter Erweiterte Einstellungen können Sie unter anderem die MAC-Adresse und die MTU ändern. Bei Physikalische Einstellungen können Sie Schnittstellen VLANs zuordnen und gegebenenfalls das Spanning-Tree-Protokoll aktivieren. In den Firewall Einstellungen bestimmen Sie, zu welcher Zone die gerade bearbeitete Schnittstelle gehören soll (Abbildung 10.20).

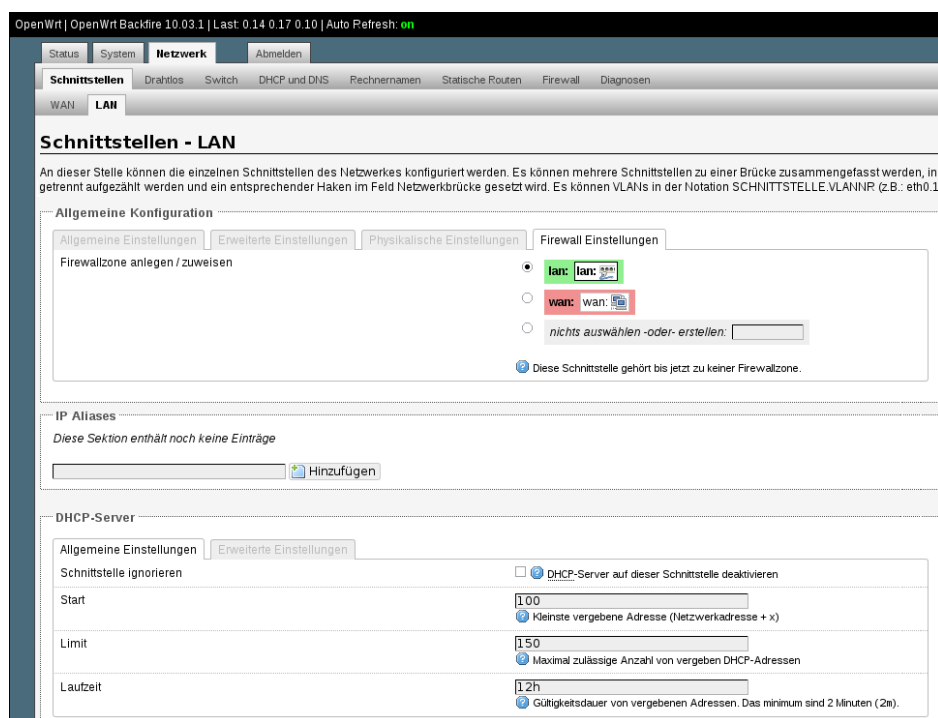


Abbildung 10.20 Zuordnung der Schnittstelle zu einer Firewall-Zone

Widmen Sie sich nun der WAN-Anbindung (Abbildung 10.21). Wählen Sie das zutreffende

Protokoll, und geben Sie Ihre Zugangsdaten ein.

OpenWrt | OpenWrt Backfire 10.03.1 | Last 1.15 1.02 0.65 | Auto Refresh: on

Status System **Netzwerk** Abmelden

Schnittstellen Drahtlos Switch DHCP und DNS Rechnernamen Statische Routen Firewall Diagnosen

WAN LAN

Schnittstellen - WAN

An dieser Stelle können die einzelnen Schnittstellen des Netzwerkes konfiguriert werden. Es können mehrere Schnittstellen zu einer Brücke zusammengefasst werden, getrennt aufgezählt werden und ein entsprechender Haken im Feld Netzwerkbrücke gesetzt wird. Es können VLANs in der Notation SCHNITTSTELLE.VLANNR (z.B.: eth0.1) verwendet werden.

Allgemeine Konfiguration

Allgemeine Einstellungen **Erweiterte Einstellungen** Physikalische Einstellungen Firewall Einstellungen

Status

Laufzeit 12h 52m 31s
RX: 205.83 MB (169923 Pkte.)
TX: 12.55 MB (129416 Pkte.)
IPv4: 217.237.62.229/32

pppoe-wan

Protokoll **PPPoE**

PAP/CHAP username

PAP/CHAP password

Access Concentrator **auto**
[Leave empty to autodetect](#)

Service Name **auto**
[Leave empty to autodetect](#)

IP Aliases

Diese Sektion enthält noch keine Einträge

[Hinzufügen](#)

Abbildung 10.21 Einrichtung des Internetzugangs

Im Menü Erweiterte Einstellungen können Sie eigene Einstellungen für das Default Gateway, den vom Provider angebotenen DNS-Server, LCP und für die Verbindungsdauer vornehmen. Bei Physikalische Einstellungen setzen Sie gegebenenfalls den Punkt bei der zutreffenden VLAN-Schnittstelle. In den Firewall Einstellungen setzen Sie die Zone WAN (Abbildung 10.22).

OpenWrt | OpenWrt Backfire 10.03.1 | Last 1.15 1.02 0.65 | Auto Refresh: on

Status System **Netzwerk** Abmelden

Schnittstellen Drahtlos Switch DHCP und DNS Rechnernamen Statische Routen Firewall Diagnosen

WAN LAN

Schnittstellen - WAN

An dieser Stelle können die einzelnen Schnittstellen des Netzwerkes konfiguriert werden. Es können mehrere Schnittstellen zu einer Brücke zusammengefasst werden, indem diese durch Leerzeichen getrennt aufgezählt werden und ein entsprechender Haken im Feld Netzwerkbrücke gesetzt wird. Es können VLANs in der Notation SCHNITTSTELLE.VLANNR (z.B.: eth0.1) verwendet werden.

Allgemeine Konfiguration

Allgemeine Einstellungen **Erweiterte Einstellungen** Physikalische Einstellungen Firewall Einstellungen

Firewallzone anlegen / zuweisen

☐ lan: lan

☒ wan: wan

☐ nichts auswählen -oder- erstellen:

[? Diese Schnittstelle gehört bis jetzt zu keiner Firewallzone.](#)

IP Aliases

Diese Sektion enthält noch keine Einträge

[Hinzufügen](#)

[Zurücksetzen](#) [Speichern](#) [Speichern & Anwenden](#)

Abbildung 10.22 Zuordnung der Schnittstelle zu einer Firewall-Zone

Unter Drahtlos konfigurieren Sie, falls notwendig, das WLAN (Abbildung 10.23). Sie können das WLAN in dieser Maske aktivieren bzw. deaktivieren sowie den Kanal und die Sendeleistung festlegen. In Erweiterte Einstellungen legen Sie den Betriebsmodus und weitere technische Parameter fest (Abbildung 10.24).

Jeweils im unteren Bereich der WLAN-Konfiguration legen Sie die ESSID, den Betriebsmodus und die Zugehörigkeit zu einem Netzwerk (lan/wan) fest. Ein eigener Unterpunkt (WLAN-Verschlüsselung) ermöglicht es Ihnen, die hierzu notwendigen Festlegungen zu treffen. Unter Erweiterte Einstellungen im unteren Menübereich können Sie noch weitere Verfeinerungen einstellen. Im Menü Netzwerk • Switch können Sie (weitere) VLANs konfigurieren.

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 1.23 0.98 0.84 | Auto Refresh: **on**

Status System **Netzwerk** Abmelden

Schnittstellen **Drahtlos** Switch DHCP und DNS Rechnernamen Statische Routen Firewall Diagnosen

wl0: Master "schule"

Drahtlosnetzwerk: Master "schule" (wl0)

Die *Gerätekonfiguration* deckt physikalische Einstellungen der WLAN-Hardware wie Kanal, Sendestärke oder Antennenauswahl ab. Diese Einstellungen werden von allen Netzwerken auf dem Gerät geteilt. Netzwerkspezifische Einstellungen wie Verschlüsselung oder Betriebsmodus sind in der *Schnittstellenkonfiguration* gruppiert.

Gerätekonfiguration

Allgemeine Einstellungen **Erweiterte Einstellungen**

Status SSID: schule | Modus: Master
100% WLAN ist deaktiviert oder nicht assoziiert

Das WLAN-Netzwerk ist deaktiviert **Aktivieren**

Kanal 11 (2.462 GHz)

Sendeleistung 18 dBm (63 mW)

Schnittstellenkonfiguration

Allgemeine Einstellungen **WLAN-Verschlüsselung** **Erweiterte Einstellungen**

ESSID schule

Modus Access Point

Netzwerk

☐ lan:

☐ wan:

☒ nichts auswählen -oder- erstellen:

Wählt die Schnittstelle die diesem Netzwerk zugeordnet wird.

ESSID verstecken ☐

Abbildung 10.23 Festlegen technischer Parameter für das WLAN

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 1.23 0.98 0.84 | Auto Refresh: **on** Änderungen:

Status System **Netzwerk** Abmelden

Schnittstellen **Drahtlos** Switch DHCP und DNS Rechnernamen Statische Routen Firewall Diagnosen

wl0: Master "schule"

Drahtlosnetzwerk: Master "schule" (wl0)

Die *Gerätekonfiguration* deckt physikalische Einstellungen der WLAN-Hardware wie Kanal, Sendestärke oder Antennenauswahl ab. Diese Einstellungen werden von allen Netzwerken auf dem Gerät geteilt. Netzwerkspezifische Einstellungen wie Verschlüsselung oder Betriebsmodus sind in der *Schnittstellenkonfiguration* gruppiert.

Gerätekonfiguration

Allgemeine Einstellungen **Erweiterte Einstellungen**

Modus 802.11b+g

Sendeanenne

☒ auto

☐ Antenne 1

☐ Antenne 2

Empfangsantenne

☒ auto

☐ Antenne 1

☐ Antenne 2

Frame Bursting ☐

Distanzoptimierung

Ländercode

Verbindungslimit

Schnittstellenkonfiguration

Allgemeine Einstellungen **WLAN-Verschlüsselung** **Erweiterte Einstellungen**

ESSID schule

Modus Access Point

Netzwerk

☐ lan:

☐ wan:

☒ nichts auswählen -oder- erstellen:

Wählt die Schnittstelle die diesem Netzwerk zugeordnet wird.

ESSID verstecken ☐

Abbildung 10.24 Erweiterte Einstellungen für das WLAN

Einstellungen zu DHCP und DNS nehmen Sie im gleichnamigen Menü Allgemeine Einstellungen vor (Abbildung 10.25). Die weiteren Punkte ermöglichen unter anderem die Verwendung einer eigenen *resolv.conf*- und *hosts*-Datei, den Betrieb eines TFTP-Servers und weiterer Einstellungen für den DNS- und DHCP-Server. Die Host-Einträge nehmen Sie dabei unter Netzwerk • Rechnernamen vor. Statische Routen tragen Sie im gleichnamigen Punkt ein, wobei das Ziel ein einzelner Rechner oder ein Netzwerk sein kann.

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 0.02 0.14 0.43 | Auto Refresh: **on** Änderungen:

Status System **Netzwerk** Abmelden

Schnittstellen Drahtlos Switch **DHCP und DNS** Rechnernamen Statische Routen Firewall Diagnosen

DHCP und DNS

Dnsmasq ist ein kombinierter DHCP-Server und DNS-Forwarder für NAT Router

Servereinstellungen

Allgemeine Einstellungen **Resolve- und Hosts-Dateien** TFTP Einstellungen Erweiterte Einstellungen

Anfragen nur mit Domain ☒ [Anfragen ohne Domainnamen nicht weiterleiten](#)

Authoritativ ☒ [Dies ist der einzige DHCP im lokalen Netz](#)

Lokaler Server [Spezifiziert den lokalen Domainnamen. Anfragen für Hostnamen welche auf diese Domain zutreffen werden nie weitergeleitet und ausschließlich aus DHCP-Namen oder Hosts-Dateien aufgelöst](#)

Lokale Domain [Lokaler Domain-Suffix welcher an DHCP Namen und Host-Datei Einträge angehängen wird](#)

Schreibe Abfrageprotokoll ☐ [Empfangene DNS-Anfragen in das Systemprotokoll schreiben](#)

DNS-Weiterleitungen [Liste von DNS-Servern an welche Requests weitergeleitet werden](#)

DNS-Rebind-Schutz ☒ [Eingehende RFC1918-Antworten verwerfen](#)

Erlaube localhost ☒ [Dies erlaubt DNS-Antworten im 127.0.0.0/8 Bereich der z.B. für RBL Dienste genutzt wird](#)

Domain-Whitelist [Liste von Domains für welche RFC1918-Antworten erlaubt sind](#)

Aktive Zuweisungen

Hostname	IPv4-Adresse	MAC-Adresse	Verbleibende Gültigkeit
Es gibt z.Z. keine aktiven Leases.			

Statische Einträge

Statische Leases werden genutzt um feste IP-Adressen und Hostnames zu DHCP-Clients zuzuordnen. Sie werden auch für nicht-dynamische Schnittstellen-Konfigurationen benötigt auf denen lediglich Hosts mit zugehörigem statischem Lease-Eintrag bedient werden. Die **Hinzufügen** Schaltfläche fügt einen neuen Lease-Eintrag hinzu. Die **MAC-Adresse** identifiziert den Host, die **IPv4-Adresse** definiert die zu nutzende statische Adresse und der **Hostname** ist der symbolische Name dem dem Host zugewiesen wird.

Hostname	MAC-Adresse	IPv4-Adresse
Diese Sektion enthält noch keine Einträge		

Zurücksetzen Speichern Speichern & Anwenden

Abbildung 10.25 Einstellungen zu DHCP und DNS
Firewall-Einstellungen und -Regeln geben Sie unter

Netzwerk • Firewall ein (Abbildung 10.26). Hier können Sie auch Port-Weiterleitungen definieren. Hierzu klicken Sie im Bereich Weiterleitungen auf Hinzufügen. In der nun verfügbaren Maske (Abbildung 10.27) wird als Beispiel ein Webserver »durchgereicht«.

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 0.16 0.04 0.19 Ungespeicherte Änderungen

Status System **Netzwerk** Abmelden

Schnittstellen Drahtlos Switch DHCP und DNS Rechnernamen Statische Routen **Firewall** Diagnosen

Firewall

Die Firewall erstellt Netzwerkzonen über bestimmte Netzwerkschnittstellen um den Netzwerkverkehr zu trennen.

Allgemeine Einstellungen Benutzerdefinierte Regeln

Schutz vor SYN-flood-Attacken ☒

Ungültige Pakete verwerfen ☒

Eingang

Ausgang

Weitergeleitet

Zonen

Zone	Eingang	Ausgang	Weitergeleitet	NAT aktivieren	MSS Korrektur
lan: lan:	annehmen	annehmen	zurückweisen	☐	☐
wan: wan:	zurückweisen	annehmen	zurückweisen	☒	☒

Hinzufügen

Weiterleitungen

Name	Protokoll	Quelle	Über	Ziel	Aktion	Sortieren
Diese Sektion enthält noch keine Einträge						

Hinzufügen

Regeln

Name	Adressfamilie	Protokoll	Quelle	Ziel	Aktion	Sortieren
-	nur IPv4	UDP	wan:0.0.0.0/*	Gerät:0.0.0.0:68	ACCEPT	
-	nur IPv4	ICMP (echo-request)	wan:0.0.0.0/*	Gerät:0.0.0.0/*	ACCEPT	
-	nur IPv6	UDP	wan:fe80::/10:547	Gerät:fe80::/10:546	ACCEPT	
-	nur IPv6	ICMP (echo-request)	wan:0.0.0.0/*	Gerät:0.0.0.0/*	ACCEPT	
-	nur IPv6	ICMP (echo-request)	wan:0.0.0.0/*	*0.0.0.0/*	ACCEPT	

Hinzufügen

Abbildung 10.26 Firewall-Einstellungen

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 0.13 0.06 0.08 Ungespeicherte Änderungen

Status System **Netzwerk** Abmelden

Schnittstellen Drahtlos Switch DHCP und DNS Rechnernamen Statische Routen **Firewall** Diagnosen

Umleitungen

Umleitungen erlauben es das Ziel von weitergeleiteten Paketen zu verändern.

Allgemeine Einstellungen Erweiterte Einstellungen

Name

Quell-Zone ☐ lan: lan: ☐ newzone: (leer) ☒ wan: wan:

Protokoll

Externer Port Eingehende Verbindungen filtern welche an den angegebenen Port oder Portbereich auf dem lokalen Gerät gerichtet sind

Interne IP-Adresse Gefilterte Verbindungen an den angegeben internen Host weiterleiten

Interner Port (optional) Gefilterte Verbindungen an den angegeben Port auf dem internen Host weiterleiten

Abbildung 10.27 Port-Weiterleitung für Webserver einstellen

Über die Weboberfläche können Sie leicht kontrollieren, ob die WAN- und zum Teil auch die LAN-Anbindung des Routers funktioniert. Unter Netzwerk • Diagnosen stehen die Werkzeuge ping, traceroute und nslookup bereit.

Schränken Sie den Netzwerkzugriff auf den Router ein (System • Administration), und lassen Sie als Administrationszugang nur das LAN zu (Abbildung 10.28). In diesem Menü können Sie auch das Admin-Kennwort ändern. Für den SSH-Zugang können Sie zudem noch einen abweichenden Port verwenden.

OpenWrt | OpenWrt Backfire 10.03.1 | Last: 0.10 0.17 0.12 Ungespeicherte Änderungen

Status **System** Netzwerk Abmelden

System **Administration** Paketverwaltung Systemstart Geplante Aufgaben Backup / Flash Firmware Neu Starten

Routerpasswort

Ändert das Administratorpasswort für den Zugriff auf dieses Gerät

Passwort

Bestätigung

SSH-Zugriff

Der SSH-Server ermöglicht Shell-Zugriff über das Netzwerk und bietet einen integrierten SCP-Dienst.

Dropbear Instanz Löschen

Schnittstelle ☒ lan: ☐ wan: ☐ unspezifiziert

☒ Nur auf die gegebene Schnittstelle reagieren, nutze alle wenn nicht spezifiziert

Port Gibt den Server-Port dieser Dropbear-Instanz an

Passwortanmeldung ☒ Erlaube Anmeldung per Passwort

"root" Login mit Passwort aktivieren ☒ Erlaubt es dem rootBenutzer sich mit einem Passwort statt einem Zertifikat einzuloggen

Gateway-Ports ☐ Entfernten Hosts erlauben zu lokale SSH-Tunnel-Ports zu verbinden

SSH-Schlüssel

Hier können öffentliche SSH-Schlüssel reinkopiert werden (einer pro Zeile).

Abbildung 10.28 Administrationskennwort und Netzwerkzugriff einstellen

Unter System • Backup/Flash Firmware sichern Sie die Einstellungen (Generate archive) oder laden sie nach dem Rücksetzen (Upload archive). Das Rücksetzen nehmen Sie mit Perform reset vor. Sollten Sie eine neue »Firmware« einspielen wollen, können Sie dies hier (Flash Image) vornehmen.

Als einfachen Router können Sie auch einen Kleinrechner wie den Raspberry Pi oder Banana Pi einsetzen. Gegenüber »richtigen« Routergeräten fehlen Switch und ein zweiter Netzwerkanschluss. Den stellen Sie mittels eines USB-LAN-Adapters (Abbildung 10.29) her. Die CPU- und Speicherausstattung ist besser als die der meisten Routergeräte. Dagegen sind die Kleinrechner nicht auf einen schnellen Datendurchsatz hin optimiert. Mittlerweile liegt vom Raspberry Pi die dritte Modellreihe vor. Die nur scheckkartengroßen Minirechner haben mittlerweile an Rechenleistung deutlich hinzugewonnen. Außerdem finden Sie in den Geräten Banana Pi, Cubieboard und Co. ebenso geeignete Hardware.



Abbildung 10.29 USB-LAN-Adapter für die WAN-Schnittstelle

Die Kleinrechner im Routereinsatz bieten einen zusätzlichen Sicherheitsaspekt. Falls Sie jeden administrativen Zugriff über das Netzwerk, egal, ob vom LAN oder WAN, unterbinden möchten, können Sie die lokale Konsole nutzen. Nur wer den körperlichen Zugriff auf das Gerät erhält, kann auch Eingriffe in die Konfiguration vornehmen.

Das praktische Vorgehen sehen Sie anhand eines Raspberry Pi 2 Model B. Lesen Sie sich vor den ersten Arbeitsschritten die Ausführung unter www.openwrt.org zum entsprechenden Gerät durch.

Bei der Überarbeitung dieses Buches war die Version 15.05.1, »Chaos Calmer« aktuell. Für das hier verwendete Gerät laden Sie das Installationsabbild der Micro-SD-Karte unter https://downloads.openwrt.org/chaos_calmer/15.05.1/brcm2708/bcm2709/ herunter. Unter Microsoft Windows benutzen Sie das Programm win32diskimager, um das Abbild auf die Micro-SD-Karte zu schreiben. Wenn Sie diesen Vorgang mittels eines Linux-Rechners erledigen wollen, gehen Sie analog Tabelle 9.3 oder wie nachstehend in Tabelle 10.4 beschrieben vor.

Aktion	Kommando	Abbildung
Feststellen der Gerätedatei	dmesg oder lsblk. Führen Sie lsblk vor und nach dem Einstecken der Micro-SD-Karte aus. Das neu hinzugekommene Gerät (hier: sde) muss beschrieben werden	Abbildung 10.30
Schreiben des Abbilds auf die Micro-SD-Karte	dd if=openwrt-15.05.1-brcm2708-bcm2709-sdcard-vfat-ext4.img of=/dev/sde bs=512k conv=fsync	Abbildung 10.31

Tabelle 10.4 Beschreiben der Micro-SD-Karte mit der Image-Datei unter Linux

Die Version »Chaos Calmer« hat bereits eine mehr oder weniger vollständige IPV6-Unterstützung. Die Weboberfläche verfügt über manche Erweiterung gegenüber der im Linksys WRT54GL gezeigten.

```

root@ZE6:~# # Vor Einlegen der SD-Karte
root@ZE6:~# lsblk
NAME    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0      11:0    1  1024M  0 rom
sda      8:0     0  111,8G  0 disk
├─sda1   8:1     0   93,1G  0 part /
└─sda2   8:2     0   18,7G  0 part [SWAP]
sdb      8:16    0  931,5G  0 disk
├─sdb1   8:17    0  838,2G  0 part /home
└─sdb2   8:18    0   93,3G  0 part /var
root@ZE6:~#
root@ZE6:~# # Nach dem Einlegen der SD-Karte
root@ZE6:~#
root@ZE6:~# lsblk
NAME    MAJ:MIN RM   SIZE RO TYPE MOUNTPOINT
sr0      11:0    1  1024M  0 rom
sda      8:0     0  111,8G  0 disk
├─sda1   8:1     0   93,1G  0 part /
└─sda2   8:2     0   18,7G  0 part [SWAP]
sdb      8:16    0  931,5G  0 disk
├─sdb1   8:17    0  838,2G  0 part /home
└─sdb2   8:18    0   93,3G  0 part /var
sdc      8:32    1    7,4G  0 disk
├─sdc1   8:33    1    20M  0 part /media/76A3-CAF6
└─sdc2   8:34    1    48M  0 part /media/bcbad195-d248-4e9b-854d-e644c3c8a0ad
root@ZE6:~#

```

Abbildung 10.30 Ermitteln der Gerätedatei mit »lsblk«

```

root@ZE6:~# dd if=openwrt-brcm2708-sdcard-vfat-ext4.img of=/dev/sdc bs=1M conv=fsync
76+0 Datensätze ein
76+0 Datensätze aus
79691776 Bytes (80 MB) kopiert, 2,37416 s, 33,6 MB/s
root@ZE6:~#

```

Abbildung 10.31 Schreiben des Abbilds auf die Micro-SD-Karte

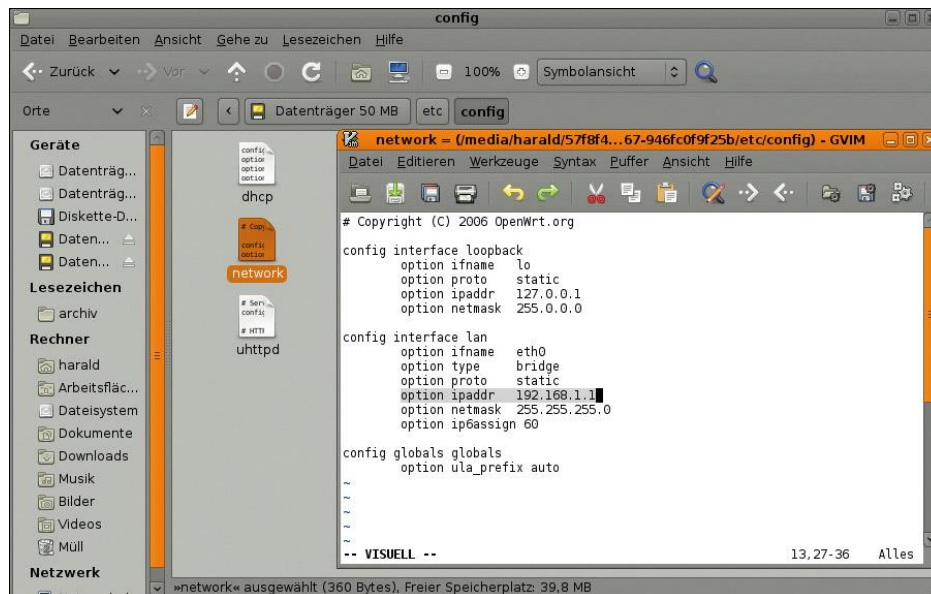


Abbildung 10.32 Ändern der LAN-IP-Adresse des »openwrt«-Routers auf der Micro-SD-Karte

Ziehen Sie die soeben beschriebene Micro-SD-Karte ab, und stecken Sie diese nochmals an Ihren PC. Sie können schon jetzt bequem einige Konfigurationsschritte im Vorfeld erledigen:

Einstellen der LAN-IP-Adresse für die Inbetriebnahme: Öffnen Sie die Datei `etc/config/network` mit dem Editor Ihrer Wahl, und ändern Sie die Einstellung zu `option ipaddr` ab (Abbildung 10.32). Vergeben Sie hierbei keinesfalls die Adresse des aktuell erreichbaren Routers! Verwenden Sie eine »Baustellenadresse« zur weiteren Konfiguration.

Es werden weitere `openwrt`-Programmpakete benötigt. Laden Sie diese von https://downloads.openwrt.org/chaos_calmer/15.05.1/brcm2708/bcm2709/packages/base/ herunter:

```
- kmod-libphy_3.18.23-1_brcm2708.ipk
- kmod-mii_3.18.23-1_brcm2708.ipk
- kmod-usb-core_3.18.23-1_brcm2708.ipk
- kmod-usb-net_3.18.23-1_brcm2708.ipk
- kmod-usb-net-asix_3.18.23-1_brcm2708.ipk
- kmod-usb-net-mcs7830_3.18.23-1_brcm2708.ipk

- kmod-usb-ohci_3.18.23-1_brcm2708.ipk
- kmod-usb-uhci_3.18.23-1_brcm2708.ipk
- iftop_1.0pre2-1_brcm2708.ipk
- terminfo_5.9-2_brcm2708.ipk
- libncurses_5.9-2_brcm2708.ipk
- libpcap_1.5.3-1_brcm2708.ipk
- libpthread_0.9.33.2-1_brcm2708.ipk
- luci-i18n-base-de_git-16.018.33482-3201903-1_all.ipk
```

Die Pakete `kmod...` werden zur Einbindung des USB-LAN-Adapters benötigt. Des Weiteren installieren Sie die deutschsprachige Erweiterung für die Weboberfläche `luci` und ein nützliches Programm zur Anzeige des Geschehens auf einer Netzwerkschnittstelle, nämlich `iftop`.

Legen Sie auf der Micro-SD-Karte ein Verzeichnis *pakete* an, und öffnen Sie dieses. Kopieren Sie die gerade heruntergeladenen Dateien in dieses neue Verzeichnis. Entfernen Sie die Micro-SD-Karte aus dem Verzeichnisbaum, und ziehen Sie diese vom PC ab.

Stecken Sie die Micro-SD-Karte in den Raspberry Pi (nachfolgend *Router* genannt), und schalten Sie das Gerät ein. Jetzt nehmen Sie die weitere Inbetriebnahme vor: Verbinden Sie sich mittels `telnet` mit dem Router, ändern Sie das Kennwort (`passwd`), und

wieder per WEB daran an.

Nach der Anmeldung klicken Sie auf System und hierin auf Language and Style, dort wählen Sie Language und Deutsch (German). Melden Sie sich ab. Melden Sie sich wieder an. Die Weboberfläche zeigt sich Ihnen nun in deutscher Sprache. Klicken Sie auf Netzwerk • Schnittstellen und dort auf Neue Schnittstelle hinzufügen. Sie müssen dort den Namen `wan` vergeben (Abbildung 10.34). Bestätigen Sie Ihre Eingaben mit einem Klick auf Absenden.

Abbildung 10.34 Anlegen der WAN-Schnittstelle

Klicken Sie auf Schnittstellen • WAN • Bearbeiten. Unter Allgemeine Konfiguration wählen Sie das zutreffende Protokoll (hier: pppoe für den Internetzugang) und klicken dann auf Wechsle Protokoll (Abbildung 10.35).

Abbildung 10.35 Schnittstelle WAN, allgemeine Konfiguration

Geben Sie die Daten hierfür ein (Abbildung 10.36), und klicken Sie auf Speichern & Anwenden.

Starten Sie die Schnittstelle durch einen Klick auf Verbinden.

Prüfen Sie die Firewall-Zoneneinstellung. Klicken Sie hierzu auf Schnittstellen • WAN • Bearbeiten • Firewall Einstellungen. Die Schnittstelle `wan` sollte der Firewall-Zone `wan` zugewiesen sein (Abbildung 10.37).

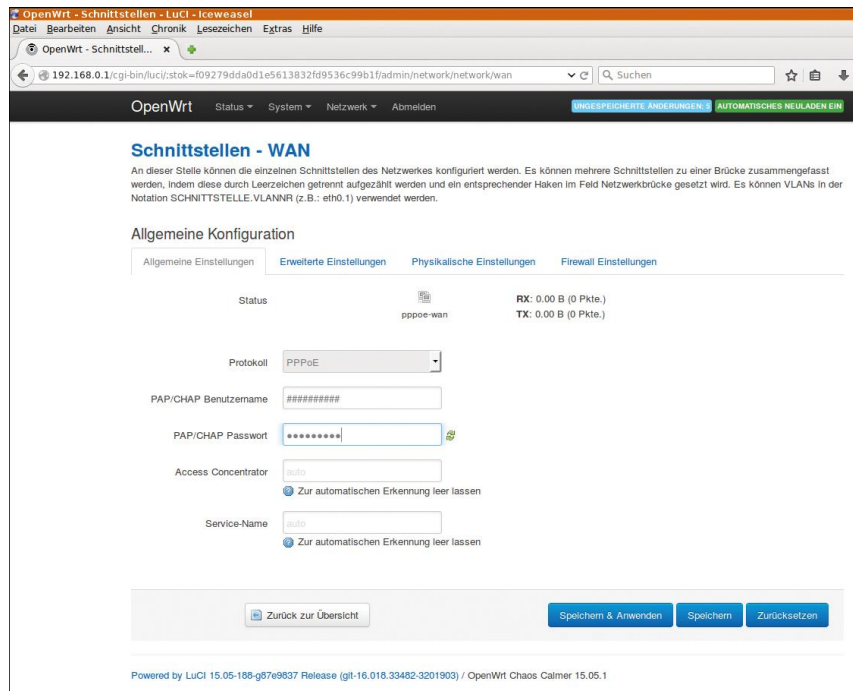


Abbildung 10.36 Konfiguration Internetzugang

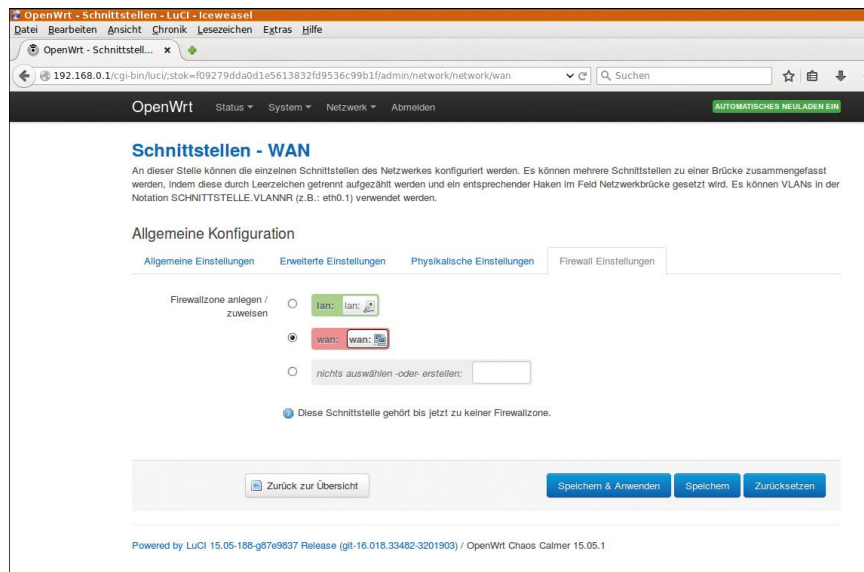


Abbildung 10.37 Kontrolle: Firewall-Einstellungen für WAN

Prüfen Sie bei Netzwerk • Diagnose die Funktion, und sichern Sie die Einstellungen auf einen PC (über die Menüpunkte System • Backup)!

Analog gilt das gezeigte Vorgehen für mit dem Raspberry Pi verwandte Rechner wie Cubie-Truck oder Banana Pi (bei Letzterem: sobald »stabile« Kartenimages vorliegen).

10.4.4 Switches

Switches erhalten Sie im Fachhandel in allen Größenordnungen. Sie können zunächst einmal grob zwischen *nicht managebaren* und *managebaren* Geräten unterscheiden. Dies ist nicht zwingend eine Frage der Größe. Auch für den Einbau in 19-Zoll-Schränke erhalten Sie nach wie vor Switches ohne Management-Modul.

Nach wie vor werden Sie noch Switches finden, die bei der Geschwindigkeit nicht über 100 Mbit/s hinauskommen. Das reicht zwar für kleine Büros und Privathaushalte aus.

Bei einem Neukauf wählen Sie aber besser ein Modell, das 1 Gbit/s leistet und dabei aber auch die älteren Normen 100Base-T und 10Base-T unterstützt.

Sie bekommen kleine Tischgeräte (Abbildung 10.38), die vier oder mehr Anschlüsse besitzen. Maximal 64 Anschlüsse weisen 19-Zoll-Geräte auf. Für kleine Firmen, Kanzleien und Pensionen reicht oft eines dieser Geräte aus (Abbildung 10.39).



Abbildung 10.38 Tisch-Switch »S21318« der Firma Synergie 21, ohne Management-Modul



Abbildung 10.39 »DGS-1210-16« der Firma D-Link, managebar

Der in Abbildung 10.39 gezeigte Switch bietet 16 1000Base-T-Anschlüsse. Weiter verfügt das Gerät über vier Einsteckplätze für SFP-Transceiver. Für jeden benutzten Einsteckplatz fällt allerdings ein 1000Base-T-Anschluss weg. D-Link bietet hierfür vier verschiedene Transceiver-Modelle an (Tabelle 10.5):

Modell	Typ	Faser	Wellenlänge	Reichweite
DEM-311GT	1000Base-SX	Multimode	850 nm	550 m
DEM-310GT	1000Base-LX	Monomode	1310 nm	10 km
DEM-314GT	1000Base-LX	Monomode	1310 nm	50 km
DEM-315GT	1000Base-LX	Monomode	1550 nm	80 km

Tabelle 10.5 Transceiver-Modelle von D-Link

Wenn Sie mehr »Switch« benötigen, wählen Sie Modelle, die über ein eigenes Backbone oder ein schnelles SFP-Modul miteinander koppelbar sind. Sie erhalten auch Switches mit einem schrankfüllenden Chassis, in das Sie verschieden bestückte Einschübe geben können. Damit bekommen Sie Ihren »Wunsch-Switch«, sogar mit Kupfer- und Glasfasertechnik gleichzeitig. Großgeräte dieser Art bieten Cisco und HP an.

Weitere Leistungsmerkmale von Switches sind redundante Netzteile, entsprechender Datendurchsatz sowie Power-over-Ethernet. Achten Sie bei einer Neubeschaffung in jedem Fall darauf, dass auch das Management-Modul IPv6-fähig ist. Vergleichen Sie die Größe der MAC-Adresstabelle und den Datendurchsatz je Port.

10.4.5 Printserver

Mit einem Printserver sorgen Sie dafür, dass ein Drucker über das Netzwerk erreichbar ist. In jedem Fall können Sie ihn unabhängig von den meist kurzen Anschlusskabeln zum PC da aufstellen, wo es Ihnen am besten erscheint. Sie können noch weitere Vorteile nutzen:

- Einsparung von Druckern; in größeren Büros teilen sich mehrere Arbeitsplätze ein Gerät.
- Drucker können getrennt vom Arbeitsplatz betrieben werden (Lärm, Staub).

Wertvolle Spezialdrucker (Großformatgeräte, Foliendrucker, Plotter, Fotodrucker) bringen Sie in zentralen Räumen unter, die unter der Kontrolle der EDV-Administration liegen.

Manchen Druckern liegt Spezialsoftware bei, mit der Sie bequem die Konfiguration und den Betrieb steuern können.

Printserver sind vom Arbeitsplatz aus per Web konfigurierbar.

Die meisten externen Printserver (Abbildung 10.40) setzen einen Netzwerkanschluss (meist 100Base-T) auf einen einzigen USB- oder Centronix-Anschluss um. Sie bekommen besser ausgestattete Modelle, wie z. B. den Edimax PS-3103P mit drei Centronix-Anschlüssen. Am Edimax PS-3207U finden Sie zwei USB-2- und einen Centronix-Anschluss. Damit können Sie vor allem »Druckerecken« in Großraumbüros einrichten.



Abbildung 10.40 Externer Printserver

Sie erhalten mittlerweile viele Drucker mit eingebautem oder nachrüstbarem internen Printserver (z. B. Kyocera FS-1370DN). Hier finden Sie auch schon Modelle, die 1000Base-T unterstützen oder sogar einen LWL-Anschluss vorweisen. In Abbildung 10.41 sehen Sie einen internen Printserver für ältere Kyocera-Drucker (FS-1900, FS-1010).



Abbildung 10.41 Interner Printserver

Ältere Printserver bergen Sicherheitsprobleme in sich:

Jeder Benutzer kann die Einstellungen ohne Authentifizierung manipulieren.
Der Printserver kann als Ablageort für Schadsoftware missbraucht werden.
Die Druckdaten können nur unverschlüsselt an den Printserver geschickt werden.

Bei modernen Printservern (wie dem des Kyocera FS-1370DN) können Sie Ihre Druckdaten mit SSL-Verschlüsselung senden. Für die Änderung von Einstellungen müssen Sie sich authentifizieren.

10.4.6 Netzwerkspeicher (NAS)

Mit einem *Network Attached Storage (NAS)* schaffen Sie eine zentrale Möglichkeit, über Ihr lokales Netz eine zentrale Datenhaltung anzulegen. Sie können meist per SMB und NFS, auch oft mit FTP darauf zugreifen. Die Konfiguration nehmen Sie über eine Weboberfläche vor. Vielfach finden Sie diese Geräte als reine Datensicherungslösung im Einsatz.

Kleine »Netzwerkfestplatten« (Bezeichnung des Fachhandels) verfügen nur über eine Festplatte. Der Vorteil gegenüber einer reinen USB-Anstecklösung besteht in der geforderten Authentifizierung. Achten Sie beim Kauf vor allem auf die Netzwerkschnittstelle. Oft verfügen preisgünstige Modelle nur über einen 100Base-T-Anschluss. Damit zieht

sich der Datentransfer bei größeren Volumen unnötig in die Länge.

Größere Geräte verfügen über mehrere Festplatten, die zu einem RAID-Verbund zusammengefasst sind. Sie finden hier auch mehrere LAN-Schnittstellen vor. Für die Leistungsaufnahme und Wärmeabgabe nehmen Sie Werte wie bei größeren PCs an. Rechnen Sie sich deshalb einmal aus, ob sich für Sie die Anschaffung so eines Geräts rentiert. Mit handelsüblichen Rechner teilen bauen Sie sich selbst einen kostengünstigen Netzwerkspeicher auf. Als Betriebssystem verwenden Sie FreeBSD. Sie können dadurch das Dateisystem ZFS verwenden. Es bietet eine komfortable Datenträgerverwaltung an. Reicht der Plattenspeicher nicht mehr aus, bauen Sie eine weitere Platte in das Gerät ein und teilen in einer Zeile dem Speicherpool mit, dass das Plattengerät »dazugehört«. Sie müssen weder vorher eine Partition noch ein Dateisystem anlegen (»formatieren«). Mehrere Datenplatten fassen Sie mit RAID-Z2 (so wird das beim ZFS bezeichnet) zu einem Array zusammen.

FreeBSD bietet Ihnen zudem die Möglichkeit, mehrere Domains für Samba, NFS oder SSHFS innerhalb verschiedener Jails anzulegen. Ein Jail ist ein stark abgeschotteter Teilbaum des Hauptdateisystems und stellt eine Erweiterung des `chroot`-Mechanismus dar. Jedes Jail verfügt über eine eigene IP-Adresse und wird in fast allen Punkten so konfiguriert, als wäre es ein eigenständiger Rechner.

10.4.7 Modems für den Netzzugang

Ein Modem stellt für Sie die Verbindung von Ihrem Rechner zu einem entfernten Rechnersystem über die normale Fernmeldeinfrastruktur her. Die Geräte erhalten Sie als Baugruppe oder als externe Einheit. In manchen Notebooks finden Sie Modems fest eingebaut vor. Sie können Modems hinsichtlich der Fernmeldetechnik unterscheiden:

Analoge Modems (Abbildung 10.42): ältester Telefonstandard, Transferrate maximal 57 kbit/s. Sie benutzen meist die serielle Schnittstelle (maximal 115 kbit/s, Anschluss über SUB-D-9- oder SUB-D-25-Stecker, auch USB-Modelle im Handel).

ISDN-Modems (Abbildung 10.43): ISDN-Standard, 64 kbit/s (1 Kanal) oder 128 kbit/s (Kanalbündelung), Anschluss über SUB-D-9- oder SUB-D-25-Stecker, auch USB-Modelle im Handel). In den USA und einigen anderen Ländern stehen nur 56 kbit/s je Kanal zur Verfügung.

DSL-Modems: digitaler Teilnehmeranschluss, Datenraten von 384 kbit/s bis 200 Mbit/s (VDSL2). DSL finden Sie in zwei Modi vor:

– ADSL: Hier ist der Downstream schneller als der Upstream.

– SDSL: Down- und Upstream sind gleich schnell. Anschluss über LAN-Kabel, RJ45.

Kabel-Modems: Übertragung über das Netz der Kabelfernsehanbieter, Datenraten derzeit bis 32 Mbit/s möglich, 100 Mbit/s in Einführung. Anschluss über LAN-Kabel (RJ45).

Funkmodems für das GSM-Netz (GPRS): zwischen 9,6 kbit/s und 55 kbit/s möglich, USB-Anschluss



Abbildung 10.42 Analog-Modem älterer Bauart



Abbildung 10.43 ISDN-Modem

Funkmodems für UMTS, HSDPA (Abbildung 10.44), LTE und LTE Advanced: Die maximal erzielbaren Datenraten liegen bei 384 kbit/s, 14,1 Mbit/s (üblich sind 7,2 Mbit/s) und 3–50 Mbit/s bzw. bis zu einem Gbit/s.

Die Funkmodems mit USB-Anschluss können Sie an geeigneten Routern anstecken. Sie versorgen damit ein lokales Netzwerk mit Internetzugang.



Abbildung 10.44 USB-Funkmodem für HSDPA

Ein Analog- oder ISDN-Modem eignet sich kaum mehr zur Internetanbindung. Bei den heute üblichen Webseiten müssten Sie mit diesen Geräten lange Wartezeiten für Übertragung und Aufbau in Kauf nehmen. Allenfalls für die Herstellung von Wartungsverbindungen

können Sie diese Art der Verbindung nutzen. Für die Anbindung von Computerkassen und Warenwirtschaftsterminals eignet sich diese Anbindung ebenso.

10.5 Einbindung externer Netzwerkteilnehmer

Filialbetriebe, Heim- und Außendienst-Mitarbeiter und Wartungspersonal benötigen eine Zugriffsmöglichkeit auf Ihr Netzwerk. Dabei können Sie verschiedene Wege nutzen:

Langsam, aber sicher: Per Analog- oder ISDN-Modem (Abbildung 10.45) können Sie das Telefonnetz benutzen und zwischen dem externen Rechner und Ihrem Netz hierüber eine Verbindung aufbauen. Dazu benötigen Sie einen »Einwahlrechner«, der unter Linux oder FreeBSD arbeitet. Dort müssen Sie die Programme `mgetty` und `ppp` installiert und konfiguriert haben. Näheres hierzu entnehmen Sie den Manual-Seiten zu diesen Programmen. Gute Erklärungen finden Sie auch im FreeBSD-Handbuch unter www.freebsd.org/doc/de/books/handbook/dialup.html. Diese Methode ist aber eher nur für Wartungszugänge gedacht.

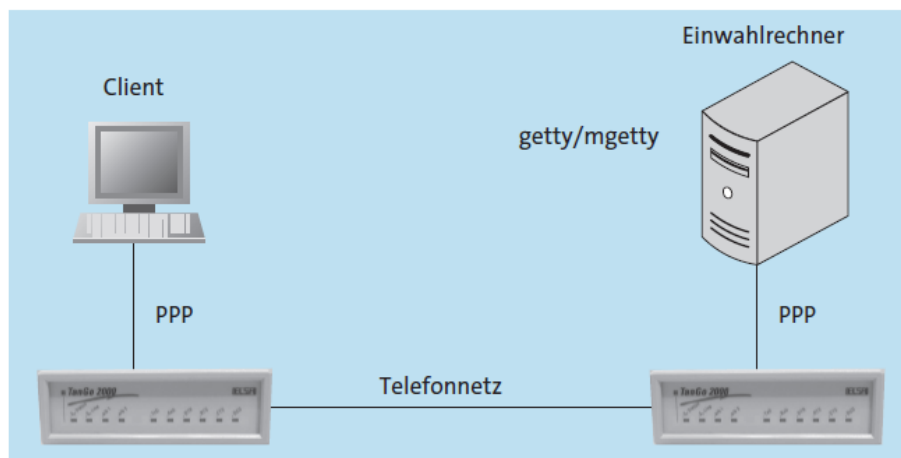


Abbildung 10.45 Rechnerverbindung über das Telefonnetz

Von jedem Punkt der Welt: Per Modem oder DSL verbinden Sie sich als externer Teilnehmer Ihres Netzwerkes über Ihren Internet-Provider mit dem Internet. Sie gelangen über Ihr Netzwerk durch die Firewall, für die Sie eine Ausnahmeregelung aufstellen müssen. Meistens werden Sie den SSH-Port benutzen. Hierüber können Sie per Tunnel Fernsitzungen (Citrix, RDP, nomachine, Display-Umleitung à la »ssh-X«) oder Datenübertragungen (SSHFS, sftp) nutzen. Über den SSH-Tunnel können Sie auch E-Mails senden und empfangen. Sie können auch eine VPN-Verbindung aufbauen.

10.6 Sicherheit

Für Ihr Netzwerk gelten Sicherheitsregeln allgemeiner Art und solche, die in der individuellen Konfiguration liegen. Ich führe hier einige häufige Sicherheitsprobleme an. Ihr Netzwerk und die damit verbundenen Systeme sind durch viele vermeidbare Umstände gefährdet:

- Kennwörter für Router, Firewall und Switches sind nicht nur den Systembetreuern bekannt.
- Ihre Benutzer wenden Programme an, die über offene Standard-Ports eigene Verbindungen zur Außenwelt schaffen.
- Die Systembetreuer ignorieren Firmware-Updates für Router, Firewall und Switches.
- Die Benutzer und Systembetreuer führen keine Sicherheits-Updates für Betriebssysteme und Anwendungen durch.
- Die Systembetreuer richten keine Kontrolle ein- und ausgehender E-Mails auf Schadsoftware ein.
- Es besteht zwar eine Kontrolle von E-Mails auf Schadsoftware, die Virensignaturen werden aber selten erneuert.
- Die Außendienst-Mitarbeiter installieren selbst Programme auf ihren Laptops.
- Die Innendienst-Mitarbeiter bringen eigene Rechner mit und schließen diese an das

Netzwerk an.

Die Innendienst-Mitarbeiter können ohne Kontrolle eigene Programme auf ihren PCs installieren.

Fremdes Wartungspersonal bekommt dauerhafte Benutzerkennungen und Kennwörter zugewiesen.

Ihre Mitarbeiter teilen dem betriebsfremden Wartungspersonal Benutzerkennungen und Kennwörter mit.

Die Systembetreuer lassen fremdes Wartungspersonal unbeaufsichtigt arbeiten.

Mitarbeiter Ihres Betriebs tauschen sich in sozialen Netzwerken aus und geben untereinander Kennwörter »für den Vertretungsfall« preis.

Mitarbeiter Ihres Betriebs äußern sich in sozialen Netzwerken und auf Fachmessen über interne Datenschutzmaßnahmen und Zugangsregeln.

»Feindlich« gesinnten Mitarbeitern gelingt es, in E-Mails wichtige Firmeninterna und Daten bequem über das Netz an Konkurrenten zu übermitteln, weil die Zugriffsmöglichkeiten hierauf bestanden.

Mit einigen allgemeinen Maßnahmen und Regeln können Sie die Gefahren eindämmen:

Schaffen Sie Zugriffsregelungen in Ihren Anwendungsprogrammen.

Verlagern Sie die Ausführung von Programmen auf einige zentrale Rechner.

Gebrauchen Sie Standard-Ports nur bei Diensten, bei denen dies unbedingt notwendig ist.

Setzen Sie Thin Clients ein. Ihre Mitarbeiter können keine lokalen Kopien irgendwelcher Dateien anfertigen und auch keine Daten auf USB-Sticks und CDs kopieren. Dies übernehmen im begründeten Bedarfsfall die Mitarbeiter der Systembetreuung.

Verlangen Sie den regelmäßigen Wechsel der Benutzerkennwörter.

Degradieren Sie Ihre Außendienst-Notebooks ebenso zu »Thin Clients«. Per gesicherter Verbindung werden die Anwendungen im Betrieb ausgeführt. Auf den Notebooks befinden sich für einen Dieb wertlose Software und vor allem keine betrieblichen Daten.

Verbieten Sie in einer Betriebsvereinbarung die private E-Mail-Nutzung.

Stellen Sie Ihren Mitarbeitern zum privaten Surfen in den Pausen entsprechende Internetplätze zur Verfügung. Für diese bauen Sie ein vom Betrieb getrenntes Netz auf (gegebenenfalls sogar mit eigenem Router ins Internet).

Für das Ausführen von Internetanwendungen (E-Mail, Surfen, Datentransfer) setzen Sie zentral einen eigenen Rechner ein. Abgehende und ankommende E-Mails und Daten lassen Sie eine eingehende Prüfung hinsichtlich Schadsoftware passieren.

10.6.1 Abschottung wichtiger Rechner

Für umfangreichere Netzwerke finden Sie vielleicht einige Details des Szenarios aus Abbildung 10.46 interessant.

Die Firewall (siehe auch Abschnitt 6.4, »Die Firewall«) schottet Ihr Netz ab und lässt nur die notwendigen Ports offen. Der Proxyserver nimmt seine Stellvertreterrolle für HTTPAbfragen wahr. Ihre Benutzer gebrauchen Thin Clients oder die Außendienst-Notebooks.

Sie sind mittels verschlüsselter Verbindung mit dem »Terminal Server« verbunden. Auf diesem laufen wiederum nur die Clients für *Citrix XenApp*, *rdp*, *xrdp* oder *X2Go*, *ssh*, *https* (nur Intranet). Die Server haben einen doppelten Netzwerkanschluss: einen für das Arbeitsnetz und einen für die Datensicherung und den administrativen Zugriff. Mit dem Verteilen von Anwendungen auf verschiedene Rechner gewinnt Ihr Netz an Sicherheit. Vergessen Sie aber nicht, Redundanzen für diese Geräte vorzuhalten. Die Netze »Intranet«, »TC-Netz« und »Wartungsnetz« haben keine Verbindung miteinander.

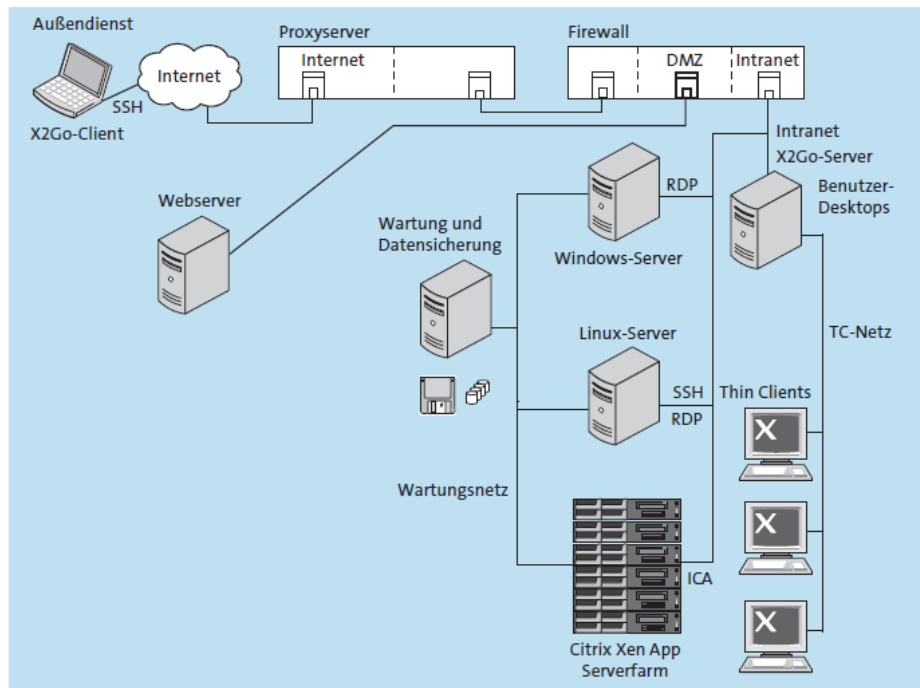


Abbildung 10.46 Abgesperrte Netze und Rechner

Hauptsächlich sehe ich Gefahren für Rechner mit Programmen wie Webbrowsern und Mail-Clients. Sehen Sie sich deshalb dieses Detail in Abbildung 10.47 an. Die Anwendungen laufen auf einem extra Rechner. Dabei helfen einige Details, System und Daten zu schützen:

Beim An- und Abmelden eines Benutzers laufen Skripte. Vom Webbrowser genutzte Unterverzeichnisse lassen sich damit löschen und neu anlegen. Dabei schreiben Sie auch die Konfigurationsdateien des Browsers neu.

E-Mail und Downloads: Anhänge und Downloads verschiebt der Anwender in ein Quarantäneverzeichnis. Die Antivirensoftware überprüft die darin liegenden Dateien. Geprüfte Dateien landen in einem Verzeichnis, aus dem der Benutzer die »sauberen« Dateien auf seinen Arbeitsplatz verschieben kann. Der Benutzer kann nur über diesen Weg an seine Daten kommen.

Der Internetanwendungsserver routet nicht zwischen dem Internet und dem internen Netz.

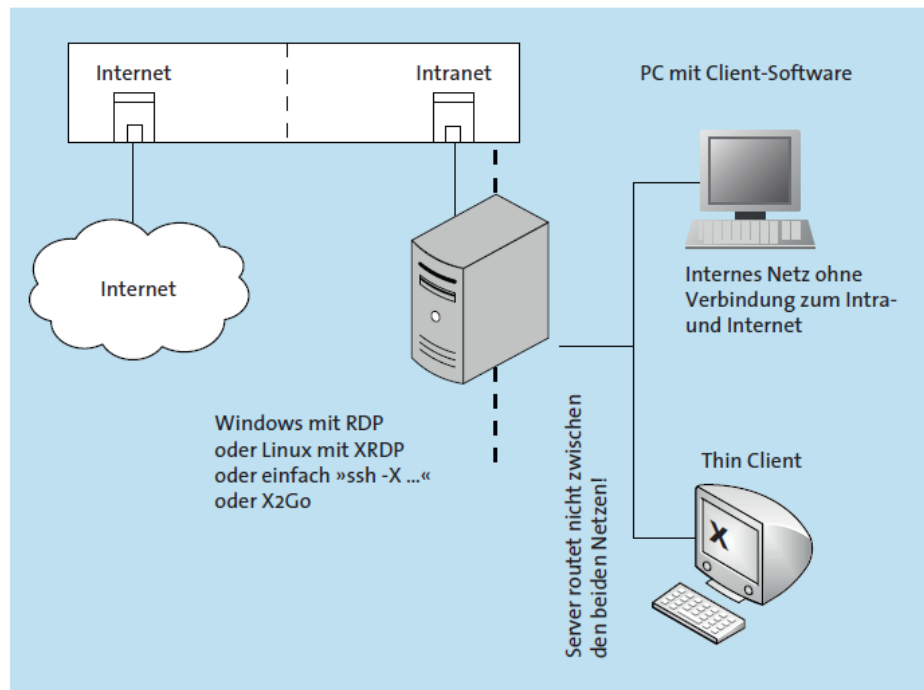


Abbildung 10.47 Internetanwendungsserver

Dieses Vorgehen hat verschiedene Vorteile für die Benutzer und die Systemsicherheit:

- Ihre Benutzer haben von jedem Arbeitsplatz aus einen Internetzugang.
- Von jedem Arbeitsplatz aus können die Benutzer auf Ihre E-Mails zugreifen.
- Es sammelt sich kein Datenmüll an, der nur Plattenspeicher belegt.
- Ihre Benutzer können nicht mehr einfach Programme aus dem Internet auf ihren Arbeitsplatzrechnern installieren. Verstöße gegen Lizenzen oder die Wirkungen von Schadsoftware brauchen Sie nicht mehr zu fürchten.

10.6.2 Netzwerkverbindung mit einem Virtual Private Network (VPN)

Mit einem VPN verbinden Sie zwei räumlich getrennte Netze (Abbildung 10.48) über das Internet. Sie können auch Einzelrechner mittels VPN in Ihr Stammnetz einbinden (Abbildung 10.49).

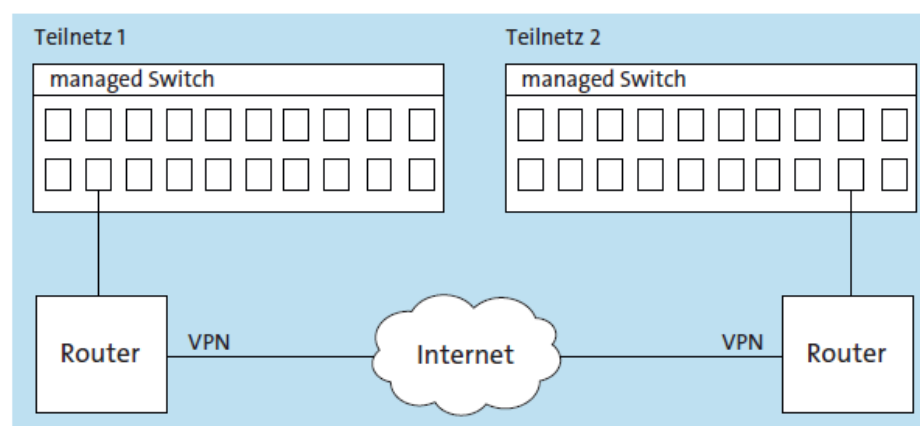


Abbildung 10.48 VPN

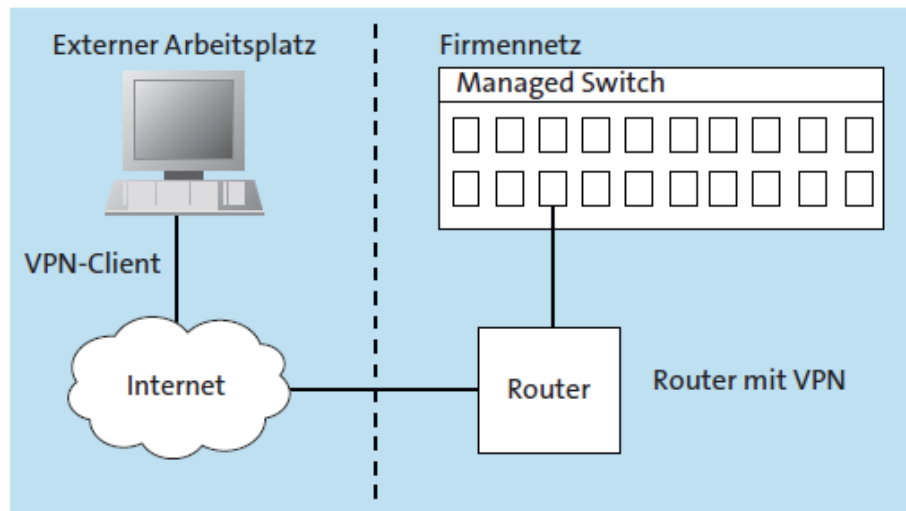


Abbildung 10.49 VPN-Einbindung eines Einzelrechners

Bei der VPN-Technik leiten Sie idealerweise den gesamten Netzwerkverkehr durch einen (mit SSL oder IPSec) verschlüsselten Tunnel. Bei VPNs müssen Sie einige Gegebenheiten beachten:

Falls Sie zwei oder mehrere Netze miteinander koppeln, müssen Sie die IP-Adressen aller Teilnehmer des dann »großen« Netzes aufeinander abstimmen. Sie dürfen eine IP-Adresse im gesamten Netz nur einmal vergeben.

Wenn Sie einen externen Einzelrechner in Ihr VPN einbinden, kann er mit seinem örtlichen lokalen Netzwerk normalerweise nicht mehr kommunizieren.

Die VPN-Router übernehmen die Aufgabe einer Bridge.

Die Netzanbindung erstreckt sich nicht auf einzelne Anwendungen, sondern auf den gesamten Netzwerkverkehr.

Innerhalb dieses zusammengeschalteten Netzwerks sind alle Teilnehmer gleichermaßen erreichbar.

OpenVPN bietet Ihnen Client-Software für externe Rechner.

Es existieren mehrere Ansätze, um VPNs zu betreiben. Diese sind nicht kompatibel.

Sie finden viele nicht kompatible VPN-Implementierungen bei Routern. Die Geräteauswahl

kann für Sie schwierig werden.

VPN-fähige Router können nur eine vorgegebene Anzahl von VPNs verwalten. Für die Einbindung vieler externer Teilnehmer und Netze benötigen Sie entweder entsprechend

leistungsfähige Geräte, oder Sie weichen auf den verschlüsselten anwendungsbezogenen

Fernzugriff aus.

Einige verbreitete Protokolle finden Sie in Tabelle 10.6.

Protokoll	RFCs
PPTP, Point-to-Point Tunneling Protocol	2637
L2TP, Layer 2 Tunneling Protocol	2661, 2809, 2888, 3070, 3145, 3193, 3301, 3308, 3355, 3371, 3437, 3438, 3573, 3817, 3931, 4045, 5641
Kombination aus SSH und PPPD	1661, 1962, 2153

Tabelle 10.6 VPN-Protokolle

Im Zusammenhang mit Cisco-Hardware wird ein spezieller VPN-Client (Abbildung 10.50) verwendet.



Abbildung 10.50 Der Anmeldebildschirm

Sie binden Ihren Rechner so, wie in Abbildung 10.49 dargestellt, in das entfernte Netz mit ein. Ihre Zugangsdaten bestehen aus je einem Host-, Gruppen- und Benutzernamen sowie dem Kennwort. Der Client legt ein eigenes Netzwerkgerät cscotun0 an. Die Kenndaten einer laufenden Verbindung erhalten Sie unter Linux mit der `ifconfig`-Abfrage (Abbildung 10.51) oder im Statusmenü, das Sie in Abbildung 10.52 sehen.

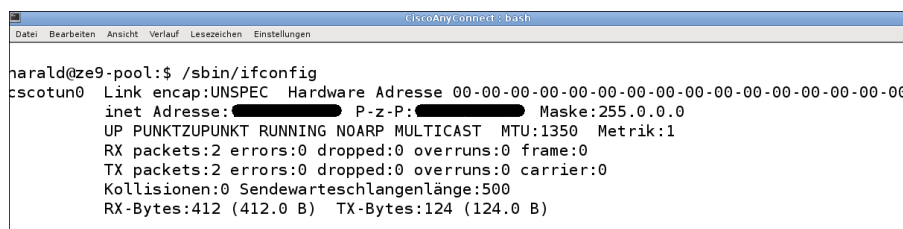


Abbildung 10.51 »ifconfig«-Abfrage, Netzwerkgerät »cscotun0«



Abbildung 10.52 Statusinformationen

Für den Betrieb eines VPNs unter *OpenWRT* kommt *OpenVPN* zum Einsatz. Umfangreiche Informationen hierzu finden Sie unter <http://www.openvpn.net>. Wenn Sie einen Server mit *OpenVPN* aufsetzen möchten, klären Sie in jedem Fall zunächst die folgenden Punkte ab. Die Anweisungen beziehen sich auf die Konfigurationsdatei */etc/openvpn/server.conf* bzw. unter Windows auf *%INSTALLVERZEICHNIS%\config\server.ovpn*. Sowohl für den Server als auch für die Clients existieren viele grafische Konfigurationswerkzeuge (für Beispiele siehe Abbildung 10.53 und Abbildung 10.54). Auf www.openvpn.net finden Sie die notwendige Anleitung auf dem neuesten Stand.

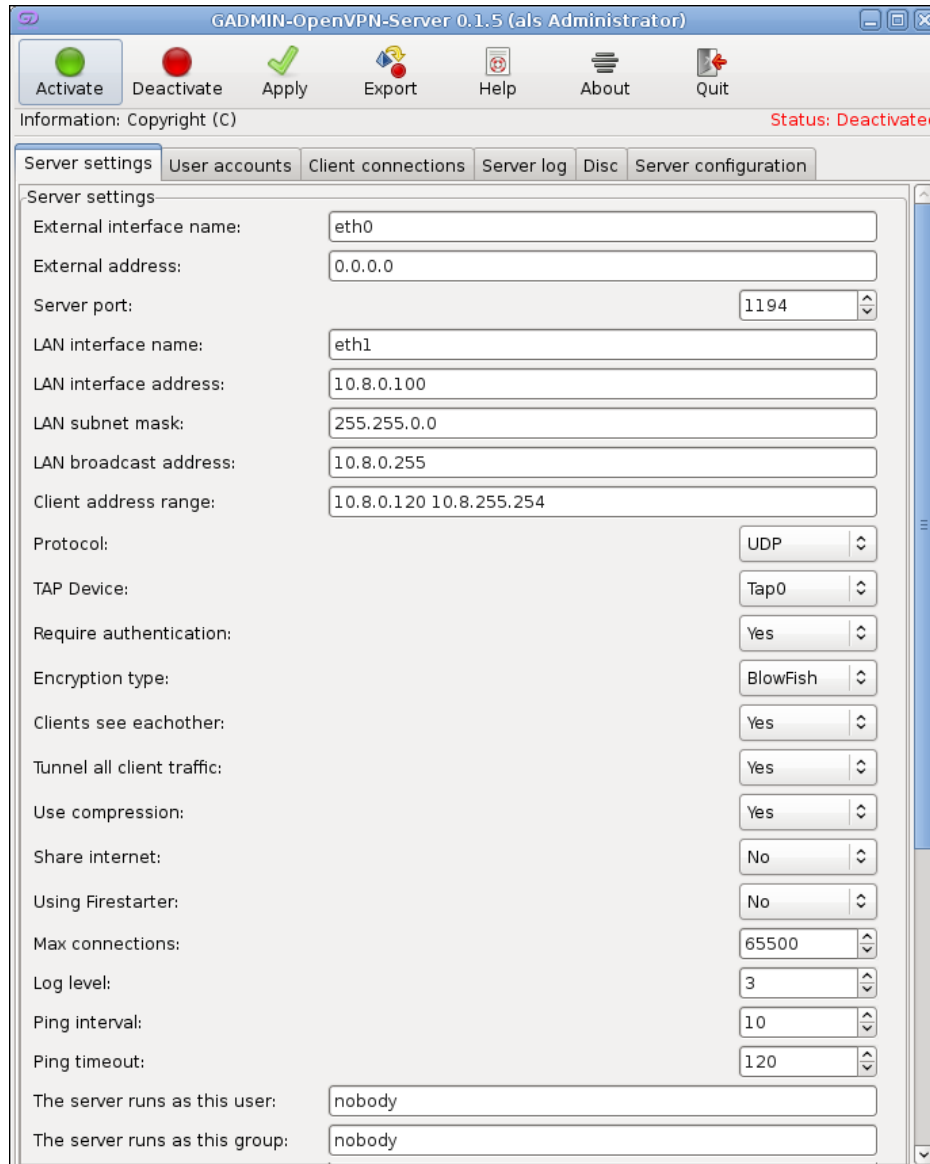


Abbildung 10.53 Server-Konfigurationsmenü

TUN oder TAP: Möchten Sie einen Ethernet-Tunnel (*dev tap*), der auch andere Netzwerkprotokolle transportiert (NetWare, NetBEUI ...), oder reicht Ihnen ein IP-Tunnel (*dev tun*) für Ihre Zwecke? Sie müssen sich für einen Typ entscheiden. Können Ihre entfernten Netzwerkteilnehmer problemlos auf den Standard-Port 1194 (*port 1194*) zugreifen? Sitzen Ihre mobilen, entfernten Netzwerkteilnehmer in gefilterten Hotel- oder Schulnetzen, sodass Sie auf andere Ports umstellen müssen (z. B. 443, den von HTTPS)? Wollen Sie TCP (*proto tcp-server*) oder UDP (*proto udp mode server*) verwenden (siehe auch Abschnitt 6.3.3, »Ports und Sicherheit«)? Möchten Sie Zertifikate oder Schlüssel einsetzen? Zertifikate benötigen einen externen

»Beglaubiger«, Schlüssel erzeugen Sie selbst, wodurch Sie die komplette Hoheit über das Verfahren haben.

Sollen die Clients untereinander kommunizieren können (client-to-client)? Der OpenVPN-Server arbeitet als Router und kann damit auch zwischen den Clients vermitteln.

Wenn dies aus Sicherheitsgründen unerwünscht ist, unterbinden Sie es!

Welche Authentifizierungsmethode (auth METHODE) kommt zum Einsatz?

Ferner müssen Sie *ICMP* (siehe dazu auch Kapitel 5, »Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen«) erlauben, damit die Verbindung zwischen dem Server und den Clients kontrolliert werden kann.

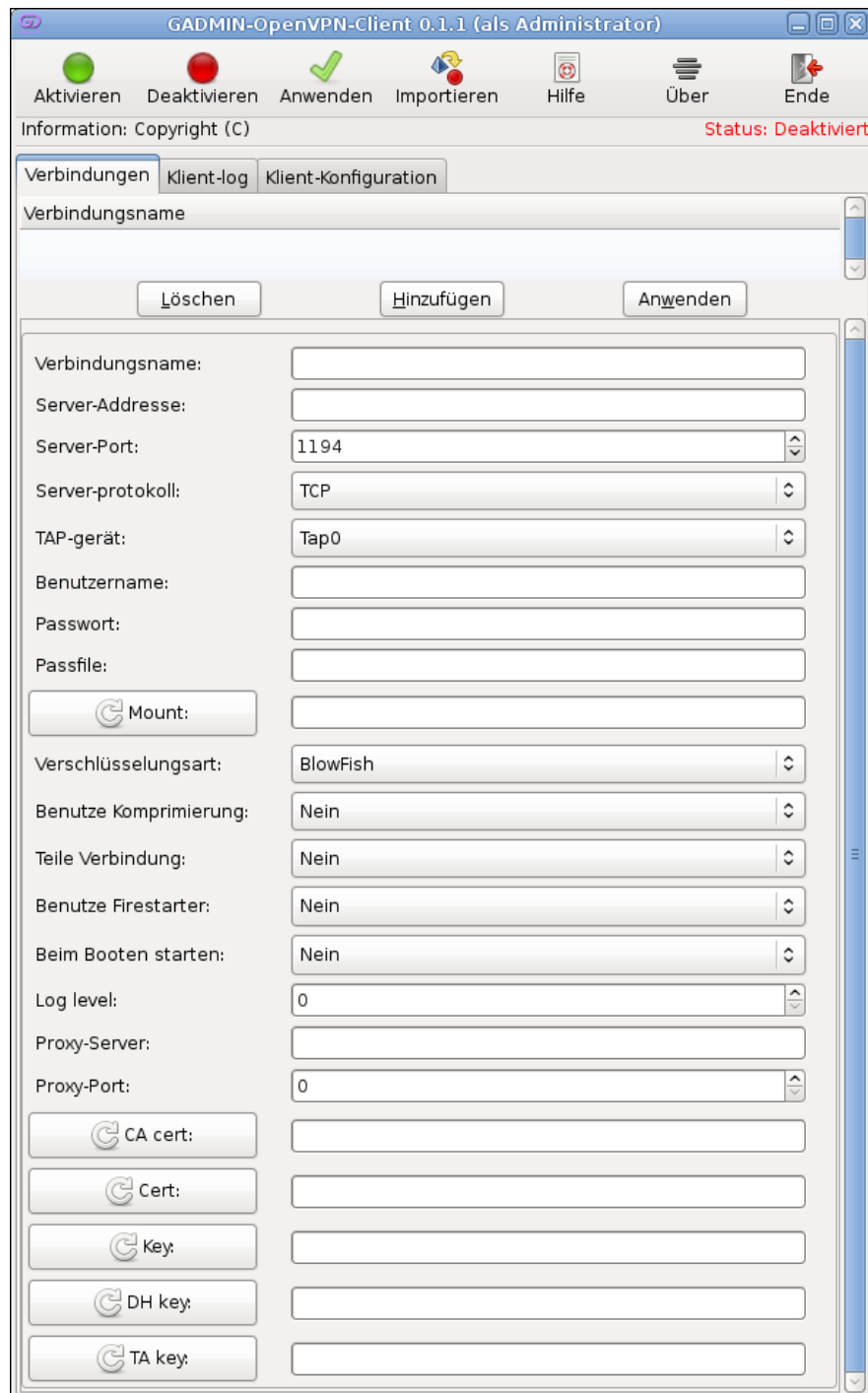


Abbildung 10.54 Client-Konfigurationsmenü

Bezüglich weitergehender Sicherheitsratschläge lesen Sie auch auf www.bsi.bund.de die verschiedenen Publikationen zu Sicherheitsthemen.

10.6.3 WLAN sicher konfigurieren

Beim WLAN fehlt Ihnen die physische Kontrolle über das Netz. Die Funkwellen machen nicht an der Grundstücksgrenze halt. Es besteht immer die Gefahr, dass Fremde Ihr Netz nutzen oder den Datenverkehr mitlesen wollen. Für die Zugangskontrolle benötigen Sie einen Radius-Server. Richten Sie sowohl eine Verschlüsselung als auch einen Zugangsschutz für Ihr Funknetz ein:

1. Der WLAN-Router muss sowohl die Verschlüsselung nach aktueller Norm (derzeit WPA2, AES) als auch den Netzzugang mit einem integrierten Radius-Server beherrschen. Der integrierte Radius-Server ist für Sie deshalb von Vorteil, weil kein zusätzlicher Rechner im Dauerbetrieb notwendig ist. In Tabelle 10.7 finden Sie einige Modelle, die die notwendigen Verfahren beherrschen. Sie finden unter <https://openwrt.org> auch ein Open-Source-Projekt, mit dem Sie eine alternative Firmware auf WLAN-Router aufspielen, die den Radius-Server enthält. Die Liste der unterstützten Router finden Sie unter <http://wiki.openwrt.org/toh/start>.

Modell	Details
Zyxel N4100	WLAN-Hotspot-Lösung mit integriertem Abrechnungssystem und Drucker
LANCOM WLC-4006	Sie benötigen noch einen oder mehrere Accesspoints.
Lancom 1780EW-3G	UMTS-VPN-Router mit HSPA+

Tabelle 10.7 WLAN-Geräte mit Radius-Server

2. Legen Sie als Verschlüsselung WPA2 fest.
3. Falls notwendig, erzeugen Sie die notwendigen Zertifikate.
4. Wählen Sie für den Radius-Server eine verschlüsselte Anmeldemethode aus.
5. Richten Sie im Radius-Server die Benutzer ein, und geben Sie diesen ihre Zugangsdaten bekannt.
6. Speichern Sie das Stammzertifikat auf einem der Client-Rechner (Windows: geschützte Verbindung, EAP), bzw. legen Sie es im Heimatverzeichnis (Linux) ab. Konfigurieren Sie hier mit dem Netzwerkmanager Ihrer Distribution die Verbindung.
7. Testen Sie mit diesem Gerät die Verbindung.

10.6.4 SSH-Tunnel mit PuTTY aufbauen

Das Programm PuTTY erhalten Sie für Microsoft Windows, Linux, FreeBSD und diverse Unix-Derivate. Sie können damit nicht nur SSH-Sitzungen abhalten, sondern auch für eine schutzwürdige Sitzung oder Datenübertragung einen Tunnel einrichten. Voraussetzung dafür ist, dass Sie am Zielsystem über einen gültigen Benutzerzugang verfügen und ein SSH-Server (OpenSSH) läuft. Sie benötigen wenige Schritte, um mit PuTTY einen SSH-Tunnel aufzubauen:

Category • Session (Abbildung 10.55): Tragen Sie bei Host Name die IP-Adresse oder den Rechnernamen ein. Im Feld Port ist der Standardwert 22 vorbelegt. Tragen Sie hier einen davon abweichenden Wert ein, wenn notwendig. Damit Sie Ihre Sitzungsdaten speichern können, vergeben Sie einen Namen im Feld Saved Sessions. Klicken Sie dann auf Save.

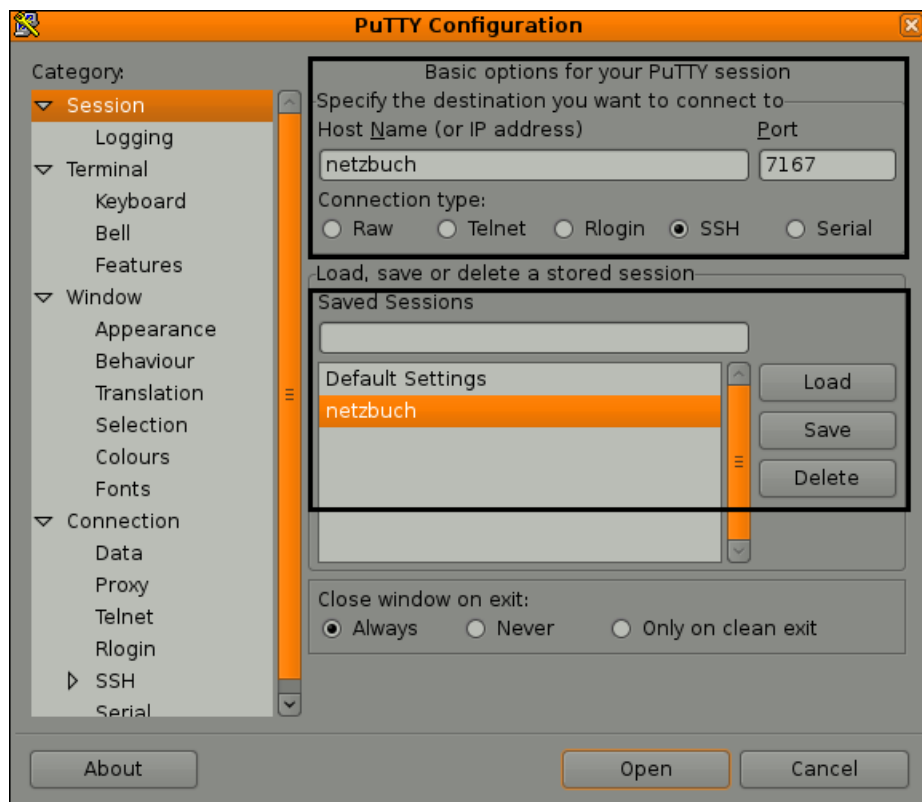


Abbildung 10.55 PuTTY: Menü »Session«

Category • Connection • Data (Abbildung 10.56): Behalten Sie die im Bild gezeigten Vorgaben bei. Sie können hier einen abweichenden Benutzernamen oder den SSHLogin-Prompt einstellen.

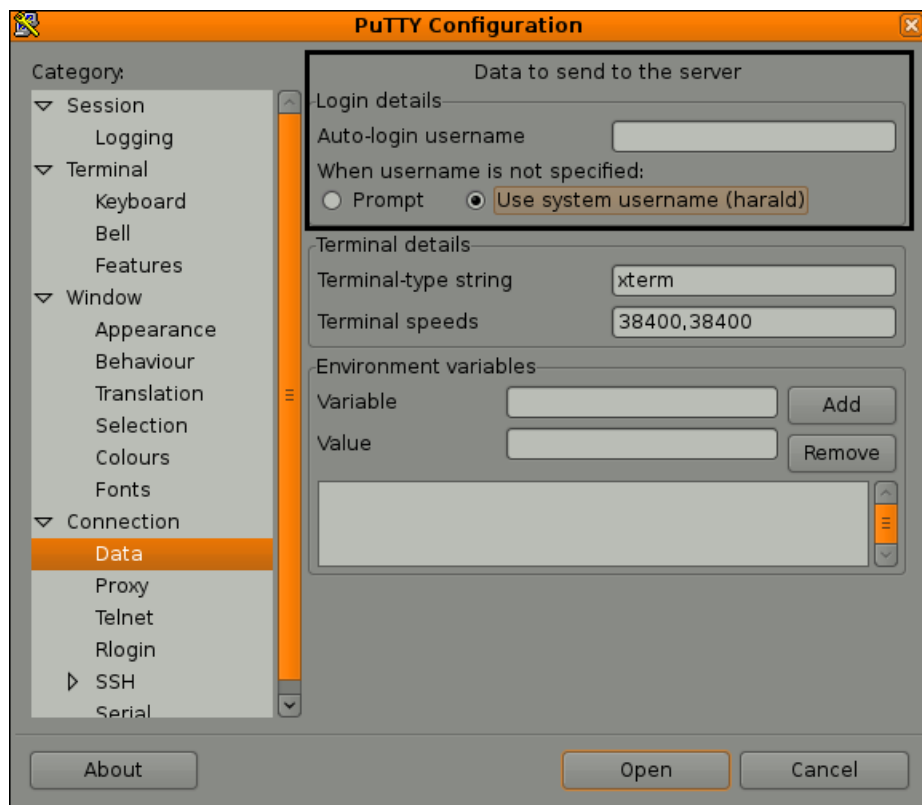


Abbildung 10.56 PuTTY: Menü »Connection • Data«

Category • SSH • Tunnels (Abbildung 10.57): Tragen Sie im Feld Source port den Port ein, auf den Sie mit Ihrer Anwendung zugreifen möchten. In das Feld Destination

schreiben Sie den entfernten Rechner und dessen Port, getrennt durch den Doppelpunkt. Klicken Sie anschließend auf Add.

Category • Session: Markieren Sie in der Auswahl Saved Sessions die eben neu angelegte Session. Klicken Sie anschließend auf Save. Die Verbindungseinstellungen sind damit gespeichert.

Category • Session (Abbildung 10.58): Klicken Sie auf die Schaltfläche Open. Die Verbindung zum entfernten Rechner wird aufgebaut. Geben Sie im kleinen Fenster, das PuTTY geöffnet hat, gegebenenfalls Ihren Benutzernamen und Ihr Kennwort oder nur das Kennwort ein. Starten Sie Ihre Anwendung, und übergeben Sie dieser auch die abweichende Port-Nummer (z. B. `http://localhost:8080`). Sie beenden die Tunnelverbindung, indem Sie sich in dem PuTTY-Terminalfenster mit `exit` abmelden. Sie können die Verbindung bei einem Neustart von PuTTY wieder aufrufen, indem Sie im Menü Session in der Auswahl von Saved Sessions Ihre Einstellungen markieren und mit Load aktivieren.

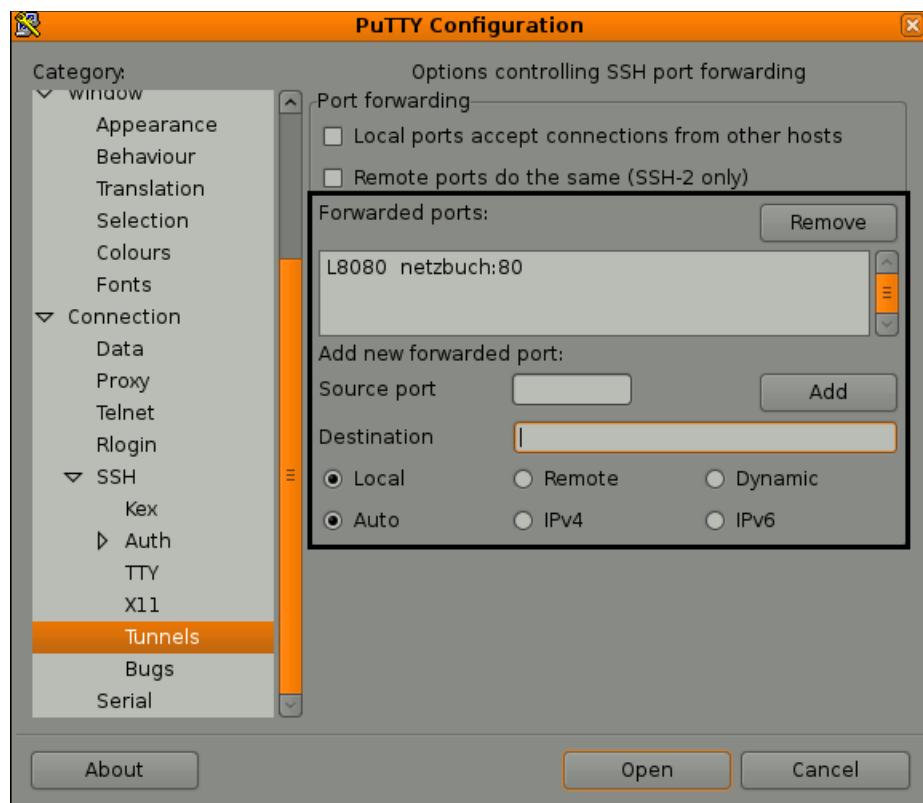


Abbildung 10.57 PuTTY: Menü »SSH • Tunnels«

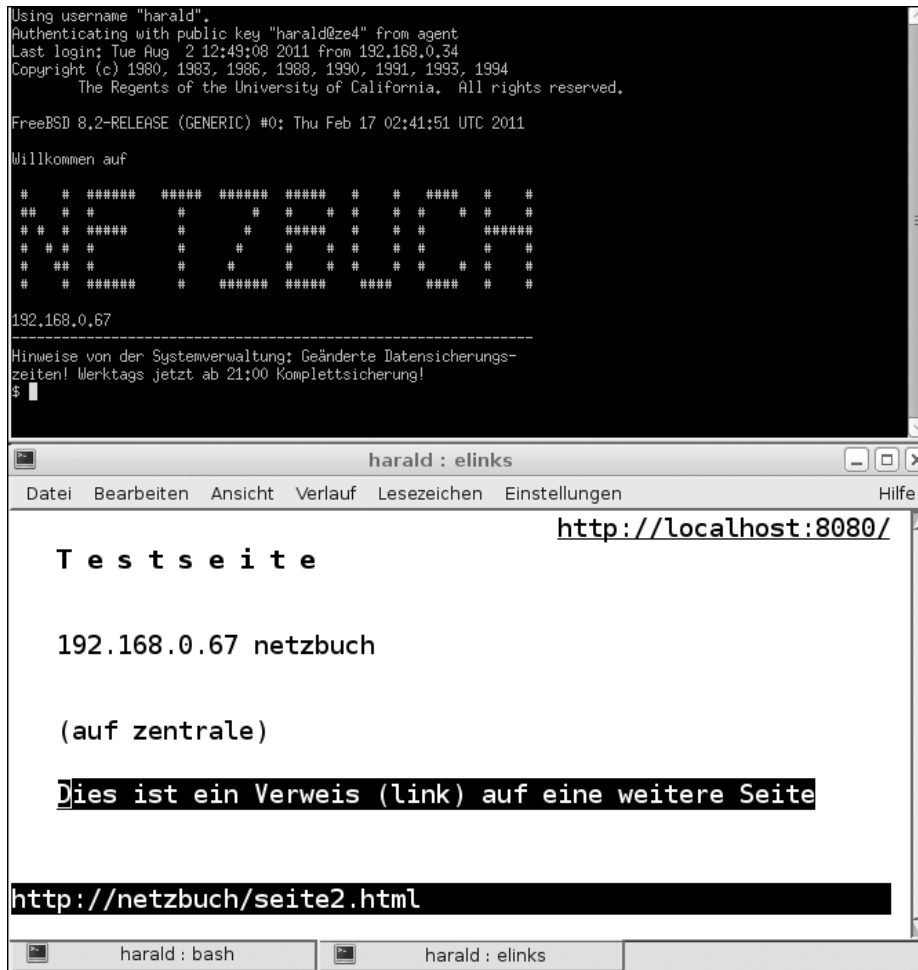
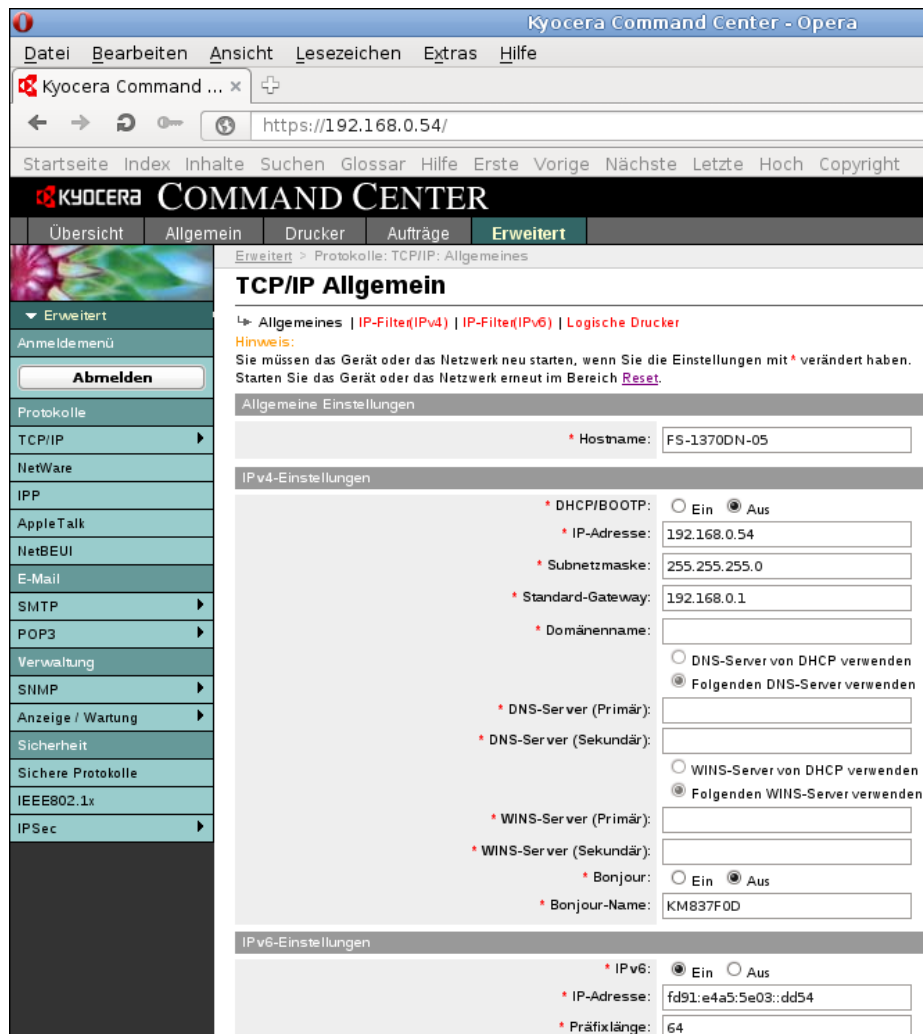


Abbildung 10.58 PuTTY-Terminalfenster (oben) und durch Tunnel geleitete HTTP-Sitzung (unten)

10.6.5 Sichere Konfiguration von Printservern

Als Beispielgerät dient der FS-1370DN von Kyocera. Dessen Printserver können Sie bequem über eine Weboberfläche konfigurieren. Sie sehen die Konfigurationsschritte für ein lokales Netz, in dem ausschließlich TCP/IP zum Einsatz kommt. Der Drucker bekommt je eine feste IP-Adresse für IPv4 und IPv6. Stellen Sie am Bedienfeld des Druckers eine für Sie erreichbare Adresse ein. Rufen Sie das Konfigurationsmenü dieses Geräts unter dieser Adresse mit Ihrem Webbrowser auf. Vergeben Sie endgültig verwendete IP-Adressen im Menü Erweitert • TCP/IP • Allgemein (Abbildung 10.59). Deaktivieren Sie auch Bonjour in dieser Maske.



Kyocera Command Center - Opera

Datei Bearbeiten Ansicht Lesezeichen Extras Hilfe

Kyocera Command ... x

https://192.168.0.54/

Startseite Index Inhalte Suchen Glossar Hilfe Erste Vorige Nächste Letzte Hoch Copyright

KYOCERA COMMAND CENTER

Übersicht Allgemein Drucker Aufträge **Erweitert**

Erweitert > Protokolle: TCP/IP: Allgemeines

TCP/IP Allgemein

↳ Allgemeines | IP-Filter(IPv4) | IP-Filter(IPv6) | Logische Drucker

Hinweis:
Sie müssen das Gerät oder das Netzwerk neu starten, wenn Sie die Einstellungen mit * verändert haben. Starten Sie das Gerät oder das Netzwerk erneut im Bereich [Reset](#).

Allgemeine Einstellungen

* Hostname: FS-1370DN-05

IPv4-Einstellungen

* DHCP/BOOTP: ☐ Ein ☒ Aus

* IP-Adresse: 192.168.0.54

* Subnetzmaske: 255.255.255.0

* Standard-Gateway: 192.168.0.1

* Domänenname:

☐ DNS-Server von DHCP verwenden
☒ Folgenden DNS-Server verwenden

* DNS-Server (Primär):

* DNS-Server (Sekundär):

☐ WINS-Server von DHCP verwenden
☒ Folgenden WINS-Server verwenden

* WINS-Server (Primär):

* WINS-Server (Sekundär):

* Bonjour: ☐ Ein ☒ Aus

* Bonjour-Name: KM837F0D

IPv6-Einstellungen

* IPv6: ☒ Ein ☐ Aus

* IP-Adresse: fd91:e4a5:5e03::dd54

* Präfixlänge: 64

Abbildung 10.59 Vergabe der IP-Adressen

Sie können in die Untermenüs IP-Filter(IPv4) und IP-Filter(IPv6) wechseln und den Zugriff auf ausgewählte Rechner festlegen (Abbildung 10.60). Für die Rechner selbst bestimmen Sie, wie diese den Drucker erreichen dürfen. Lassen Sie vor allem unverschlüsselte Verfahren deaktiviert. Die Zugriffsbeschränkung hat weniger Sicherheitsgründe. Vielmehr verhindern Sie die Benutzung von Geräten mit hohen Verbrauchskosten wie Farbdrucker.

The image shows two screenshots of the KYOCERA COMMAND CENTER web interface. The top screenshot displays the 'IP-Filter(IPv4)' configuration page. The bottom screenshot displays the 'IP-Filter(IPv6)' configuration page. Both pages show a left sidebar with navigation options and a main content area with filter settings.

Top Screenshot: IP-Filter(IPv4)

Header: KYOCERA COMMAND CENTER, FS-1370DN, Status: OK

Navigation: Übersicht, Allgemein, Drucker, Aufträge, **Erweitert**

Left Sidebar: Erweitert, Anmelden, Abmelden, Protokolle, TCP/IP, NetWare, IPP, AppleTalk, NetBEUI, E-Mail, SMTP, POP3, Verwaltung, SNMP, Anzeige / Wartung, Sicherheit, Sichere Protokolle, IEEE802.1x, IPSec

Breadcrumb: Erweitert > Protokolle: TCP/IP: IP-Filter(IPv4)

IP-Filter(IPv4)

↳ [Allgemeines](#) | [IP-Filter\(IPv4\)](#) | [IP-Filter\(IPv6\)](#) | [Logische Drucker](#)

Hinweis:
Wenn keine Einträge vorhanden sind, ist Zugriff auf alle gestattet.
Um den Zugriff auf ein Netzwerk zu gestatten, geben Sie die Netzwerk-IP-Adresse (IPv4) und die Subnetzmaske ein.
Um Zugriff auf eine einzelne IP-Adresse zu erlauben, geben Sie die IP-Adresse und 255.255.255.255 als Subnetzmaske ein.
Sie müssen das Gerät oder das Netzwerk neu starten, wenn Sie die Einstellungen mit * verändert haben.
Starten Sie das Gerät oder das Netzwerk erneut im Bereich [Reset](#).

Filter 1

* IP-Adresse (IPv4):

* Subnetzmaske:

* Protokolle: ☐ LPD ☐ FTP ☐ IPP ☐ HTTP ☐ RAW Port
☐ SNMP ☐ IPP over SSL ☐ HTTPS

Filter 2

* IP-Adresse (IPv4):

* Subnetzmaske:

* Protokolle: ☐ LPD ☐ FTP ☐ IPP ☐ HTTP ☐ RAW Port
☐ SNMP ☐ IPP over SSL ☐ HTTPS

Bottom Screenshot: IP-Filter(IPv6)

Header: KYOCERA COMMAND CENTER, FS-1370DN, Status: OK

Navigation: Übersicht, Allgemein, Drucker, Aufträge, **Erweitert**

Left Sidebar: Erweitert, Anmelden, Abmelden, Protokolle, TCP/IP, NetWare, IPP, AppleTalk, NetBEUI, E-Mail, SMTP, POP3, Verwaltung, SNMP, Anzeige / Wartung, Sicherheit, Sichere Protokolle, IEEE802.1x, IPSec

Breadcrumb: Erweitert > Protokolle: TCP/IP: IP-Filter(IPv6)

IP-Filter(IPv6)

↳ [Allgemeines](#) | [IP-Filter\(IPv4\)](#) | [IP-Filter\(IPv6\)](#) | [Logische Drucker](#)

Hinweis:
Wenn keine Einträge vorhanden sind, ist Zugriff auf alle gestattet.
Um den Zugriff auf ein Netzwerk zu gestatten, geben Sie die Netzwerk-IP-Adresse (IPv6) und die Präfixlänge ein.
Sie müssen das Gerät oder das Netzwerk neu starten, wenn Sie die Einstellungen mit * verändert haben.
Starten Sie das Gerät oder das Netzwerk erneut im Bereich [Reset](#).

Filter 1

* IP-Adresse (IPv6):

* Präfixlänge:

* Protokolle: ☐ LPD ☐ FTP ☐ IPP ☐ HTTP ☐ RAW Port
☐ SNMP

Filter 2

* IP-Adresse (IPv6):

* Präfixlänge:

* Protokolle: ☐ LPD ☐ FTP ☐ IPP ☐ HTTP ☐ RAW Port
☐ SNMP

Abbildung 10.60 Einschränkung des Zugriffs

Deaktivieren Sie jetzt alle weiteren Protokolle. Dazu wechseln Sie in das Menü Allgemein

- Gerätesicherheit
- Netzwerksicherheit

und wählen bei den nicht benötigten Diensten und Protokollen die Option Sperren. Insbesondere HTTP und FTP sollten Sie sperren (Abbildung 10.61).

KYOCERA COMMAND CENTER

Übersicht **Allgemein** Drucker Aufträge Erweitert

Allgemein > Sicherheit: Gerätesicherheit: Netzwerksicherheit

Netzwerksicherheit

↳ Allgemeines | Schnittstellen Sperre | Netzwerksicherheit

Hinweis:
Sie müssen das Gerät oder das Netzwerk neu starten, wenn Sie die Einstellungen mit * verändert haben. Starten Sie das Gerät oder das Netzwerk erneut im Bereich [Reset](#).

Einstellungen

* SNMPv3:	☒ Sperren ☐ Entsperren
* NetWare:	☒ Sperren ☐ Entsperren
* AppleTalk:	☒ Sperren ☐ Entsperren
* NetBEUI:	☒ Sperren ☐ Entsperren
* Raw:	☐ Sperren ☒ Entsperren
* IPP:	☒ Sperren ☐ Entsperren
* IPP over SSL:	☒ Sperren ☐ Entsperren
* HTTP:	☒ Sperren ☐ Entsperren
* HTTPS:	☐ Sperren ☒ Entsperren
* FTP:	☒ Sperren ☐ Entsperren
* SNMP:	☐ Sperren ☒ Entsperren
SMTP:	☒ Sperren ☐ Entsperren
POP3:	☒ Sperren ☐ Entsperren
* LPD:	☐ Sperren ☒ Entsperren
* WSD-Druck:	☐ Sperren ☒ Entsperren

Abbildung 10.61 Netzwerksicherheit einstellen, Sperren nicht benötigter Protokolle

Unter Allgemein • Passwortänderung vergeben Sie ein neues, sicheres Kennwort. Legen Sie unter Allgemein • Gerätesicherheit • Allgemeines fest, ob Sie das Bedienfeld generell, teilweise oder überhaupt nicht verriegeln. Über eine offene USB-Schnittstelle am Drucker kann ein versierter Angreifer einen Datenaustausch mit dem ansonsten geschützten Netz vornehmen. Verriegeln Sie deshalb USB-Gerät und -Host (Allgemein • Gerätesicherheit • Schnittstellen Sperre), wie in Abbildung 10.62 gezeigt.

Abbildung 10.62 Sperre der USB-Schnittstelle

10.6.6 Sicherer E-Mail-Verkehr

Üblicherweise werden E-Mails ohne Verschlüsselung versandt. Sie können auf dem Transportweg von jedem mitgelesen werden, wie beispielsweise eine Postkarte. Außerdem sind E-Mail-Clients (MUAs) oft Ziel von Angriffen. Adressbücher werden kopiert, und die darin enthaltenen E-Mail-Adressen werden von Spam-Versendern benutzt. Schadsoftware findet über den unsicheren MUA Wege, ihre Wirkung zu entfalten. Und – unerwünschte E-Mails kommen nicht nur von außen! Auch von der sicheren Seite aus verlassen vertrauliche Informationen das Haus. Tabelle 10.8 zeigt Ihnen Möglichkeiten, um diesen Problemen wenigstens etwas abzuwehren. In jedem Betrieb oder Haushalt herrschen individuelle Problemstellungen und verlangen nach eigenen Lösungen. Deshalb kann ich hier nur ganz allgemein gehaltene Anregungen geben.

Problem	Abhilfe
Mitlesen von E-Mail-Inhalten	1. E-Mail-Text verschlüsseln. Leider existieren keine einheitlichen Verfahren, weshalb Sie das Vorgehen mit der Empfängerseite absprechen müssen. 2. Ausschließlich E-Mail per HTTPS-Webmail abwickeln. Die Verbindung der Browser zum Server ist verschlüsselt. Voraussetzung für eine hohe Sicherheit ist, dass Sie »Herr des Mail-Servers« sind.

Tabelle 10.8 Den Gefahren des E-Mail-Verkehrs begegnen

Problem	Abhilfe
	3. Inhalte in Anlagen verbergen, <i>Steganografie</i> . Hier verstecken Sie den Nachrichtentext in einer Bild-, Sound- oder Videodatei. Die »offizielle« Nachricht enthält belanglose Inhalte.
Adressbücher werden durch Dritte ausgelesen.	Von bekanntermaßen mit diesen Problemen behafteten MUA-Programmen auf »robustere« Produkte wechseln oder eine lokale, vom Programm unabhängige Datenbank einsetzen
Im E-Mail-Header stehen alle Empfänger einer E-Mail.	Jeder Empfänger wird als BCC (Blindkopie) eingetragen.
Schadsoftware in E-Mails	1. keine HTML-Mails akzeptieren 2. Anhänge speichern und gegebenenfalls durch Antivirenprogramme untersuchen lassen 3. für die E-Mail-Anwendung einen eigenen, schwach privilegierten Benutzer anlegen
Vertrauliche Inhalte können das »Haus« verlassen.	1. Deep-Packet-Inspektion für E-Mails und Webzugriff 2. Mails zwischenlagern und freigeben durch Kontrollperson des E-Mail-Ausgangs

Tabelle 10.8 Den Gefahren des E-Mail-Verkehrs begegnen (Forts.)

10.6.7 Sicherer Internetzugang mit IPv6

Datenschützer befürchten eine verstärkte Benutzerverfolgung (Tracking) mit der Einführung von IPv6. Adress- und Datensammler können mit IPv6 leichter Profile über das Nutzerverhalten aufbauen und einem Anschluss zuordnen. Im Jahre 2014 gaben einige Provider hierzu Absichtserklärungen ab, dem Kunden gegebenenfalls auf Wunsch die gewohnte Anonymität aus IPv4-Zeiten zurückzugeben. Zum Zeitpunkt der Überarbeitung dieses Buches war leider keine konkrete Umsetzung in der Praxis zu sehen. Manche Provider äußerten die Überlegung, dass wohl eine Zeit lang eine Dualstack-Lösung (IPv4 + IPv6) angeboten werden könnte.

Neben dem Präfix können Sie auch den Interface Identifier (MAC-Adresse) verschleiern.

Die Adresse wird beim Einsatz der *Privacy Extension* per *Stateless Address Autoconfiguration*

(SLAAC) vergeben und nicht per DHCP oder Festvergabe. Der Geräteteil der IPv6-Adresse wird dabei nicht mehr in Abhängigkeit von der MAC-Adresse erzeugt. Bei einigen Betriebssystemen geschieht dies automatisch, bei manchen per manuellem Konfigurationsschritt (Tabelle 10.9).

System	Maßnahme	Aktivierung
Windows	keine notwendig, ab Windows XP vorhanden; Kontrolle: netsh interface ipv6 show privacy	automatisch aktiv
Linux	Eintrag in <code>/etc/sysctl.conf</code> : net.ipv6.conf.default.use_tempaddr = 2 net.ipv6.conf.default.temp_valid_lft = 86400 net.ipv6.conf.default.temp_preferred_lft = 86400	manuell
OS X	Benutzen des Programms IPv6 Anonymizer (www.heise.de/download/ipv6-anonymizer-1179954.html)	manuell
OpenWRT (Router)	Skript installieren, siehe Artikel auf www.heise.de/netze/artikel/OpenWRT-wuerfelt-IPv6-Praefixe-1445607.html	manuell
FreeBSD	Absetzen folgender Kommandos: sysctl net.inet6.ip6.use_tempaddr=1 sysctl net.inet6.ip6.prefer_tempaddr=1	manuell

Tabelle 10.9 Maßnahmen zur Erzeugung einer MAC-unabhängigen IPv6-Adresse (Geräteteil)

10.6.8 Mit Portknocking Brute Force-Angriffe vermeiden

Ein offener SSH-Port ruft bei seinem Entdecker natürlich den Wunsch nach »mehr« hervor. Ein Brute Force-Angriff wird gestartet, und dies kann durchaus von Erfolg gekrönt sein.

Mit dem als *Portknocking* bezeichneten Verfahren wird der gewünschte Port erst geöffnet, wenn eine definierte Reihe von Ports am Zielsystem Datenpakete empfängt. Alternativ können anstelle der Firewall-Anweisung auch andere Aktionen ausgelöst werden. So könnten Sie damit überhaupt den SSH-Daemon starten und nach getaner Arbeit wieder beenden.

Unter Linux installieren Sie dabei das `knockd`-Paket. Dieses enthält auch die notwendige »Fernbedienung«.

Was beim Anklopfen geschehen soll, wird in der Datei `/etc/knockd.conf` bestimmt. In der Grundausstattung hat diese folgenden Inhalt:

Ausgangszustand der Datei »/etc/knockd.conf«

```
[options]
  UseSyslog
[openSSH]
  sequence = 7000,8000,9000
  seq_timeout = 5
  command = /sbin/iptables -A INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
  tcpflags = syn
[closeSSH]
  sequence = 9000,8000,7000
  seq_timeout = 5
  command = /sbin/iptables -D INPUT -s %IP% -p tcp --dport 22 -j ACCEPT
  tcpflags = syn
```

Sie können recht einfach testen, ob der Dienst an sich funktioniert. Fertigen Sie eine Sicherungskopie von `/etc/knockd.conf` an. Anschließend ändern Sie das Original auf diesen Inhalt ab:

Änderungen der Datei

```
[options]
  UseSyslog
[openSSH]
  sequence = 7000,8000,9000
  seq_timeout = 5
  command = /usr/bin/wall "Einschalten"
  tcpflags = syn
[closeSSH]
  sequence = 9000,8000,7000
  seq_timeout = 5
  command = /usr/bin/wall "Ausschalten"
  tcpflags = syn
```

Damit sehen Sie am Terminal, ob die Signalisierung funktioniert. Das `wall`-Kommando übermittelt Nachrichten an alle Terminale eines Linux-Systems und eignet sich daher wunderbar als Testkandidat.

Starten Sie nun den `knockd`-Daemon und klopfen von »außen« an. Dazu müssen Sie die Reihenfolge der Port-Nummern und das Protokoll, also TCP oder UDP, angeben. Standard ist TCP mit SYN-Paketen. So könnte der Eintrag `sequenze` auch `sequenze = PORT1:tcp, PORT2:udp:PORT3:tcp` lauten.

Hier für das Beispiel im Buch lautet die Eingabe von einem anderen Rechner aus:

```
knock IP-Adresse PORT1:PROTOKOLL PORT2:PROTOKOLL PORT3:PROTOKOLL.
```

Die Abbildung 10.63 zeigt Ihnen den Ablauf in der Praxis. Das obere Terminal ist hierbei der »Anklopfer«, das untere zeigt das Geschehen am Zielsystem.



Abbildung 10.63 Testen des Portknockings

Wenn dies so funktioniert, kopieren Sie die ursprüngliche Konfigurationsdatei wieder zurück und nehmen darin Ihre Feineinstellungen vor.

10.7 Prüf- und Diagnoseprogramme für Netzwerke

Prüfen Sie Ihr Netzwerk regelmäßig. Finden Sie unerwünscht offene Ports heraus. Klären Sie Fehler mithilfe einer Datenanalyse.

10.7.1 Rechtliche Hinweise

Werkzeuge sind nicht »gut« oder »böse«. In den falschen Händen sind sie aber gefährlich. Seien Sie sich dessen bewusst, und installieren Sie sie nicht in Standardverzeichnisse (sondern außerhalb der *Path*-Variable liegend). Setzen Sie diese Werkzeuge nur zum Überprüfen der eigenen Systeme ein. Lassen Sie sich von Kunden am besten einen schriftlichen Auftrag geben, wenn Sie deren Systeme damit prüfen sollen.

10.7.2 Verbindungen mit »netstat« anzeigen

Mit `netstat` ermitteln Sie TCP-Sockets, Verbindungen und Routen am eigenen Rechner. Sie erkennen eventuell aktive Schadsoftware, die über das Netzwerk kommuniziert. Sie können sich die Gegenstellen, Prozess-IDs und Benutzer zu den Verbindungen anzeigen

lassen. Eine Auflistung aller aktiven Netzwerkschnittstellen mit einer Nutzungsstatistik hilft Ihnen, Fehlfunktionen im Netzwerk zu finden. Das Programm kann von Ihnen auch mit laufend aktualisierender Anzeige aufgerufen werden. Ich zeige Ihnen einige Beispiele für Ihre Praxis (Tabelle 10.10).

Aktion	Eingabe	Beispiel
Auflistung von Routen	<code>netstat -r</code>	1
Auflistung der Netzwerkschnittstellen	<code>netstat -i</code>	2
Auflistung aller TCP/UDP-Ports	<code>netstat -lptun</code>	3
Anzeigen statistischer Angaben	<code>netstat -s</code>	4
Anzeigen offener Ports	<code>netstat -atup</code>	5

Tabelle 10.10 Abfragen mit »netstat«

Beispiel 1: Sie fragen mit der Option `-r` die Routing-Einträge ab. Genauere Informationen finden Sie in Abschnitt 4.7.3, »Routing-Tabelle abfragen (>netstat)<«. Dort finden Sie die Ausführungen zur Ausgabe der Routen.

Beispiel 2: Bei der Auflistung der Netzwerkschnittstellen zeigt `netstat` Ihnen die gesetzten Werte für MTU und Metric an. Sie erhalten die Zahlen erfolgreich gesendeter und empfangener Pakete sowie die von fehlerhaften Vorgängen.

Beispiel 3: Mit dieser kombinierten Anweisung erhalten Sie umfangreiche Informationen über offene TCP- und UDP-Ports:

- l: empfangsbereite Serversockets
- p: Die Prozess-IDs und die Namen von Programmen werden angezeigt.
- t: TCP-Verbindungen
- u: UDP-Verbindungen
- n: Anstelle von Host-Namen erhalten Sie IP-Adressen angezeigt.

Beispiel 4: Sie erhalten umfangreiche statistische Angaben zum Netzwerkgeschehen auf Ihrem Rechner. Sie erkennen eventuelle Probleme bei der Netzlast.

Beispiel 5: Mit `-a` fordern Sie alle Ports an, nicht nur jene mit einer Verbindung (die restlichen Optionen finden Sie bei Beispiel 3). Diese Liste hilft Ihnen, nicht benötigte Netzwerkanwendungen oder auch Schadsoftware zu entdecken und zu entfernen. Die Ausgabe dieses Befehls finden Sie in Abbildung 10.64.

```

root@ze4:~# netstat -atup
Aktive Internetverbindungen (Server und stehende Verbindungen)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 *:sunrpc                *:*                     LISTEN      1047/portmap
tcp        0      0 *:ssh                   *:*                     LISTEN      2155/sshd
tcp        0      0 localhost:ipp           *:*                     LISTEN      1774/cupsd
tcp        0      0 localhost:postgresql    *:*                     LISTEN      1683/postmaster
tcp        0      0 localhost:smtp          *:*                     LISTEN      2160/exim4
tcp        0      0 *:57768                 *:*                     LISTEN      1066/rpc.statd
tcp6       0      0 [::]:ssh                [::]:*                  LISTEN      2155/sshd
tcp6       0      0 localhost:ipp           [::]:*                  LISTEN      1774/cupsd
tcp6       0      0 localhost:postgresql    [::]:*                  LISTEN      1683/postmaster
tcp6       0      0 localhost:smtp          [::]:*                  LISTEN      2160/exim4
udp        0      0 *:sunrpc                *:*                     LISTEN      1047/portmap
udp        0      0 *:ipp                   *:*                     LISTEN      1774/cupsd
udp        0      0 *:60452                 *:*                     LISTEN      1471/avahi-daemon:
udp        0      0 *:36006                 *:*                     LISTEN      1066/rpc.statd
udp        0      0 *:818                   *:*                     LISTEN      1066/rpc.statd
udp        0      0 *:bootpc                *:*                     LISTEN      2199/dhclient
udp        0      0 *:mdns                  *:*                     LISTEN      1471/avahi-daemon:
udp6       0      0 [::]:40329              [::]:*                  LISTEN      1471/avahi-daemon:
udp6       0      0 localhost:35088         localhost:35088         VERBUNDEN   1683/postmaster
udp6       0      0 [::]:mdns                [::]:*                  LISTEN      1471/avahi-daemon:
root@ze4:~#

```

Abbildung 10.64 Liste offener Ports

Weitere Ausführungen zu `netstat` finden Sie in Abschnitt 6.3.3, »Ports und Sicherheit«.

10.7.3 Hosts und Ports mit »nmap« finden

Mittels `nmap` gewinnen Sie viele Informationen über Ihr Netzwerk und die daran angeschlossenen

Hosts. Sie erfahren, welche Hosts in Ihrem Netzwerk aktiv sind und welche Ports an diesen offen sind. Lesen Sie unbedingt die umfangreiche Manual-Seite dieses

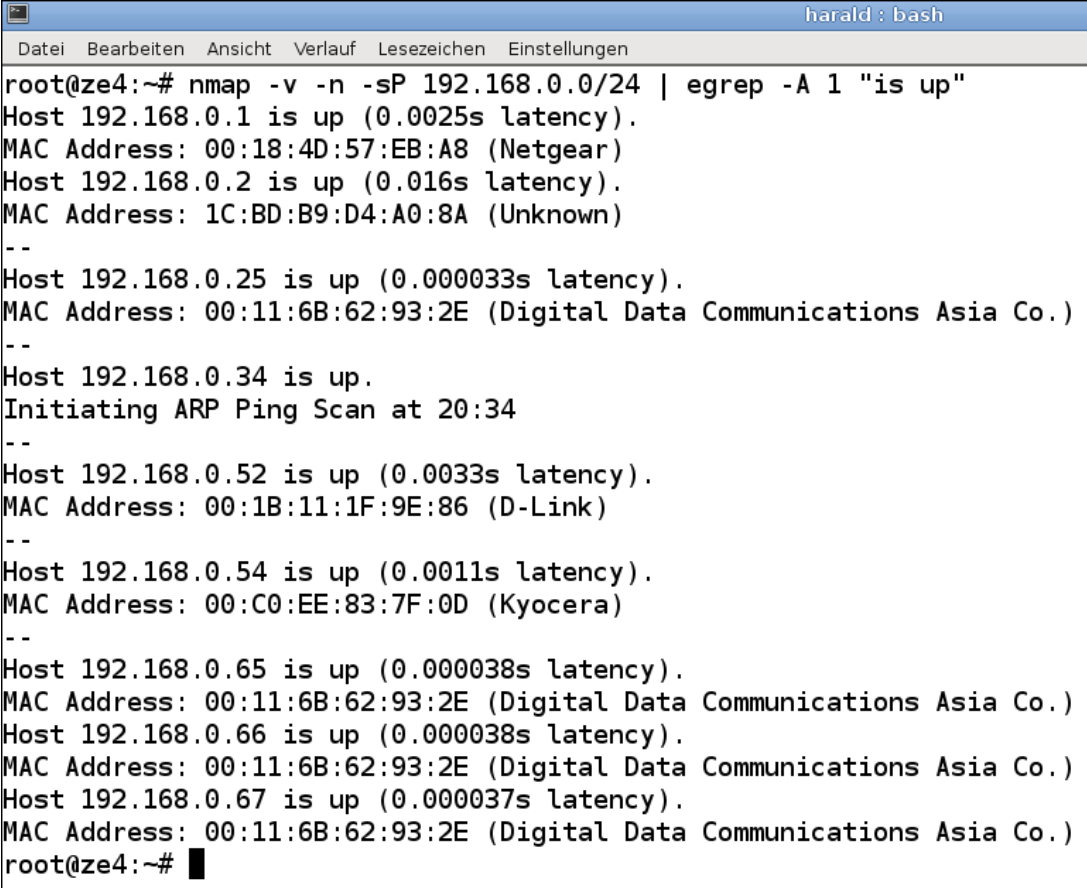
Programms.

Ich greife hier nur wenige Anwendungsszenarien heraus. Eines davon zeigt, wie Sie sich eine Übersicht über im LAN aktive Geräte verschaffen. Sie bekommen neben der IP-Adresse die MAC-Adresse. Damit können Sie unter Umständen schon ungebetene Gäste erkennen.

Das Netzwerk geben Sie in der CIDR-Notation an. Die sonst recht unübersichtliche, weil umfangreiche Ausgabe filtern Sie mit `egrep`. Damit lassen Sie sich die übereinstimmenden und die jeweils darauf folgenden Zeilen anzeigen. Sie finden im ersten Beispiel folgende Optionen von `nmap`:

- v: ausführliche Ausgabe
- n: verzicht auf die Namensauflösung, zeigt nur die IP-Adresse an
- sP: Ping-Scan

In Abbildung 10.65 sehen Sie eine kleine Bestandsaufnahme eines lokalen Netzes.



```

harald : bash
Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
root@ze4:~# nmap -v -n -sP 192.168.0.0/24 | egrep -A 1 "is up"
Host 192.168.0.1 is up (0.0025s latency).
MAC Address: 00:18:4D:57:EB:A8 (Netgear)
Host 192.168.0.2 is up (0.016s latency).
MAC Address: 1C:BD:B9:D4:A0:8A (Unknown)
--
Host 192.168.0.25 is up (0.000033s latency).
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
--
Host 192.168.0.34 is up.
Initiating ARP Ping Scan at 20:34
--
Host 192.168.0.52 is up (0.0033s latency).
MAC Address: 00:1B:11:1F:9E:86 (D-Link)
--
Host 192.168.0.54 is up (0.0011s latency).
MAC Address: 00:C0:EE:83:7F:0D (Kyocera)
--
Host 192.168.0.65 is up (0.000038s latency).
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
Host 192.168.0.66 is up (0.000038s latency).
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
Host 192.168.0.67 is up (0.000037s latency).
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
root@ze4:~#

```

Abbildung 10.65 »nmap«: Inventur eines lokalen Netzwerks

Wenn Sie nur das Vorhandensein bestimmter Hosts kontrollieren wollen, verwenden Sie eine Liste. Diese Liste besteht aus IP-Adressen oder Rechnernamen und befindet sich in einer Textdatei. Im folgenden Beispiel werden IPv6-Hosts kontrolliert. Die neu verwendeten Optionen im folgenden Beispiel sind:

- 6: Bei den Angaben handelt es sich um IPv6-Adressen.
- iL <DATEI>: liest aus Datei <DATEI>

Die Ausgabe dieses abgewandelten Inventur-Scans sehen Sie in Abbildung 10.66.

```

harald : bash
Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
root@ze4:~# # I n h a l t  liste2.txt
root@ze4:~# cat liste2.txt
fd91:e4a5:5e03::dd05
fd91:e4a5:5e03::dd54
fd91:e4a5:5e03::dd04
fd91:e4a5:5e03::dd06
root@ze4:~# #
root@ze4:~# #
root@ze4:~# #
root@ze4:~# nmap -v -6 -n -sP -iL liste2.txt

Starting Nmap 5.00 ( http://nmap.org ) at 2011-08-04 20:49 CEST
NSE: Loaded 0 scripts for scanning.
Initiating Ping Scan at 20:49
Scanning 4 hosts [2 ports/host]
Completed Ping Scan at 20:49, 1.20s elapsed (4 total hosts)
Host fd91:e4a5:5e03::dd05 is up (0.000042s latency).
Host fd91:e4a5:5e03::dd54 is up (0.00064s latency).
Host fd91:e4a5:5e03::dd04 is up (0.00019s latency).
Host fd91:e4a5:5e03::dd06 is down.
Nmap done: 4 IP addresses (3 hosts up) scanned in 1.21 seconds
root@ze4:~# █

```

Abbildung 10.66 »nmap«: Ping-Scan auf eine IPv6-Adressen aus einer Liste

Zur Überprüfung eines einzelnen Hosts wählen Sie aus diesen Optionen:

- p<PORT-Anfang>-<PORT-Ende>: Festlegung des Port-Bereichs
- O: Ermittlung des Betriebssystems
- A: zusätzlich zur Ermittlung des Betriebssystems Ermittlung der Traceroute

Ohne weitere Angabe außer der des Rechnernamens oder der IP-Adresse erhalten Sie eine »kurze« Auskunft (Abbildung 10.67). In dieser Abbildung sehen Sie auch den erweiterten Scan (-A). In Abbildung 10.68 sehen Sie die Suche mit erweitertem Port-Bereich (-p). Wenn Sie die Option -A benutzen, versucht `nmap`, auch die erreichbaren Angaben zum Port darzustellen. Im Beispiel sehen Sie die Angaben zum HTTP- und SSH-Server.

Weitere Ausführungen zu `nmap` finden Sie auch in Abschnitt 6.7.2, »Durchführen von Portscans zum Austesten von Sicherheitsproblemen«.

In Abschnitt 6.7.3, »Schließen von Ports«, finden Sie Hinweise zum Schließen von offenen und nicht benötigten Ports.

```

harald : bash
Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
root@ze4:~# nmap -n 192.168.0.67

Starting Nmap 5.00 ( http://nmap.org ) at 2011-08-04 21:51 CEST
Interesting ports on 192.168.0.67:
Not shown: 999 closed ports
PORT      STATE SERVICE
80/tcp    open  http
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)

Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds
root@ze4:~#
root@ze4:~# nmap -n -A 192.168.0.67

Starting Nmap 5.00 ( http://nmap.org ) at 2011-08-04 21:51 CEST
Interesting ports on 192.168.0.67:
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      tthttpd 2.25b 29dec2003
|_ html-title: Site doesn't have a title (text/html; charset=iso-8859-1).
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
Device type: general purpose
Running: FreeBSD 7.X
OS details: FreeBSD 7.0-RELEASE-p1 - 7.1-RELEASE
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.14 seconds
root@ze4:~#

```

Abbildung 10.67 »nmap«: ohne und mit erweiterter Ausgabe

```

harald : bash
Datei Bearbeiten Ansicht Verlauf Lesezeichen Einstellungen
root@ze4:~# nmap -n -p1-9000 -A 192.168.0.67

Starting Nmap 5.00 ( http://nmap.org ) at 2011-08-04 21:57 CEST
Interesting ports on 192.168.0.67:
Not shown: 8998 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http      tthttpd 2.25b 29dec2003
|_ html-title: Site doesn't have a title (text/html; charset=iso-8859-1).
7167/tcp  open  ssh       OpenSSH 5.4p1 (FreeBSD 20100308; protocol 2.0)
|_ ssh-hostkey: 1024 1a:24:04:6a:25:9e:1b:45:27:f7:1c:a1:39:d5:0c:b8 (DSA)
|_ 2048 5f:ba:88:37:22:28:9d:dc:21:c6:fb:01:3a:e5:21:6f (RSA)
MAC Address: 00:11:6B:62:93:2E (Digital Data Communications Asia Co.)
Device type: general purpose
Running: FreeBSD 7.X
OS details: FreeBSD 7.0-RELEASE-p1 - 7.1-RELEASE
Network Distance: 1 hop
Service Info: OS: FreeBSD

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 55.73 seconds
root@ze4:~#

```

Abbildung 10.68 »nmap«: erweiterte Ausgabe mit vorgegebenem Port-Bereich

10.7.4 Datenverkehr protokollieren (Wireshark, tcpdump)

Mit *Wireshark* können Sie per Mausklick den Datenverkehr protokollieren und analysieren. Beim Programmstart legen Sie die Netzwerkschnittstelle fest, auf der das Programm lauscht. Wireshark ermöglicht auch den Zugriff auf alle vorhandenen Netzwerkkarten und den `localhost`.

Die Benutzeroberfläche (Abbildung 10.69) gliedert sich in vier Teile. Oben finden Sie die Programmleiste. Die protokollierten Daten werden in drei Ebenen dargestellt. Die untersuchten Pakete laufen zeilenweise, verschiedenfarbig gekennzeichnet, in der oberen Ebene durch. Sie können per Mausklick eine dieser Zeilen markieren. Im mittleren Feld klicken Sie links auf einen der Protokollpfeile. Die Daten werden im Klartext dargestellt. Das untere Feld gibt die Daten hexadezimal aus.

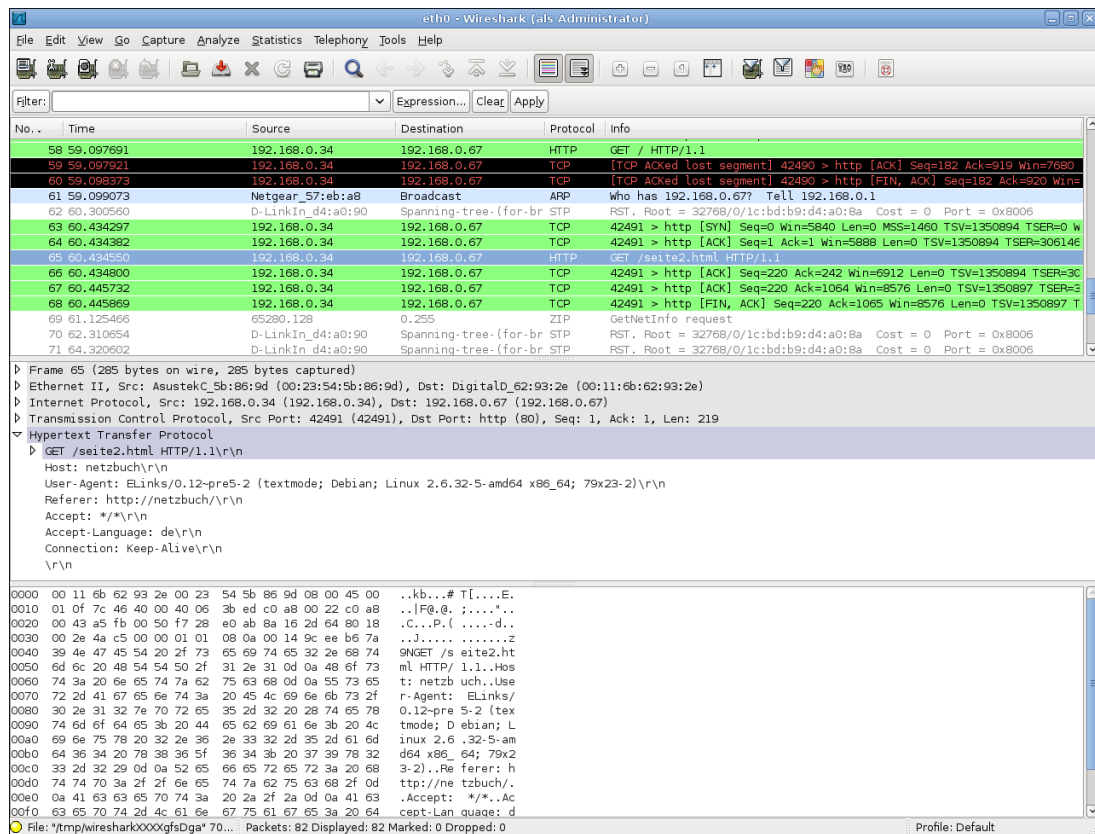


Abbildung 10.69 Wireshark

Sie können Scanläufe speichern und später auswerten. Damit können Sie erkennen, ob schon Programme im Netzwerk aktiv sind, und gegebenenfalls Gegenmaßnahmen ergreifen.

Mit `tcpdump` nehmen Sie die gleichen Tests wie mit Wireshark vor. Die Log-Dateien von `tcpdump` können Sie bequem per Mausklick mit Wireshark auswerten. Ich zeige Ihnen in Tabelle 10.11 einige wichtige Optionen.

Aktion	Option
Auflisten von Netzwerkgeräten (Abbildung 10.70)	-D
Festlegen des Netzwerkgeräts	-i <GERÄT>
Nur IP-Adressen anzeigen	-n
Mitschneiden von Ethernet-Headern	-e
Ausgabe eines Paketinhalts im ASCII-Format	-A
Angabe des Informationsgrads	-v -vv, -vvv
Port festlegen	port <PORT>
Port-Bereich festlegen	portrange <von-bis>
Log-Datei, in die <code>tcpdump</code> schreibt	-w <DATEI>

Tabelle 10.11 Wichtige Optionen von »tcpdump«

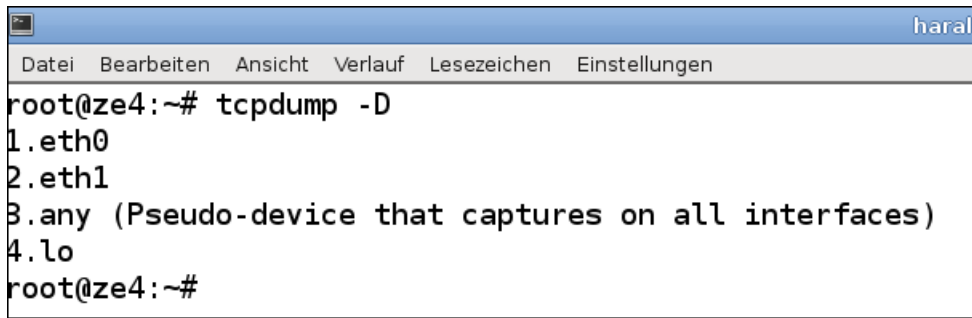


Abbildung 10.70 »tcpdump«: Auflistung der Netzwerkgeräte

Das Beispiel in Abbildung 10.71 zeigt Ihnen die Abfrage eines Browsers beim HTTP-Server. Damit können Sie eventuelle Angriffe entdecken.

Die von `tcpdump` erzeugten Daten können Sie im Shell-Skript oder auch später mit Wireshark auswerten. Das nächste Beispiel zeigt die Kommunikation zwischen einem Browser und dem HTTP-Server. Die Abfrage wird dabei auf den Port 80 begrenzt. Das Mitschnittprotokoll wird in einer Datei abgelegt. Das vollständige Kommando lautet:

```
tcpdump -n -vvv -A -i eth0 port 80 and dst 192.168.0.67 or dst 192.168.0.34  
-w ausgabe.dmp
```

Sie können die Ausgabedatei von `tcpdump` formatiert ausgeben lassen. Dazu geben Sie einfach `tcpdump -r <DATEI>` ein.

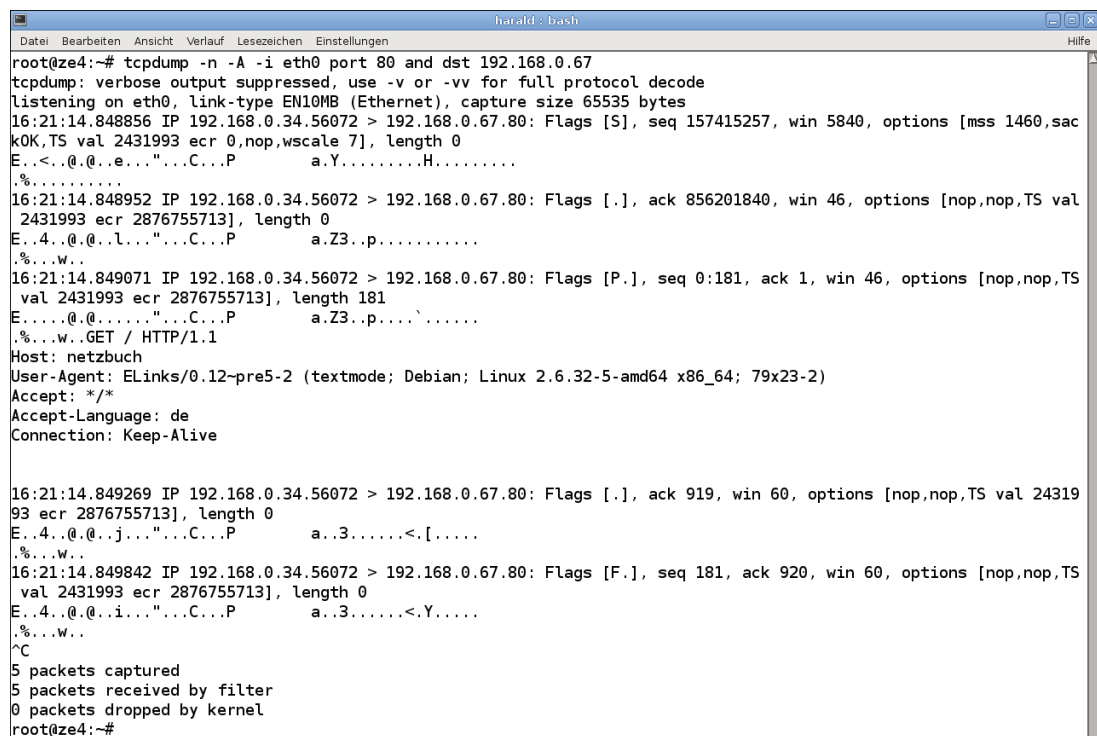


Abbildung 10.71 »tcpdump«: Protokollierung von Webbrowser-Anfragen

Lesen Sie weitere Informationen in der Manual-Seite von `tcpdump`.

10.7.5 Netzaktivitäten mit »darkstat« messen

Sie erhalten mit `darkstat` relativ schnell einen guten Überblick über die Auslastung Ihres Netzes. Das Programm selbst starten Sie in der Shell; die Anzeige erhalten Sie per Webbrowser. Um sämtlichen Verkehr Ihrer Rechner zu erfassen, starten Sie das Programm nur mit diesen Angaben:

```
darkstat -i eth0 -p 8080
```

Mit der Option `-i` geben Sie die Netzwerkschnittstelle an, mit `-p` den Port, auf den Sie

mittels Browser zugreifen. Wenn Sie eine Netzwerkadresse angeben möchten, verwenden Sie -1. Das Netzwerk geben Sie zusammen mit der ausgeschriebenen Subnetzmaske an. Möchten Sie nur ein bestimmtes Netz sehen, geben Sie z. B.

```
darkstat -i eth0 -l 192.168.0.0/255.255.255.0 -p 8080
```

ein.

In der Webanzeige erhalten Sie einen Graphen (Abbildung 10.72) und eine Liste der Hosts (Abbildung 10.73).

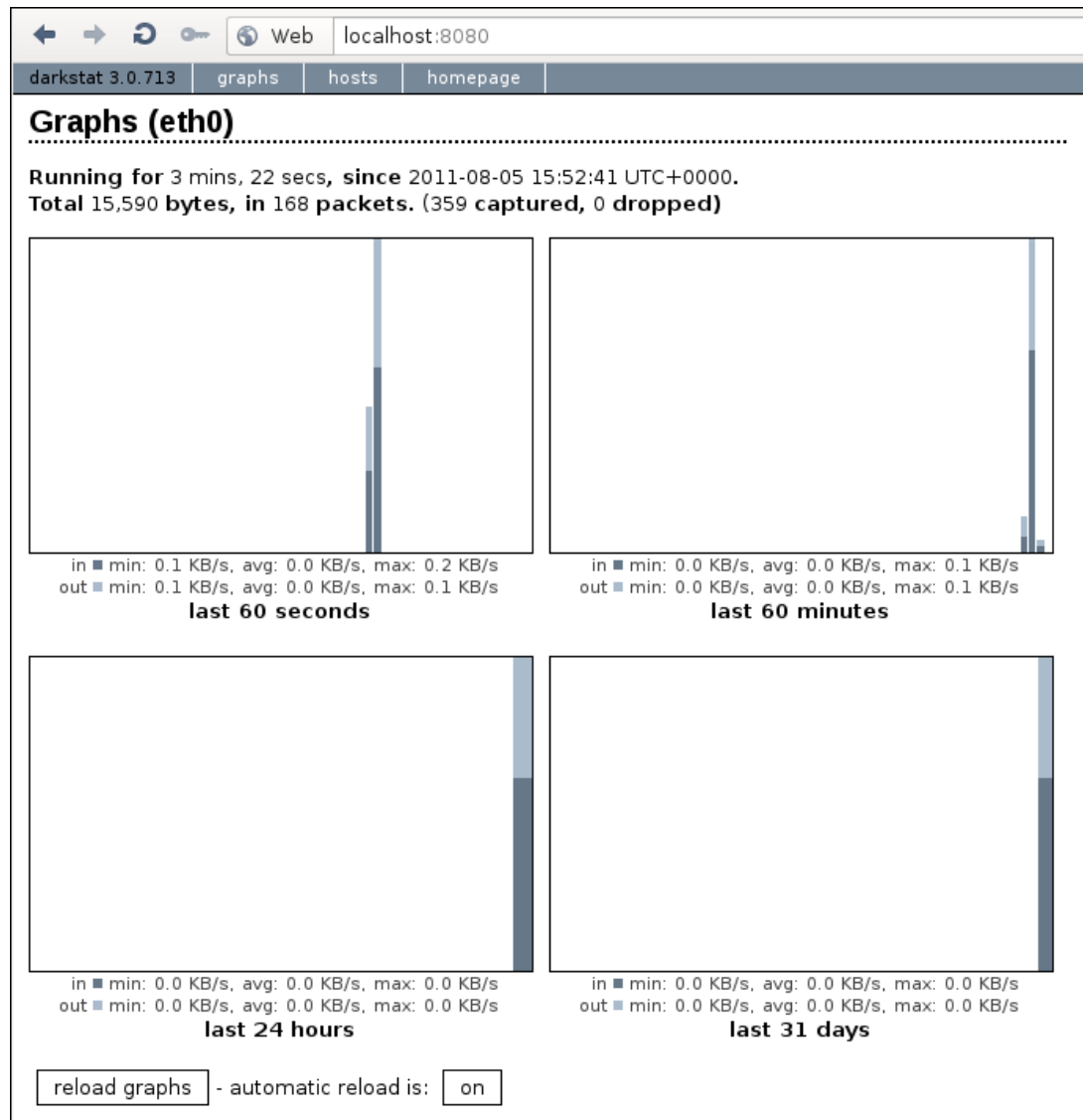


Abbildung 10.72 »darkstat«: Aktivitätsanzeige

IP	Hostname	MAC Address	In	Out	Total	Last seen
192.168.0.34	ze4	00:23:54:5b:86:9d	8,934	5,551	14,485	1 min, 34 secs
192.168.0.25	zentrale	00:11:6b:62:93:2e	3,960	7,828	11,788	2 mins, 32 secs
224.0.0.251	(Unknown host)	01:00:5e:00:00:fb	1,937	0	1,937	2 mins, 19 secs
192.168.0.1	(Unknown host)	00:18:4d:57:eb:a8	667	1,106	1,773	1 min, 34 secs
192.168.0.103	ze4.local	00:18:e7:16:71:30	0	1,013	1,013	2 mins, 19 secs
192.168.0.2	(Unknown host)	1c:bd:b9:d4:a0:8a	0	184	184	1 min, 1 sec
239.255.255.100	(Unknown host)	01:00:5e:7f:ff:64	184	0	184	1 min, 1 sec

Abbildung 10.73 »darkstat«: Liste der Hosts

10.7.6 Netzlast mit »fping« erzeugen

Wenn Sie z. B. mit `darkstat` eine Netzübersicht erzeugen wollen, müssen Sie so lange warten, bis jeder der angeschlossenen Hosts im selben Netz einmal aktiv war. Ohne Aktivität werden diese Geräte sonst nicht erfasst und tauchen damit nicht in der HostÜbersicht auf. Mit `fping` haben Sie das Werkzeug dafür. Sie können damit bei jedem Gerät »anklopfen«, sodass die gewünschte Aktivität entsteht. Der Aufruf hierfür lautet

```
fping -r 0 -aA -g 192.168.0.0/24
```

für das Netz 192.168.0.0. Anstelle der Subnetzmaske müssen Sie hier die CIDR-Schreibweise anwenden. Die einzelnen Optionen von `fping` bedeuten:

- r 0: Anzahl der Wiederholungen je Host. Im Beispiel versucht es `fping` einmal (ohne Wiederholungen).
- a: nur Hosts anzeigen, die geantwortet haben
- u: nur Hosts anzeigen, die unerreichbar sind
- A: keine Namensauflösung, nur IP-Adressen werden angezeigt.
- e: Anzeige der Round-Trip-Zeit
- s: bildet am Schluss eine zusammenfassende Statistik
- g <NETZADRESSE/CIDR>: Angabe des zu prüfenden Netzes

10.7.7 Weitere Einsatzmöglichkeiten von »fping«

Mit `fping` können Sie ohne großen Aufwand weitere Aufgaben erledigen. Das Programm dient als Datenquelle in Shell-Skripten. Es ermittelt Hosts, die entweder erreichbar oder nicht erreichbar sind. Ich zeige Ihnen hier ein Shell-Skript und einige Skriptfragmente als Anregung für Ihre tägliche Arbeit.

Das Shell-Skript (Listing 10.1) zeigt Ihnen alle erreichbaren Hosts innerhalb des angegebenen Netzwerks an. Im Ergebnis stehen auch die Zeitangaben. Am Schluss der Ausgabe finden Sie eine zusammenfassende Statistik. Die Anzeige lasse ich mit dem Programm `less` puffern. Sie können mit den Cursor-Tasten und zeilenweise blättern. Mit den Tasten (Bild AUF) und (Bild AB) bewegen Sie sich seitenweise. Möchten Sie das angezeigte Ergebnis speichern, drücken Sie die Taste (S) und geben einen Dateinamen an. Mit (Q) beenden Sie die Anzeige.

```
#!/bin/sh
# Eingabe der Netzwerkadresse
echo -n "Netzwerkadresse: ";read netz
echo "Ermittle Netzwerkteilnehmer....."

# Durchführen von fping und Umleitung der gesamten Ausgabe
# in Log-Datei
fping -r 0 -aA -e -s -g $netz/24 > fping.log 2>&1
# Anzeigen der Log-Datei ohne die nicht erreichten Hosts
cat fping.log | grep -v "ICMP Host" | less
```

Listing 10.1 Shell-Skript »netz4.sh«

Die Ausgabe sehen Sie in Abbildung 10.74.

```

192.168.0.2 (12.0 ms)
192.168.0.25 (1.24 ms)
192.168.0.34 (0.03 ms)
192.168.0.52 (3.32 ms)
192.168.0.54 (2.32 ms)
192.168.0.65 (4.20 ms)
192.168.0.66 (1.28 ms)
192.168.0.67 (1.32 ms)
192.168.0.102 (0.02 ms)
192.168.0.1 (2.23 ms)

    256 targets
      10 alive
    248 unreachable
      0 unknown addresses

    244 timeouts (waiting for response)
    254 ICMP Echos sent
      10 ICMP Echo Replies received
    244 other ICMP received

0.02 ms (min round trip time)
2.80 ms (avg round trip time)
12.0 ms (max round trip time)
    10.794 sec (elapsed real time)

(END)

```

Abbildung 10.74 Ergebnisanzeige von »netz4.sh«

Das folgende Skriptfragment (Listing 10.2) dient Ihnen als Anregung für eigene Anwendungen:

```

#!/bin/sh
# Eingabe der Netzadresse
echo -n "Netzadresse eingeben: "; read netz
# fping als Datenquelle für for-Schleife
# Ausführen von fping, Umleitung der Fehlerausgabe nach /dev/null,
echo "Erreichbare Hosts"
for i in `fping -r 0 -aA -g $netz/24 2>/dev/null`
do
# Anzeige IP-Adresse
echo $i
# Auswertung für weitere Aktion
if [ "$i" = "192.168.0.1" ];
then
echo "Standard-Gateway"
fi
done
echo "-----"
echo "Nicht erreichbare Hosts"
# fping als Datenquelle für for-Schleife
# Ausführen von fping,
for i in `fping -r 0 -uA -g $netz/24 2> /dev/null`
do
echo $i

```

```
if [ "$i" = "192.168.0.0" ];
then
echo "Netzadresse, kein Host"
fi
done
```

Listing 10.2 Skriptfragment für eigene Entwicklungen

In dem Skriptfragment aus Listing 10.2 finden Sie zunächst eine `for`-Schleife, die die aktiven Hosts auflistet. Anstelle der Abfrage nach der Netzadresse können Sie die Variable `$netz` mit einem festen Wert belegen (`netz="192.168.0.0"`). Diese Zuweisung ersetzt dann die Abfragezeile. Mit dem `if`-Konstrukt werten Sie die mit dem Schleifendurchgang wechselnden Inhalte der Variable `i` aus. Als »Aktion« habe ich hier nur eine `echo`-Anweisung gewählt, die den angegebenen Text ausgibt. An dieser Stelle können Sie hier Ihre eigenen Anweisungen setzen: Wake-on-LAN, Softwareverteilung, Datensicherung, Rechner herunterfahren, da am Abend vom Benutzer vergessen, u. Ä.

Übrigens können Sie auch auf Windows-Rechnern solche Shell-Skripte laufen lassen. Den Shell-Interpreter `bash` finden Sie unter <http://win-bash.sourceforge.net>. Für die anderen Befehle (wie `less`) suchen Sie unter www.freecode.com.

10.7.8 Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen

Mit `ping` verwenden Sie ein Standardwerkzeug, das Sie auf allen Betriebssystemen vorfinden. Für Ihren Arbeitsalltag werden Sie vor allem die Optionen `-c <ZAHL der Pings>` und `-f` (»Dauerfeuer«) verwenden. Je nach Ausführung erhalten Sie als Antwort entweder ein schlichtes `alive` oder `not alive`. Andere Versionen zeigen Ihnen die Laufzeit, die Größe der Testpakete und eine statistische Zusammenfassung an:

```
harald@ze4:~$ ping -c 3 192.168.0.25
PING 192.168.0.25 (192.168.0.25) 56(84) bytes of data.
64 bytes from 192.168.0.25: icmp_req=1 ttl=64 time=0.056 ms
64 bytes from 192.168.0.25: icmp_req=2 ttl=64 time=0.049 ms
64 bytes from 192.168.0.25: icmp_req=3 ttl=64 time=0.052 ms
--- 192.168.0.25 ping statistics ---
3 packets transmitted, 3 received, 0 % packet loss, time 1999ms
rtt min/avg/max/mdev = 0.049/0.052/0.056/0.006 ms
```

Konnten Sie den Host nicht erreichen, sieht Ihre `ping`-Ausgabe so aus:

```
harald@ze4:~$ ping -c 1 192.168.0.26
PING 192.168.0.26 (192.168.0.26) 56(84) bytes of data.
From 192.168.0.34 icmp_seq=1 Destination Host Unreachable
--- 192.168.0.26 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100 % packet loss, time 0ms
```

Weitere Informationen liefert Ihnen die Manual-Seite (Linux, FreeBSD) oder die `help`-Option. Beachten Sie auch die Ausführungen zur Namensauflösung (Abschnitt 4.4.1, »Prüfung der Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6«) und ICMP (Kapitel 5, »Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen«).

Sie können auf ein weiteres Programm mit ähnlicher Funktionalität zurückgreifen. Mit `oping` testen Sie wahlweise IPv4- und IPv6-Adressen.

10.7.9 »cryptcat«: im Dienste der Sicherheit

Dieses bereits in Abschnitt 9.1.5 erwähnte Programm kann Ihnen helfen, offene Ports an Ihren Rechnern zu erkennen oder aber auf Portscans zu reagieren. Um sowohl die offenen als auch geschlossenen Ports eines Rechners zu scannen, wenden Sie diese Syntax an:

```
cryptcat -vv -z RECHNERNAME|IPADRESSE PORT|PORTBEREICH
```

Das Beispiel finden Sie in Abbildung 10.75.

```

harald@ze8:~$ cryptcat -vv -z sc03 20-25
sc03 [192.168.0.70] 25 (smtp) : Connection refused
sc03 [192.168.0.70] 24 (?) : Connection refused
sc03 [192.168.0.70] 23 (telnet) : Connection refused
sc03 [192.168.0.70] 22 (ssh) open
sc03 [192.168.0.70] 21 (ftp) : Connection refused
sc03 [192.168.0.70] 20 (ftp-data) : Connection refused
sent 0, rcvd 0
harald@ze8:~$

```

Abbildung 10.75 Anzeige des angegebenen Portbereichs

Möchten Sie nur offene Ports aufspüren, lassen Sie bei den Optionen ein `v` weg (Abbildung 10.76):

```
cryptcat -v -z RECHNERNAME|IPADRESSE PORT|PORTBEREICH
```

```

harald@ze8:~$ cryptcat -v -z sc03 20-25
sc03 [192.168.0.70] 22 (ssh) open
harald@ze8:~$

```

Abbildung 10.76 Anzeige offener Ports des angegebenen Portbereichs

Sie können das Programm gut in Shell-Skripte einbinden, denn bei der Verwendung einer einzigen Port-Angabe ist auch der Exitcode `$?` zur weiteren Steuerung auswertbar. Dies möchte Ihnen das minimalistische Beispiel in Listing 10.3 zeigen. Für Ihre Versuche in Ihrem eigenen lokalen Netz ersetzen Sie die großgeschriebenen Begriffe durch die entsprechenden Angaben.

```

#!/bin/sh
cryptcat -v -z RECHNERNAME|IPADRESSE PORT > /dev/null 2>&1
if [ $? -eq 0 ];
then
echo "SSH-Port geöffnet"
else
echo "SSH-Port geschlossen"
fi

```

Listing 10.3 Ein Shell-Skript mit »cryptcat«

Weitaus interessanter für die Praxis ist die Möglichkeit, auf Port-Ansprachen durch Scans oder andere Maßnahmen zu reagieren. Dazu starten Sie das Programm im Lauschmodus. Die Grundsyntax hierfür lautet:

```
cryptcat -v -n -l -p PORT
```

Dabei steht die Option `-n` für die Unterbindung der Namensauflösung (was ja eine nach außen gerichtete verräterische Aktion darstellen kann). Mit `-l` versetzen Sie das Programm in den Empfangsmodus. Der Port wird mittels `-p PORT` angegeben. Der angegebene Port darf nicht bereits durch andere Anwendungen belegt sein, andernfalls erhalten Sie nur eine Fehlermeldung.

`cryptcat` beendet sich nach einem einzigen Kontakt des Ports mit der Außenwelt und gibt den Exitcode `0` aus. Das in Listing 10.4 gezeigte Shell-Kommando `wall` dient der Ausgabe der Nachricht auf allen aktiven Terminalsitzungen. Aber Sie können hier natürlich auch noch weitere Aktionen vorsehen, bis hin zum kurzzeitigen Deaktivieren der Netzwerkkarte! Den Ablauf des Shell-Skripts und die Port-Abfrage von einem anderen Rechner aus finden Sie in Abbildung 10.77.

```
#!/bin/sh
cryptcat -v -n -l -p 7071
if [ $? -eq 0 ]
then
wall "Da hat wer angeklopft"
fi
```

Listing 10.4 »cryptcat« meldet einen Anklopfer.

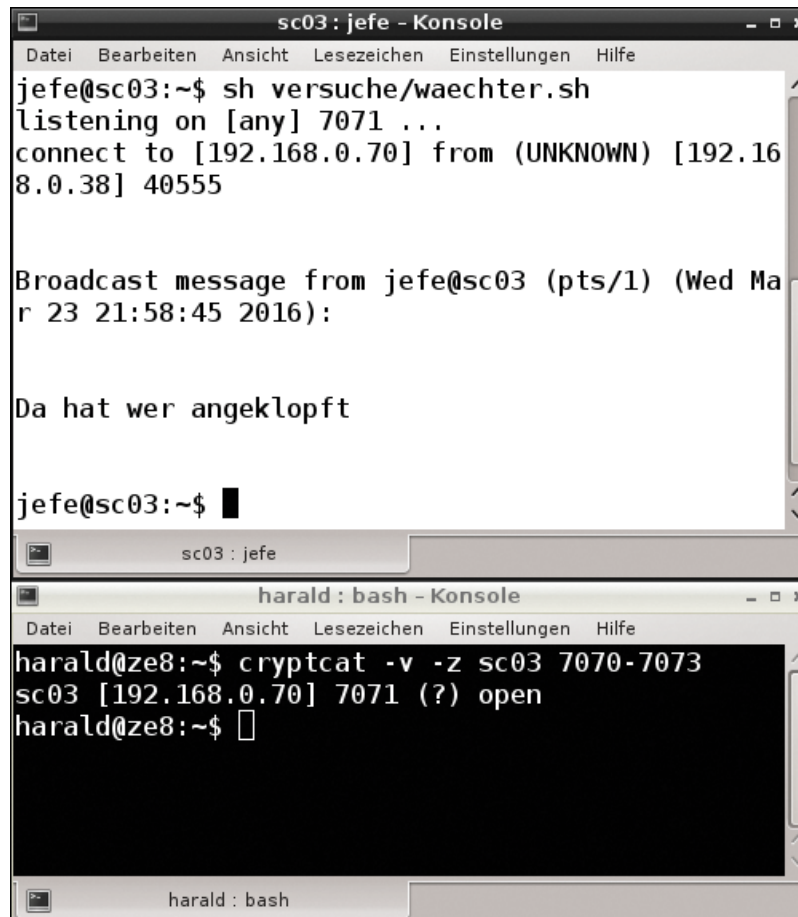


Abbildung 10.77 Reaktion auf Portscan

10.7.10 Weitere Systemabfragen auf Linux-Systemen

Mit `fuser` können Sie unter anderem ermitteln, welche Prozesse und deren Eigentümer welchen Port belegen. Die Informationen hieraus sind dann von Bedeutung, wenn sich eine Netzwerkanwendung nicht starten lässt, weil der gewünschte Port schon anderweitig belegt ist.

Die Abfrage geschieht in der Form:

```
fuser -u PORT/TCP|UDP
```

Die Abbildung 10.78 zeigt Ihnen die Ausgabe für den Port 22, der von einigen Prozessen genutzt wird.



Abbildung 10.78 Ausgabe von »fuser«

Im Verzeichnis `proc` finden Sie Informationen zu belegten Ressourcen, die der Kernel verwaltet. Mit den Shell-Befehlen `ls` und `cat` können Sie viele Informationen zu Prozessen auslesen. Sie müssen dafür als Benutzer `root` agieren.

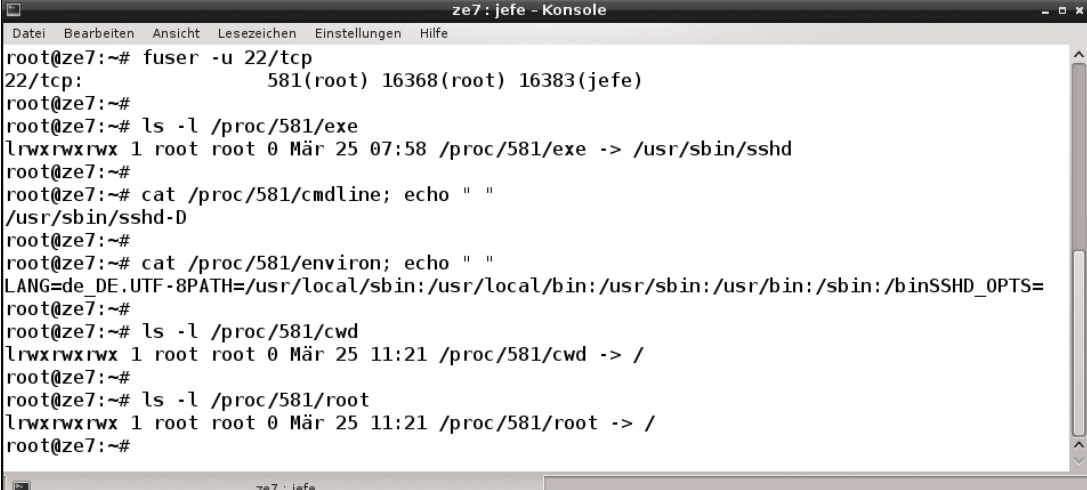
Nachdem die Prozesse über einen Port durch `fuser` ermittelt wurden, interessieren uns nun die Details dazu. Mit `PID` wird die betreffende Prozessnummer bezeichnet. Bei manchen Befehlen wurde das Kommando `echo " "` angereicht. Dies dient nur der Verbesserung der Lesbarkeit. Nachdem der von `cat` ausgegebene Information der Zeilenvorschub fehlt, würde unmittelbar daran der Systemprompt »geklebt«. Die Ausführung der nachfolgend gezeigten Vorgehensweise finden Sie in Abbildung 10.79.

```

Programm, das den Port belegt: ls -l /proc/PID/exe
Aufruf des Programms: cat /proc/PID/cmdline
Ausgabe der Umgebungstabelle: cat /proc/PID/enviro
Arbeitsverzeichnis des Prozesses: ls -l /proc/PID/cwd
Wurzelverzeichnis des Prozesses: ls -l /proc/PID/root

```

Mit `lsof` finden Sie ebenso Angaben über belegte Ressourcen. Dieses Programm verfügt über verschiedene Optionen, hier verwenden wir nur `-i`. Ports werden in der Form `:PORT` nach den Optionen angegeben. Die Manual-Seite informiert Sie über die vollständigen Möglichkeiten. In Abbildung 10.80 wird gezeigt, wie man Prozesse und Eigentümer ermittelt, die einen bestimmten Port benutzen.

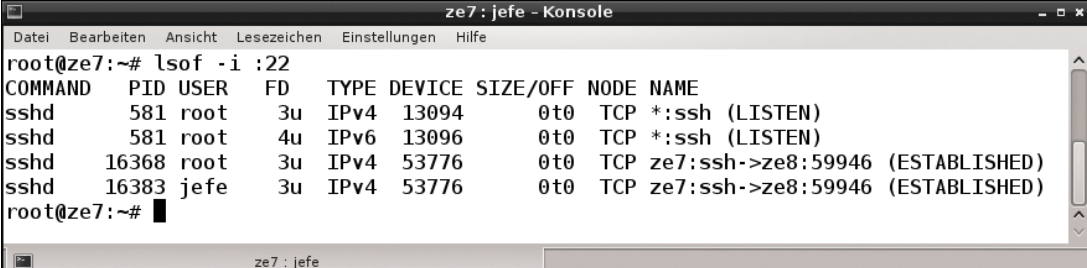


```

ze7: jefe - Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@ze7:~# fuser -u 22/tcp
22/tcp:          581(root) 16368(root) 16383(jefe)
root@ze7:~#
root@ze7:~# ls -l /proc/581/exe
lrwxrwxrwx 1 root root 0 Mär 25 07:58 /proc/581/exe -> /usr/sbin/sshd
root@ze7:~#
root@ze7:~# cat /proc/581/cmdline; echo " "
/usr/sbin/sshd-D
root@ze7:~#
root@ze7:~# cat /proc/581/enviro; echo " "
LANG=de_DE.UTF-8PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/binSSH_OPTS=
root@ze7:~#
root@ze7:~# ls -l /proc/581/cwd
lrwxrwxrwx 1 root root 0 Mär 25 11:21 /proc/581/cwd -> /
root@ze7:~#
root@ze7:~# ls -l /proc/581/root
lrwxrwxrwx 1 root root 0 Mär 25 11:21 /proc/581/root -> /
root@ze7:~#

```

Abbildung 10.79 Ermittlung weiterer Informationen über eine PID



```

ze7: jefe - Konsole
Datei Bearbeiten Ansicht Lesezeichen Einstellungen Hilfe
root@ze7:~# lsof -i :22
COMMAND  PID USER  FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      581 root   3u    IPv4  13094      0t0  TCP *:ssh (LISTEN)
sshd      581 root   4u    IPv6  13096      0t0  TCP *:ssh (LISTEN)
sshd     16368 root   3u    IPv4  53776      0t0  TCP ze7:ssh->ze8:59946 (ESTABLISHED)
sshd     16383 jefe   3u    IPv4  53776      0t0  TCP ze7:ssh->ze8:59946 (ESTABLISHED)
root@ze7:~#

```

Abbildung 10.80 Abfragen mit »lsof«

Ohne Angabe des Ports würden alle Prozesse, Benutzer und Programmaufrufe bezüglich belegter Netzwerkressourcen aufgelistet.

Beachten Sie, dass hier nur Grundlagen zur Netzwerksicherheit aufgeführt werden können. Die verschiedenen Gefahrenbilder sind leider dynamischer Natur und wechseln rasch. Halten Sie sich deshalb stets auf dem Laufenden. Führen Sie Sicherheitsupdates zeitnah aus. Verfolgen Sie den vielzitierten Grundsatz der Datensparsamkeit. Sensible Daten gehören in sichere »Schatzkammern«!